

Der Stellvertretende Generalsekretär

Herrn
Dr. Harald Dossi
Parlamentsdirektor
Parlament der Republik Österreich
Dr.-Karl-Renner-Ring 3
1017 Wien
ÖSTERREICH

D 313928 06.12.2022

Betrifft: Übermittlung von vom Europäischen Parlament während der Tagung vom 9. bis 10. November 2022 angenommenen Texten

Sehr geehrter Herr Parlamentsdirektor,

das Europäische Parlament hat auf seiner Tagung vom 9. bis 10. November 2022 folgende Texte angenommen, die es gemäß den den Verträgen beigefügten Protokollen Nr. 1 und 2 übermittelt:

Im Rahmen von Gesetzgebungsverfahren festgelegte Standpunkte

- Standpunkt festgelegt in erster Lesung im Hinblick auf den Erlass der Verordnung des Europäischen Parlaments und des Rates über den Binnenmarkt verzerrende drittstaatliche Subventionen,
- Standpunkt festgelegt in erster Lesung im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen,
- Standpunkt festgelegt in erster Lesung im Hinblick auf den Erlass der Verordnung des Europäischen Parlaments und des Rates 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) Nr. 2016/1011,
- Standpunkt festgelegt in erster Lesung im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates 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,

- Standpunkt festgelegt in erster Lesung im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

Die genannten Texte werden allen nationalen Parlamenten der Mitgliedstaaten gleichzeitig in der jeweiligen Landessprache zugeleitet. Als Datum der Zuleitung gilt das Datum dieses Schreibens.

Das Europäische Parlament hat ferner beschlossen, den nationalen Parlamenten die folgenden Texte zu übermitteln, die während derselben Tagung angenommen wurden und unter kein Gesetzgebungsverfahren fallen:

- Standpunkt zu dem Entwurf eines Beschlusses des Rates über den Abschluss – im Namen der Europäischen Union – des Abkommens zwischen der Europäischen Union und der Ukraine über die Beförderung von Gütern im Straßenverkehr,
- Standpunkt zu dem Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens – im Namen der Europäischen Union – zwischen der Europäischen Union und der Republik Moldau über die Beförderung von Gütern im Straßenverkehr,
- Standpunkt zu dem Entwurf eines Beschlusses des Rates über den Abschluss – im Namen der Europäischen Union – eines Abkommens über die Änderung der Listen spezifischer Verpflichtungen im Rahmen des Allgemeinen Übereinkommens über den Handel mit Dienstleistungen zur Einbeziehung von Anhang 1 der Erklärung über den Abschluss der Verhandlungen über die innerstaatliche Regelung von Dienstleistungen vom 2. Dezember 2021.

Als Anlage übermittle ich Ihnen im Namen der Präsidentin des Europäischen Parlaments die genannten Texte.

Mit vorzüglicher Hochachtung



Markus Winkler

Anlagen



EUROPÄISCHES PARLAMENT

2022 - 2023

AUSZUG

AUS DEM DOKUMENT „ANGENOMMENE TEXTE“

DER TAGUNG VOM
09. – 10. November 2022



INHALTSVERZEICHNIS

P9_TA(2022)0379	5
DEN BINNENMARKT VERZERRENDE DRITTSTAATLICHE SUBVENTIONEN	
P9_TA(2022)0380	171
RICHTLINIE HINSICHTLICH DER NACHHALTIGKEITSBERICHTERSTATTUNG VON UNTERNEHMEN	
P9_TA(2022)0381	405
DIGITALES FINANZWESEN: VERORDNUNG ÜBER DIE BETRIEBSSTABILITÄT DIGITALER SYSTEME DES FINANZSEKTORS (DORA)	
P9_TA(2022)0382	675
DIGITALES FINANZWESEN: ÄNDERUNG DER RICHTLINIE HINSICHTLICH DER ANFORDERUNGEN AN DIE DIGITALE BETRIEBSSTABILITÄT	
P9_TA(2022)0383	715
HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU IN DER UNION	
P9_TA(2022)0376	963
ABKOMMEN EU-UKRAINE ÜBER DIE BEFÖRDERUNG VON GÜTERN IM STRAßENVERKEHR	
P9_TA(2022)0377	965
ABKOMMEN EU-MOLDAU ÜBER DIE BEFÖRDERUNG VON GÜTERN IM STRAßENVERKEHR	
P9_TA(2022)0378	967
ABSCHLUSS EINES ABKOMMENS IM RAHMEN DES GATS ÜBER DIE ÄNDERUNG DER LISTEN SPEZIFISCHER VERPFLICHTUNGEN	



ANGENOMMENE TEXTE

P9_TA(2022)0379

Den Binnenmarkt verzerrende drittstaatliche Subventionen

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Binnenmarkt verzerrende drittstaatliche Subventionen (COM(2021)0223 – C9-0167/2021 – 2021/0114(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2021)0223),
 - gestützt auf Artikel 294 Absatz 2 und die Artikel 207 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0167/2021),
 - unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 20. Oktober 2021¹,
 - unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 13. Juli 2022 gemachte Zusage, den Standpunkt des Parlaments gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,
 - gestützt auf Artikel 59 seiner Geschäftsordnung,
 - unter Hinweis auf die Stellungnahmen des Ausschusses für Wirtschaft und Währung, des Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses;
 - unter Hinweis auf den Bericht des Ausschusses für internationalen Handel (A9-0135/2022),
1. legt den folgenden Standpunkt in erster Lesung fest²;

¹ ABl. C 105 vom 4.3.2022, S. 87.

2. billigt die Gemeinsame Erklärung des Parlaments, des Rates und der Kommission, die im *Amtsblatt der Europäischen Union*, Reihe C, veröffentlicht wird;
3. nimmt die dieser Entschließung beigefügten Erklärungen der Kommission zur Kenntnis, die im *Amtsblatt der Europäischen Union*, Reihe C, veröffentlicht werden;
4. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;
5. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

² Dieser Standpunkt ersetzt die am 4. Mai 2022 angenommenen Abänderungen (Angenommene Texte P9_TA(2022)0143).

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 10. November 2022 im Hinblick auf den Erlass der Verordnung (EU) 2022/... des Europäischen Parlaments und des Rates über den Binnenmarkt verzerrende drittstaatliche Subventionen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 114 und 207,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses³,

gemäß dem ordentlichen Gesetzgebungsverfahren⁴,

³ ABl. C 105 vom 4.3.2022, S. 87.

⁴ Stellungnahme des Europäischen Parlaments vom 10. November 2022.

in Erwägung nachstehender Gründe:

- (1) Ein starker, offener und wettbewerbsorientierter Binnenmarkt stellt sicher, dass sowohl europäische als auch drittstaatliche Unternehmen miteinander in Leistungswettbewerb treten können. Die Union verfügt über ein ausgefeiltes und wirksames System der Beihilfenkontrolle, das darauf abzielt, für alle Unternehmen, die eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausüben, faire Bedingungen zu gewährleisten. Dieses System der Beihilfenkontrolle verhindert, dass Mitgliedstaaten staatliche Beihilfen gewähren, die den Wettbewerb auf dem Binnenmarkt in ungerechtfertigter Weise verzerren.
- (2) Sowohl ***private Unternehmen als auch öffentliche*** Unternehmen, die der direkten oder indirekten Kontrolle eines Staates unterliegen, können jedoch von Drittstaaten Subventionen erhalten, die dann beispielsweise für die Finanzierung wirtschaftlicher Tätigkeiten in einem Wirtschaftszweig auf dem Binnenmarkt verwendet werden, etwa für die Teilnahme an öffentlichen Vergabeverfahren oder für den Erwerb von Unternehmen, unter Umständen auch derer, die über strategische Vermögenswerte wie kritische Infrastrukturen und innovative Technologien verfügen. Solche drittstaatlichen Subventionen unterliegen bislang nicht den Unionsvorschriften für staatliche Beihilfen.

- (3) *Diese Verordnung gilt für alle Wirtschaftszweige, einschließlich derer, die für die Union von strategischem Interesse sind, und für kritische Infrastrukturen, wie etwa jene, die in Artikel 4 Absatz 1 Buchstabe a der Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates genannt werden⁵.*
- (4) Drittstaatliche Subventionen können den Binnenmarkt verzerren und den fairen Wettbewerb für verschiedene wirtschaftliche Tätigkeiten in der Union untergraben. Diese Gefahr besteht insbesondere in Fällen, in denen Zusammenschlüsse eine Änderung der Kontrolle über Unionsunternehmen zur Folge haben, wenn sie ganz oder teilweise durch drittstaatliche Subventionen finanziert werden, oder in denen **Wirtschaftsteilnehmer**, denen drittstaatliche Subventionen gewährt werden, bei Vergabeverfahren in der Union den Zuschlag erhalten.

⁵ 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 79I vom 21.3.2019, S. 1).

- (5) Die Union verfügt bislang nicht über Instrumente, um durch drittstaatliche Subventionen verursachte Verzerrungen anzugehen. Die Kommission kann auf der Grundlage handelspolitischer Schutzinstrumente tätig werden, wenn subventionierte Waren in die Union eingeführt werden, nicht aber in Fällen, in denen drittstaatliche Subventionen in Form subventionierter Investitionen gewährt werden oder in denen es um Dienstleistungen bzw. Finanzströme geht. Gemäß dem WTO-Übereinkommen über Subventionen und Ausgleichsmaßnahmen hat die Union bei bestimmten von WTO-Mitgliedern gewährten drittstaatlichen Subventionen, die auf Waren beschränkt sind, die Möglichkeit, ein zwischenstaatliches Streitschlichtungsverfahren einzuleiten.
- (6) Es ist daher notwendig, die bestehenden Unionsinstrumente durch ein neues Instrument zu ergänzen, mit dem durch drittstaatliche Subventionen verursachte Verzerrungen auf dem Binnenmarkt wirksam angegangen werden können, **um** faire Wettbewerbsbedingungen zu gewährleisten. Das neue Instrument ergänzt insbesondere die Beihilfenvorschriften der Union, die durch mitgliedstaatliche Subventionen verursachte Verzerrungen auf dem Binnenmarkt betreffen.

- (7) Es ist wichtig, dass Regeln und Verfahren zur Prüfung drittstaatlicher Subventionen, die den Binnenmarkt tatsächlich oder potenziell verzerren, festgelegt werden, und dass die festgestellten Verzerrungen gegebenenfalls beseitigt werden. Drittstaatliche Subventionen könnten den Binnenmarkt verzerren, wenn ein Unternehmen, das von der drittstaatlichen Subvention profitiert, eine wirtschaftliche Tätigkeit in der Union ausübt. **Die ordnungsgemäße Anwendung und Durchsetzung dieser Verordnung soll zur Resilienz des Binnenmarkts gegen Verzerrungen durch drittstaatliche Subventionen und dadurch zur offenen strategischen Autonomie der Union beitragen.** Daher legt diese Verordnung Vorschriften für alle Unternehmen, **einschließlich öffentlicher Unternehmen, die der direkten oder indirekten Kontrolle eines Staates unterliegen,** fest, die in der Union eine wirtschaftliche Tätigkeit ausüben. Angesichts der Bedeutung der von kleinen und mittleren Unternehmen (KMU) ausgeübten wirtschaftlichen Tätigkeiten und ihres Beitrags zur Verwirklichung der wichtigsten politischen Ziele der Union muss den Auswirkungen dieser Verordnung auf KMU besondere Aufmerksamkeit gewidmet werden.

- (8) Um einen fairen Wettbewerb im gesamten Binnenmarkt und eine kohärente Anwendung dieser Verordnung zu gewährleisten, liegt die ausschließliche Zuständigkeit für die Anwendung dieser Verordnung bei der Kommission. Die Kommission sollte befugt sein, jegliche drittstaatliche Subvention in einem Wirtschaftszweig, soweit sie in den Anwendungsbereich dieser Verordnung fällt, von Amts wegen zu prüfen und sich dabei auf Informationen aus allen verfügbaren Quellen stützen können. Um speziell bei großen Zusammenschlüssen (Fusionen und Übernahmen) und öffentlichen Vergabeverfahren, die bestimmte Schwellenwerte überschreiten, eine wirksame Kontrolle zu gewährleisten, sollte die Kommission befugt sein, drittstaatliche Subventionen auf der Grundlage einer vorherigen Anmeldung bzw. Meldung seitens des jeweiligen Unternehmens bei der Kommission zu prüfen.
- (9) ***Diese Verordnung sollte unter Berücksichtigung der einschlägigen Rechtsvorschriften der Union, einschließlich der Rechtsvorschriften über staatliche Beihilfen, Fusionen und die Vergabe öffentlicher Aufträge, angewandt und ausgelegt werden.***

- (10) *Die Durchführung dieser Verordnung lässt das Recht jedes Mitgliedstaats, seine wesentlichen Sicherheitsinteressen gemäß Artikel 346 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zu schützen, unberührt.*
- (11) *Als „drittstaatliche Subvention“ sollte eine finanzielle Zuwendung gelten, die direkt oder indirekt von einem Drittstaat stammt, die einen Vorteil verschafft und die auf ein oder mehrere Unternehmen oder Wirtschaftszweige beschränkt ist. Diese Bedingungen sind kumulativ.*

- (12) **Eine** finanzielle Zuwendung kann von öffentlichen oder privaten Einrichtungen gewährt werden. Ob eine öffentliche Einrichtung eine finanzielle Zuwendung gewährt **hat**, sollte jeweils im Einzelfall unter gebührender Berücksichtigung von Elementen wie den Merkmalen der betreffenden Einrichtung und dem rechtlichen und wirtschaftlichen Umfeld in dem **Drittstaat**, in dem die Einrichtung tätig ist, einschließlich der Rolle der Regierung in der Wirtschaft **jenes Staats**, festgestellt werden. Die finanzielle Zuwendung kann auch von einer privaten Einrichtung gewährt werden, wenn die Handlungen dieser privaten Einrichtung einem Drittstaat zugerechnet werden können. **Der Begriff „finanzielle Zuwendung“ umfasst eine breite Palette von Unterstützungsmaßnahmen, die nicht auf Geldtransfers beschränkt sind, wie beispielsweise die Gewährung besonderer oder ausschließlicher Rechte an ein Unternehmen ohne angemessene, den normalen Marktbedingungen entsprechende Vergütung.**

- (13) Durch eine finanzielle Zuwendung sollte einem Unternehmen, das eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausübt, ein Vorteil verschafft werden. Eine finanzielle Zuwendung sollte als Vorteil für ein Unternehmen angesehen werden, **wenn dieser Vorteil unter normalen Marktbedingungen nicht hätte erlangt werden können.** Die Feststellung, ob ein Vorteil entsteht, sollte auf der Grundlage komparativer Referenzwerte erfolgen, wie der Investitionspraxis privater Investoren, der auf dem Markt erhältlichen Finanzierungssätze, einer vergleichbaren steuerlichen Behandlung oder der angemessenen Vergütung für eine bestimmte Ware oder Dienstleistung. Stehen keine direkt vergleichbaren Referenzwerte zur Verfügung, könnten bestehende Referenzwerte angepasst oder alternative Referenzwerte auf der Grundlage allgemein anerkannter Beurteilungsmethoden ermittelt werden. **Vorteile können beispielsweise im Rahmen der Beziehungen zwischen Behörden und öffentlichen Unternehmen verschafft werden, wenn eine solche Beziehung und insbesondere eine etwaige Finanzierung öffentlicher Unternehmen durch die Behörden nicht den normalen Marktbedingungen entspricht. Bei der Bereitstellung oder dem Erwerb von Waren oder Dienstleistungen im Rahmen eines wettbewerbsorientierten, transparenten und diskriminierungsfreien Vergabeverfahrens ist davon auszugehen, dass sie den normalen Marktbedingungen entspricht.**

Eine finanzielle Zuwendung an ein Unternehmen, das eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausübt, sollte nicht als Zuwendung betrachtet werden, durch die ein Vorteil entsteht, wenn die Beurteilung aufgrund der Referenzwerte ergibt, dass das Unternehmen diesen Vorteil auch unter normalen Marktbedingungen erlangt hätte. Durch Verrechnungspreise im Zusammenhang mit Waren und Dienstleistungen, die innerhalb eines Unternehmens ausgetauscht werden, kann ein Vorteil verschafft werden, wenn diese Verrechnungspreise nicht den normalen Marktbedingungen entsprechen. Der durch eine finanzielle Zuwendung entstandene Vorteil kann an ein Unternehmen weitergegeben werden, das eine wirtschaftliche Tätigkeit in der Union ausübt.

- (14) *Der* Vorteil sollte **einem oder mehreren** Unternehmen oder Wirtschaftszweigen verschafft werden. Die **Spezifizität einer drittstaatlichen Subvention** kann rechtlich oder faktisch festgestellt werden.

- (15) *Eine drittstaatliche Subvention gilt von dem Moment an als gewährt, ab dem der Begünstigte einen Anspruch auf die drittstaatliche Subvention erhält. Die tatsächliche Auszahlung der drittstaatlichen Subvention ist keine notwendige Voraussetzung dafür, dass eine drittstaatliche Subvention in den Anwendungsbereich dieser Verordnung fällt.*
- (16) *Eine finanzielle Zuwendung, die ausschließlich für die nichtwirtschaftlichen Tätigkeiten eines Unternehmens geleistet wird, stellt keine drittstaatliche Subvention dar. Wird jedoch eine finanzielle Zuwendung für eine nichtwirtschaftliche Tätigkeit zur Quersubventionierung der wirtschaftlichen Tätigkeiten des Unternehmens verwendet, so kann dies einer drittstaatlichen Subvention gleichkommen, die in den Anwendungsbereich dieser Verordnung fällt. Verwendet ein Unternehmen finanzielle Zuwendungen – z. B. in Form besonderer oder ausschließlicher Rechte oder als Ausgleich für eine von Behörden auferlegte Belastung – zur Quersubventionierung anderer Tätigkeiten, könnte diese Quersubventionierung ein Hinweis darauf sein, dass die besonderen oder ausschließlichen Rechte ohne angemessene Vergütung gewährt werden oder dass die Belastung überkompensiert wird und somit einer drittstaatlichen Subvention gleichkommt.*

- (17) Sobald das Vorliegen einer drittstaatlichen Subvention festgestellt wurde, sollte die Kommission **im Einzelfall** prüfen, ob diese den Binnenmarkt verzerrt. Im Unterschied zu staatlichen Beihilfen, die von einem Mitgliedstaat gewährt werden, sind drittstaatliche Subventionen im Allgemeinen nicht verboten. ■
- (18) Aufgrund des bei zahlreichen drittstaatlichen Subventionen bestehenden Mangels an Transparenz und der Komplexität der wirtschaftlichen Gegebenheiten kann es unter Umständen schwierig sein, die Auswirkungen einer bestimmten drittstaatlichen Subvention auf den Binnenmarkt eindeutig zu ermitteln oder zu quantifizieren. Daher erscheint es notwendig, bei der Feststellung von Verzerrungen eine nicht erschöpfende Liste von Indikatoren zu verwenden. Bei der Beurteilung, inwieweit eine drittstaatliche Subvention geeignet ist, die Wettbewerbsposition **eines** Unternehmens zu verbessern und dadurch den Wettbewerb auf dem Binnenmarkt tatsächlich oder potenziell zu beeinträchtigen, könnte die Kommission bestimmte Indikatoren heranziehen, darunter Höhe und Art der drittstaatlichen Subvention, ihren Zweck und die an sie geknüpften Bedingungen sowie ihre Verwendung auf dem Binnenmarkt.

- (19) Bei der Anwendung der Indikatoren zur Feststellung einer Verzerrung auf dem Binnenmarkt könnte die Kommission verschiedene Faktoren wie den Umfang der drittstaatlichen Subvention in absoluten Zahlen oder im Verhältnis zur Größe des Marktes oder zum Wert der Investition berücksichtigen. So dürfte beispielsweise ein Zusammenschluss, bei dem eine drittstaatliche Subvention einen wesentlichen Teil des für den Erwerb des Zielunternehmens gezahlten Preises deckt, eine verzerrende Wirkung haben. Ebenso dürften drittstaatliche Subventionen, die einen wesentlichen Teil des geschätzten Wertes eines Auftrags, der bei einem öffentlichen Vergabeverfahren vergeben werden soll, decken, zu Verzerrungen führen. Gewährt ein Drittstaat eine Subvention für Betriebskosten, so dürfte diese mit höherer Wahrscheinlichkeit zu Verzerrungen führen als eine drittstaatliche Subvention für Investitionskosten. Bei drittstaatlichen Subventionen für KMU ist die Wahrscheinlichkeit geringer, dass sie Verzerrungen bewirken, als bei drittstaatlichen Subventionen für große Unternehmen. Darüber hinaus sollten die Merkmale des Marktes, insbesondere die Wettbewerbsbedingungen auf dem Markt, beispielsweise Marktzutrittsschranken, berücksichtigt werden.

Drittstaatliche Subventionen **auf Märkten, die durch Überkapazitäten gekennzeichnet sind**, oder drittstaatliche Subventionen, die zu Überkapazitäten führen, weil dadurch unwirtschaftliche Vermögenswerte weiterbetrieben werden oder Investitionen in Kapazitätserweiterungen, die andernfalls nicht errichtet worden wären, gefördert werden, dürften zu Verzerrungen führen. Eine drittstaatliche Subvention für einen Begünstigten, dessen Tätigkeit auf dem Binnenmarkt, beispielsweise gemessen an dem in der Union erzielten Umsatz, nicht umfangreich ist, führt mit geringerer Wahrscheinlichkeit zu Verzerrungen als eine drittstaatliche Subvention für einen Begünstigten, der eine umfangreichere Tätigkeit auf dem Binnenmarkt ausübt. Es sollte bei drittstaatlichen Subventionen, die **4 Mio. EUR in einem Zeitraum von drei aufeinanderfolgenden Geschäftsjahren** nicht übersteigen, grundsätzlich als unwahrscheinlich angesehen werden, dass sie im Sinne dieser Verordnung den Binnenmarkt verzerren. **Drittstaatliche Subventionen für ein einziges Unternehmen, die in einem Zeitraum von drei aufeinanderfolgenden Geschäftsjahren den Betrag einer von einem Drittstaat gewährten De-minimis-Beihilfe im Sinne von Artikel 3 Absatz 2 der Verordnung (EU) Nr. 1407/2013 der Kommission⁶ nicht übersteigen, sollten im Sinne dieser Verordnung als den Binnenmarkt nicht verzerrend gelten.**

⁶ Verordnung (EU) Nr. 1407/2013 der Kommission vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen (ABl. L 352 vom 24.12.2013, S.1).

- (20) Ebenso wie bestimmte Arten staatlicher Beihilfen dürften aufgrund ihrer Natur insbesondere auch bestimmte Kategorien drittstaatlicher Subventionen, wie etwa unbegrenzte Garantien, **jene, für die die Höhe oder Laufzeit der Garantie nicht begrenzt ist**, zu Verzerrungen auf dem Binnenmarkt führen. **Gleiches gilt für ein ungerechtfertigt günstiges Angebot, dessen Vorteilhaftigkeit, wie etwa sein Preis, nicht durch andere Faktoren gerechtfertigt werden kann. Darüber hinaus können Subventionen in Form von Ausführfinanzierungen, sofern sie nicht im Einklang mit dem OECD-Übereinkommen über öffentlich unterstützte Exportkredite gewährt werden, aufgrund ihrer verzerrenden Auswirkungen Anlass zu besonderer Besorgnis geben. Da bei diesen Kategorien drittstaatlicher Subventionen die Wahrscheinlichkeit am größten ist, dass sie zu Verzerrungen auf dem Binnenmarkt führen, ist es nicht erforderlich**, dass die Kommission eine detaillierte Beurteilung auf der Grundlage von Indikatoren **vornimmt**. Ein Unternehmen könnte in jedem Fall nachweisen, dass die betreffende drittstaatliche Subvention den Binnenmarkt unter den besonderen Umständen des jeweiligen Falls nicht verzerren würde.

- (21) **Die Mitgliedstaaten sowie jede natürliche oder juristische Person können Informationen über die positiven Auswirkungen einer drittstaatlichen Subvention vorlegen, die die Kommission bei der Abwägungsprüfung gebührend berücksichtigen sollte. Die Kommission sollte die positiven Auswirkungen der drittstaatlichen Subvention auf der Grundlage der während der Untersuchung vorgelegten Belege für solche positiven Auswirkungen berücksichtigen. Die positiven Auswirkungen sollten sich auf die Entwicklung der jeweils subventionierten wirtschaftlichen Tätigkeit auf dem Binnenmarkt beziehen. Gegebenenfalls sollten andere positive Auswirkungen berücksichtigt werden, um zu vermeiden, dass die Abwägungsprüfung zu einer ungerechtfertigten Diskriminierung führt. Die Kommission sollte auch die umfassenderen positiven Auswirkungen in Bezug auf die einschlägigen politischen Ziele, insbesondere diejenigen der Union, prüfen. Zu diesen politischen Zielen können insbesondere ein hohes Niveau bei Umweltschutz und Sozialstandards sowie die Förderung von Forschung und Entwicklung gezählt werden.** Diese positiven Auswirkungen sollte die Kommission gegen die negativen Auswirkungen einer drittstaatlichen Subvention in Form von Verzerrungen auf dem Binnenmarkt abwägen.

*Im Rahmen eines öffentlichen Vergabeverfahrens sollte die Kommission die Verfügbarkeit alternativer Bezugsquellen für die betreffenden Waren und Dienstleistungen berücksichtigen. Die Abwägungsprüfung kann zu dem Schluss führen, dass **keine** Abhilfemaßnahmen eingeführt werden sollten, **wenn die positiven Auswirkungen der drittstaatlichen Subvention die negativen Auswirkungen überwiegen. Bei Kategorien** drittstaatlicher Subventionen, bei denen die Wahrscheinlichkeit, dass sie den Binnenmarkt verzerren, als am größten angesehen wird, ist es weniger wahrscheinlich, dass die **positiven Auswirkungen die negativen Auswirkungen überwiegen. Wenn die negativen Auswirkungen überwiegen, kann die Abwägungsprüfung helfen, die angemessene Art und den angemessenen Umfang der Verpflichtungen oder Abhilfemaßnahmen festzustellen. Da bei der Abwägungsprüfung die positiven Auswirkungen einer drittstaatlichen Subvention geprüft werden, sollte die Durchführung einer solchen Abwägungsprüfung nicht zu einem Ergebnis führen, das für das Unternehmen schlechter wäre als ohne die Durchführung einer Abwägungsprüfung. Wenn die Kommission eine Abwägungsprüfung durchführt, sollte sie ihre Begründung im Beschluss zum Abschluss einer eingehenden Prüfung darlegen.***

- (22) Wenn die Kommission eine drittstaatliche Subvention von Amts wegen prüft, sollte sie befugt sein, einem Unternehmen gegenüber Abhilfemaßnahmen aufzuerlegen, um eine durch die drittstaatliche Subvention verursachte Verzerrung auf dem Binnenmarkt zu beseitigen. Die Abhilfemaßnahmen sollten **strukturelle und nichtstrukturelle Maßnahmen sowie** die Rückzahlung der drittstaatlichen Subvention umfassen; **sie sollten geeignet sein, die betreffende Verzerrung zu beseitigen, und verhältnismäßig sein. Bei der Prüfung alternativer Abhilfemaßnahmen, die jeweils die Verzerrung vollständig und wirksam beseitigen würden, sollte die Kommission diejenige Abhilfemaßnahme wählen, die für das untersuchte Unternehmen die geringste Belastung darstellt.**
- (23) Das Unternehmen, **das Gegenstand der Prüfung ist**, sollte die Möglichkeit haben, Verpflichtungszusagen zu unterbreiten, um die durch die drittstaatliche Subvention verursachte Verzerrung zu beseitigen. Wenn die Kommission der Auffassung ist, dass die angebotenen Verpflichtungen die Verzerrung vollständig und wirksam beseitigen, kann sie sie akzeptieren und durch Beschluss für bindend erklären. **In diesem Fall sollte die Kommission keine Abhilfemaßnahmen auferlegen.**

- (24) Das Unternehmen, **das Gegenstand der Prüfung ist**, kann anbieten, die Subvention zuzüglich angemessener Zinsen zurückzuzahlen. Die Kommission sollte eine als Verpflichtung angebotene Rückzahlung akzeptieren, wenn sie feststellen kann, dass die Rückzahlung die Verzerrung vollständig beseitigt, transparent **und überprüfbar** durchgeführt wird und in der Praxis wirksam ist; dabei trägt die Kommission dem Risiko einer Umgehung der Ziele dieser Verordnung Rechnung.
- (25) Wenn das **Unternehmen, das Gegenstand der Prüfung ist**, keine Verpflichtungszusagen unterbreitet, mit denen die festgestellte Verzerrung vollständig und wirksam beseitigt würde, sollte die Kommission befugt sein, einen Zusammenschluss bzw. einen Zuschlag vor dem Vollzug des Zusammenschlusses bzw. der Auftragsvergabe zu untersagen. In Fällen, in denen der Zusammenschluss bereits vollzogen wurde, insbesondere weil keine vorherige Anmeldung erforderlich war, da die Anmeldeschwellen nicht erreicht wurden, kann die Verzerrung dennoch so erheblich sein, dass sie nicht durch verhaltensbezogene oder strukturelle Maßnahmen oder durch die Rückzahlung der Subvention beseitigt werden kann. In solchen Fällen sollte die Kommission beschließen können, die Verzerrung zu beseitigen, indem sie anordnet, dass die Unternehmen den Zusammenschluss rückgängig machen.

- (26) *Das Unternehmen, das Gegenstand der Prüfung ist, könnte anbieten, oder die Kommission könnte, wenn dies verhältnismäßig und erforderlich ist, das Unternehmen, das Gegenstand der Prüfung ist, verpflichten, die Kommission einen angemessenen Zeitraum lang über ihre Teilnahme an künftigen Zusammenschlüssen oder öffentlichen Vergabeverfahren in der Union zu unterrichten. Die Übermittlung einer solchen Unterrichtung bzw. die Antwort oder das Ausbleiben einer Antwort der Kommission kann bei dem Unternehmen kein berechtigtes Vertrauen darauf begründen, dass die Kommission nicht zu einem späteren Zeitpunkt eine Prüfung möglicher drittstaatlicher Subventionen für das an dem Zusammenschluss oder dem öffentlichen Vergabeverfahren beteiligte Unternehmen einleiten wird.*

- (27) Die Kommission sollte befugt sein, jegliche Informationen über drittstaatliche Subventionen von Amts wegen zu prüfen. *Die Mitgliedstaaten sowie jede natürliche oder juristische Person oder Vereinigung sollten der Kommission Informationen über mutmaßliche drittstaatliche Subventionen, die den Binnenmarkt verzerren, übermitteln können. Die Kommission könnte eine Kontaktstelle einrichten, um die vertrauliche Übermittlung solcher Informationen zu erleichtern. Die Kommission sollte sicherstellen, dass diejenigen Mitgliedstaaten, die der Kommission einschlägige Informationen über mutmaßliche den Binnenmarkt verzerrende drittstaatliche Subventionen übermitteln, eine Antwort erhalten. Zur Untersuchung möglicher drittstaatlicher Subventionen und ob diese den Binnenmarkt verzerren, und zur Beseitigung solcher Verzerrungen wird mit der vorliegenden Verordnung ein zweistufiges Verfahren eingeführt, das aus einer Vorprüfung und einer eingehenden Prüfung besteht. Ein Unternehmen, das Gegenstand eines dieser beiden Schritte ist, sollte als Unternehmen gelten, das Gegenstand einer Prüfung ist.*

- (28) Der Kommission sollten angemessene Untersuchungsbefugnisse übertragen werden, damit sie alle erforderlichen Informationen einholen kann. Sie sollte daher befugt sein, während des gesamten Verfahrens von allen Unternehmen bzw. Unternehmensvereinigungen Auskünfte einzuholen. Darüber hinaus sollte die Kommission befugt sein, Geldbußen oder Zwangsgelder zu verhängen, wenn die angeforderten Auskünfte nicht fristgerecht erteilt werden oder unvollständige, unrichtige oder irreführende Angaben gemacht werden. Die Kommission sollte auch Fragen an Mitgliedstaaten oder Drittstaaten richten können. Darüber hinaus sollte die Kommission befugt sein, Nachprüfungen in den *in der Union gelegenen* Räumlichkeiten *eines* Unternehmens *bzw.* einer *Unternehmensvereinigung bzw. – vorbehaltlich der offiziellen Unterrichtung und Zustimmung des betreffenden Drittstaats* – in den Räumlichkeiten des Unternehmens in dem Drittstaat durchzuführen. *Um eine wirksame Nachprüfung zu gewährleisten, sollte die Kommission die Befugnis haben, das Unternehmen oder die Unternehmensvereinigung zu ersuchen, der Nachprüfung zuzustimmen.* Wenn das Unternehmen, *das Gegenstand der Prüfung ist, oder der Drittstaat, der die Subvention gewährt hat*, nicht kooperiert, sollte die Kommission ferner befugt sein, einen Beschluss auf der Grundlage der verfügbaren Informationen zu erlassen.

- (29) Darüber hinaus sollte die Kommission befugt sein, einstweilige Maßnahmen anzuordnen, wenn dies erforderlich ist, um eine **nicht wiedergutzumachende Schädigung** des Wettbewerbs auf dem Binnenmarkt abzuwenden.
- (30) Wenn der Kommission aufgrund der Vorprüfung hinreichende Anhaltspunkte für das Vorliegen einer den Binnenmarkt verzerrenden drittstaatlichen Subvention vorliegen, sollte die Kommission befugt sein, eine eingehende Prüfung einzuleiten, um zusätzliche sachdienliche Informationen zur Beurteilung der drittstaatlichen Subvention einzuholen. **Das Unternehmen, das Gegenstand der Prüfung ist, sollte die Möglichkeit haben**, seine Verteidigungsrechte auszuüben.
- (31) Die Kommission sollte die eingehende Prüfung mit dem Erlass eines Beschlusses abschließen. **Sie sollte sich bemühen, die eingehende Prüfung möglichst innerhalb von 18 Monaten abzuschließen, wobei insbesondere die Komplexität des Falls und die Kooperationsbereitschaft von den betreffenden Unternehmen und Drittländern zu berücksichtigen sind.**

- (32) Die Kommission sollte über geeignete Instrumente verfügen, um die Wirksamkeit der Verpflichtungen und der Abhilfemaßnahmen sicherzustellen. Kommt ein Unternehmen einem Beschluss, mit dem Verpflichtungen für bindend erklärt wurden, einem Beschluss ***zur Auferlegung von*** Abhilfemaßnahmen, oder einem Beschluss, mit dem einstweilige Maßnahmen angeordnet wurden, nicht nach, sollte die Kommission befugt sein, Geldbußen oder Zwangsgelder ***mit hinreichend abschreckender Wirkung*** zu verhängen. ***Die Kommission sollte bei der Verhängung dieser Geldbußen oder Zwangsgelder Fälle wiederholter Verstöße berücksichtigen. Um die Wirksamkeit dieser Verordnung zu erhöhen, kann die Kommission Verpflichtungen oder Abhilfemaßnahmen gleichzeitig mit der Verhängung von Geldbußen oder Zwangsgeldern auferlegen.***
- (33) Um die ordnungsgemäße und wirksame Anwendung dieser Verordnung zu gewährleisten, sollte die Kommission befugt sein, einen Beschluss aufzuheben und einen neuen zu erlassen, wenn der ursprüngliche Beschluss auf unvollständigen, unrichtigen oder irreführenden Informationen beruhte, wenn ein Unternehmen gegen die eingegangenen Verpflichtungen oder die auferlegten Abhilfemaßnahmen verstößt ***oder wenn die Verpflichtungen oder Abhilfemaßnahmen nicht wirksam waren.***

- (34) Da Zusammenschlüsse unter Umständen erhebliche Auswirkungen auf den Binnenmarkt haben können, sollte die Kommission befugt sein, nach der Anmeldung eines geplanten Zusammenschlusses Informationen über drittstaatliche finanzielle Zuwendungen im Rahmen des Zusammenschlusses zu untersuchen. Vor Abschluss der Prüfung durch die Kommission sollte es den beteiligten Unternehmen nicht gestattet sein, den Zusammenschluss zu vollziehen. Diese Untersuchung durch die Kommission sollte demselben Verfahren folgen, dem auch bei einer von der Kommission von Amts wegen eingeleiteten Prüfung einer drittstaatlichen Subvention gefolgt wird; dabei können Anpassungen vorgenommen werden, um den Besonderheiten von Zusammenschlüssen Rechnung zu tragen.
- (35) Es muss ein Gleichgewicht gefunden werden zwischen dem wirksamen Schutz des Binnenmarkts und der Notwendigkeit, den Verwaltungsaufwand für die dieser Verordnung unterliegenden Unternehmen zu begrenzen. Daher sollten nur solche Zusammenschlüsse der Pflicht zur vorherigen Anmeldung unterliegen, bei denen die kombinierten, nach dieser Verordnung geltenden Schwellenwerte, die auf dem in der Union erzielten Umsatz bzw. der Höhe der ***drittstaatlichen finanziellen Zuwendung*** basieren, erreicht werden.

- (36) Wird die Anmelde- bzw. Meldeschwelle nicht erreicht, sollte die Kommission die Anmeldung von möglicherweise subventionierten Zusammenschlüssen, die noch nicht vollzogen wurden, bzw. die Meldung von möglicherweise subventionierten Angeboten vor der Vergabe eines Auftrags verlangen können, wenn sie der Auffassung ist, dass der Zusammenschluss bzw. das Angebot angesichts seiner Auswirkungen in der Union einer vorherigen Prüfung bedarf. Die Kommission sollte ferner die Möglichkeit haben, von Amts wegen bereits vollzogene Zusammenschlüsse oder bereits vergebene öffentliche Aufträge zu prüfen.
- (37) Bei der Prüfung eines Zusammenschlusses sollte sich die Beurteilung des Vorliegens einer Verzerrung auf dem Binnenmarkt auf den betreffenden Zusammenschluss beschränken, und bei der Beurteilung sollten ausschließlich diejenigen drittstaatlichen Subventionen berücksichtigt werden, die in den drei Jahren vor dem Zusammenschluss gewährt wurden.
- (38) *Im Rahmen des Vorabprüfungsmechanismus von Zusammenschlüssen sollten Unternehmen vor der Anmeldung auf Treu und Glauben basierende Konsultationen mit der Kommission beantragen können, um einen Hinweis darauf zu erhalten, ob die Anmeldeschwellen erreicht werden oder nicht.*

- (39) *Wird ein Zusammenschluss nach Artikel 4 der Verordnung (EG) Nr. 139/2004 des Rates⁷ und nach der vorliegenden Verordnung bei der Kommission angemeldet, so sollte sich die Kommission bemühen, den Verwaltungsaufwand im Rahmen der vorliegenden Verordnung für die Anmelder zu begrenzen. Insbesondere sollten Unternehmen die Möglichkeit haben, die im Rahmen eines Verfahrens nach der vorliegenden Verordnung übermittelten spezifischen Informationen anzugeben, die die Kommission auch in Verfahren nach der Verordnung (EG) Nr. 139/2004 verwenden kann.*
- (40) Die Notwendigkeit, den Binnenmarkt verzerrende drittstaatliche Subventionen anzugehen, ist im Bereich der öffentlichen Auftragsvergabe angesichts von deren wirtschaftlicher Bedeutung auf dem Binnenmarkt und der Tatsache, dass öffentliche Aufträge aus Steuergeldern finanziert werden, besonders ausgeprägt. Die Kommission sollte im Falle einer Meldung vor der Vergabe eines Auftrags befugt sein, Informationen über drittstaatliche finanzielle Zuwendungen zu prüfen, die der beteiligte **Wirtschaftsteilnehmer** im Zusammenhang mit einem öffentlichen Vergabeverfahren erhalten hat.

⁷ Verordnung (EG) Nr. 139/2004 des Rates vom 20. Januar 2004 über die Kontrolle von Unternehmenszusammenschlüssen („EG-Fusionskontrollverordnung“) (ABl. L 24 vom 29.1.2004, S. 1).

Vorherige Meldungen sollten ab einem in dieser Verordnung festgelegten Schwellenwert Pflicht sein, damit wirtschaftlich bedeutsame Fälle erfasst werden, gleichzeitig aber der Verwaltungsaufwand so gering wie möglich bleibt und die Teilnahme von KMU an öffentlichen Vergabeverfahren nicht behindert wird. Diese Pflicht zur vorherigen Meldung ab einem bestimmten Schwellenwert sollte auch für Gruppen von Wirtschaftsteilnehmer nach Artikel 26 Absatz 2 der Richtlinie 2014/23/EU des Europäischen Parlaments und des Rates⁸, Artikel 19 Absatz 2 der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates⁹ sowie Artikel 37 Absatz 2 der Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates¹⁰ gelten. **Die Kommission hat auch das Recht, die vorherige Meldung einer drittstaatlichen finanziellen Zuwendung während eines öffentlichen Vergabeverfahrens zu verlangen, auch wenn ihr geschätzter Wert unterhalb der Meldeschwellen liegt. Die Kommission sollte sich bemühen, den Eingriff in die öffentlichen Vergabeverfahren zu begrenzen, indem sie bei der Entscheidung, ob eine solche vorherige Meldung verlangt wird, berücksichtigt, wie nahe der Zeitpunkt der Auftragsvergabe ist.**

⁸ Richtlinie 2014/23/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Konzessionsvergabe (ABl. L 94 vom 28.3.2014, S. 1)

⁹ Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

¹⁰ Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG (ABl. L 94 vom 28.3.2014, S. 243).

- (41) *Das Gleichgewicht zwischen dem Aufbau eines europäischen Marktes für Verteidigungs- und Sicherheitsgüter, der für die Aufrechterhaltung einer technologischen und industriellen Basis der europäischen Verteidigung von wesentlicher Bedeutung ist, und dem Schutz der nationalen Sicherheit der Mitgliedstaaten erfordert eine spezifische Regelung für die Aufträge in den Bereichen Verteidigung und Sicherheit, die unter die Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates¹¹ fallen. Öffentliche Vergabeverfahren für solche Aufträge sollten daher nicht den Meldepflichten nach dieser Verordnung unterliegen. Dennoch sollte es möglich sein, die drittstaatlichen Subventionen im Zusammenhang mit solchen Verträgen von Amts wegen einer Prüfung zu unterziehen. Darüber hinaus sollten öffentliche Aufträge, die unter die Richtlinie 2009/81/EG fallen und die von jener Richtlinie ausgenommen sind oder bei denen die Bedingungen für die Anwendung von Artikel 346 AEUV erfüllt sind, nicht unter die vorliegende Verordnung fallen, wobei beispielsweise beachtet werden sollte, dass die Möglichkeit, von solchen Ausnahmen Gebrauch zu machen, nach der Rechtsprechung des Gerichtshofs der Europäischen Union nur so weit in Anspruch genommen werden sollte, wie dies zur Wahrung der nach den genannten Artikeln als legitim anerkannten Interessen unbedingt erforderlich ist; zudem sollte dazu die Mitteilung der Kommission zu Auslegungsfragen bezüglich der Anwendung des Artikels 296 AEUV auf die Beschaffung von Verteidigungsgütern beachtet werden.*

¹¹ *Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit und zur Änderung der Richtlinien 2004/17/EG und 2004/18/EG (ABl. L 216 vom 20.8.2009, S. 76).*

- (42) *Rahmenvereinbarungen sind eine effiziente Beschaffungsmethode, die von öffentlichen Auftraggebern und Auftraggebern weithin genutzt wird. Die den Einkäufern nach Abschluss der Rahmenvereinbarung gewährte Flexibilität sollte von der vorliegenden Verordnung nicht berührt werden. Daher sollte die in der vorliegenden Verordnung vorgesehene Meldepflicht für drittstaatliche Zuwendungen bei öffentlichen Vergabeverfahren auf das Verfahren beschränkt werden, das dem Abschluss einer Rahmenvereinbarung selbst vorausgeht, und nicht für Aufträge gelten, die auf einer Rahmenvereinbarung beruhen.*
- (43) *Angesichts der Dringlichkeit von Vergabeverfahren, die gemäß Artikel 27 Absatz 3 oder Artikel 28 Absatz 6 der Richtlinie 2014/24/EU oder Artikel 45 Absatz 3 der Richtlinie 2014/25/EU durchgeführt werden, sollte sich die Kommission nach besten Kräften bemühen, solche Verfahren im Laufe einer Vorprüfung und einer eingehenden Prüfung vorrangig zu behandeln, um so bald wie möglich zu einem guten Ergebnis zu gelangen. Dies sollte entsprechend für ähnliche Verfahren gelten, die gemäß der Richtlinie 2014/23/EU durchgeführt werden.*

- (44) *Aufgrund der Besonderheiten von mehrstufigen Verfahren bei der Vergabe öffentlicher Aufträge sollte die Kommission eine Vorprüfung anhand der einschlägigen Informationen einleiten, die in einer Meldung bei Einreichung eines Antrags auf Teilnahme an einem Verfahren verfügbar sind. Um die Vollständigkeit der Informationen und die rasche Durchführung der Untersuchung zu gewährleisten, sollte zusammen mit dem endgültigen Angebot eine aktualisierte Meldung übermittelt werden. Die Kommission sollte außerdem das Recht haben, vor der Einreichung des endgültigen Angebots zusätzliche Informationen anzufordern.*
- (45) *Diese Verordnung regelt nicht den Zugang von Wirtschaftsteilnehmern aus Drittländern zum Markt der Union für öffentliche Aufträge. Diese Angelegenheit fällt unter das einschlägige Unionsrecht und völkerrechtliche Übereinkünfte.*
- (46) Wird im Zusammenhang mit einem öffentlichen Vergabeverfahren eine drittstaatliche finanzielle Zuwendung gemeldet, sollte die Beurteilung auf dieses Vergabeverfahren beschränkt bleiben.
- (47) *Die Kommission sollte gegebenenfalls nach Wegen suchen, um die Nutzung elektronischer Kommunikationsmittel sicherzustellen, um die Erfüllung der Verpflichtungen im Zusammenhang mit öffentlichen Vergabeverfahren im Rahmen dieser Verordnung zu erleichtern.*

- (48) Auch sollte gewährleistet werden, dass die für die öffentliche Auftragsvergabe geltenden Grundsätze, **insbesondere** Verhältnismäßigkeit, Nichtdiskriminierung, Gleichbehandlung, Transparenz **und Wettbewerb**, in Bezug auf alle an dem öffentlichen Vergabeverfahren beteiligten **Wirtschaftsteilnehmer** eingehalten werden, unabhängig von gemäß dieser Verordnung eingeleiteten und laufenden Prüfverfahren. **Diese Verordnung lässt die Richtlinien 2014/23/EU, 2014/24/EU und 2014/25/EU im Hinblick auf die geltenden Verpflichtungen in den Bereichen Umwelt-, Sozial- und Arbeitsrecht unberührt.**
- (49) **Öffentliche Auftraggeber oder Auftraggeber können beschließen, einen Auftrag in Form mehrerer Lose zu vergeben, gemäß insbesondere Artikel 46 der Richtlinie 2014/24/EU und Artikel 65 der Richtlinie 2014/25/EU und unter Beachtung des Verbots der künstlichen Aufspaltung. Drittstaatliche finanzielle Zuwendungen an Bieter, die ein Angebot für Lose einreichen, deren Wert über einem anwendbaren Schwellenwert liegt, sollten gemeldet werden.**
- (50) **Diese Verordnung sollte die Möglichkeit der Wirtschaftsteilnehmer unberührt lassen, die Kapazitäten anderer Unternehmen gemäß den Richtlinien 2014/24/EU, 2014/25/EU und 2014/23/EU in Anspruch zu nehmen.**

- (51) *Diese Verordnung sollte die Möglichkeit von öffentlichen Auftraggebern und von Auftraggebern unberührt lassen, die Wirtschaftsteilnehmer aufzufordern, die einschlägigen Informationen oder Unterlagen gemäß der Richtlinie 2014/24/EU, der Richtlinie 2014/25/EU oder der Richtlinie 2014/23/EU oder gemäß den nationalen Rechtsvorschriften, mit denen sie umgesetzt werden, zu ergänzen, zu erläutern oder zu vervollständigen, sofern diese Aufforderungen in vollem Einklang mit den Grundsätzen der Gleichbehandlung und der Transparenz stehen.*
- (52) *Öffentliche Einkäufer neigen stark dazu, die Einkäufe zu zentralisieren, um Skaleneffekte und Effizienzgewinne zu erzielen. Diese zentralen Beschaffungsstellen sind öffentliche Auftraggeber oder Auftraggeber im Sinne der Richtlinien 2009/81/EG, 2014/24/EU und 2014/25/EU. Es ist daher angemessen, dass die Kommission in der Lage sein sollte, drittstaatliche Subventionen im Zusammenhang mit Aufträgen, die von diesen öffentlichen oder anderen Auftraggebern vergeben werden, zu prüfen.*

- (53) Drittstaatliche Subventionen, die einen **Wirtschaftsteilnehmer** in die Lage versetzen, ein in Bezug auf die betreffenden Bauleistungen, Lieferungen oder Dienstleistungen ungerechtfertigt günstiges Angebot abzugeben, sollten als tatsächliche oder potenzielle Ursache für eine Wettbewerbsverzerrung im Rahmen eines öffentlichen Vergabeverfahrens angesehen werden. Solche Verzerrungen sollten folglich auf Grundlage **einer** nicht erschöpfenden Liste von Indikatoren beurteilt werden. Anhand der Indikatoren sollte festgestellt werden können, wie eine drittstaatliche Subvention den Wettbewerb verzerrt, indem sie die Wettbewerbsposition eines Unternehmens verbessert und es in die Lage versetzt, ein ungerechtfertigt günstiges Angebot abzugeben. **Wirtschaftsteilnehmern** sollte Gelegenheit gegeben werden darzulegen, dass das Angebot nicht ungerechtfertigt günstig ist, u. a. durch Berufung auf die Elemente, die in Artikel 69 Absatz 2 der Richtlinie 2014/24/EU **oder in Artikel 84 Absatz 2 der Richtlinie 2014/25/EU, die ungewöhnlich niedrige Angebote zum Gegenstand haben**, genannt werden. Das Zuschlagsverbot sollte nur dann gelten, wenn der günstige Charakter des Angebots, das aufgrund drittstaatlicher Subventionen abgegeben werden konnte, nicht **durch andere Faktoren** gerechtfertigt werden kann, wenn der Bieter den Zuschlag erhalten würde und wenn das das Angebot einreichende Unternehmen keine Verpflichtungszusagen vorgelegt hat, die als angemessen und hinreichend angesehen werden, um die Verzerrung vollständig und wirksam zu beseitigen.

Daher betrifft das Zuschlagsverbot das spezifische Verfahren, in dem das ungerechtfertigt günstige Angebot abgegeben wurde. Die Feststellung der Kommission, dass ein Wirtschaftsteilnehmer von einer den Binnenmarkt verzerrenden drittstaatlichen Subvention profitiert hat, die es ihm ermöglichte, ein ungerechtfertigt günstiges Angebot einzureichen, sollte daher nicht als ein Element angesehen werden, das zu einem Ausschluss aufgrund der fakultativen Ausschlussgründe gemäß Artikel 38 Absatz 7 der Richtlinie 2014/23/EU, Artikel 57 Absatz 4 der Richtlinie 2014/24/EU oder Artikel 80 der Richtlinie 2014/25/EU im Rahmen desselben oder eines anderen öffentlichen Vergabeverfahrens im Einklang mit diesen Richtlinien führt.

- (54) *Ein ungerechtfertigt günstiges Angebot kann sich auch aus drittstaatlichen Subventionen ergeben, die einem Unterauftragnehmer oder Lieferanten gewährt werden, weil es Auswirkungen auf den Wettbewerb in Bezug auf das bei einem öffentlichen Auftraggeber oder Auftraggeber eingereichte Angebot hat. Um den Verwaltungsaufwand zu begrenzen, sollten jedoch nur die Hauptunterauftragnehmer oder Hauptlieferanten, d. h. diejenigen, deren Produkte oder Dienstleistungen wesentliche Elemente des Auftrags betreffen oder einen bestimmten Prozentsatz des Auftragswerts überschreiten, drittstaatliche finanzielle Zuwendungen melden. Elemente des Auftrags können insbesondere aufgrund ihrer besonderen Bedeutung für die Qualität des Angebots, einschließlich des spezifischen Know-hows, der Technologie, des Fachpersonals, der Patente oder ähnlicher Vorteile, die dem Unterauftragnehmer oder Lieferanten zur Verfügung stehen, als wesentliche Elemente eingestuft werden, insbesondere wenn diese Elemente bei einem öffentlichen Vergabeverfahren für die Erfüllung des größten Teils von mindestens einem der Auswahlkriterien ausschlaggebend sind.*

Um eine stabile Tatsachengrundlage für die Prüfung zu gewährleisten, sollten bei der Vorprüfung die Hauptunterauftragnehmer und die Hauptlieferanten berücksichtigt werden, die zum Zeitpunkt der Einreichung der vollständigen Meldung oder Erklärung oder im Falle mehrstufiger Verfahren zum Zeitpunkt der aktualisierten Meldung oder aktualisierten Erklärung bereits bekannt sind. Diese Verordnung sollte die Möglichkeit der Wirtschaftsteilnehmer unberührt lassen, bei der Ausführung ihrer Verträge neue Unterauftragnehmer einzusetzen. Folglich sollte der Wechsel von Unterauftragnehmern und Lieferanten nach Einreichung der vollständigen Meldung oder Erklärung bzw. der aktualisierten Meldung oder Erklärung oder während der Ausführung eines Vertrags keine zusätzlichen Meldepflichten nach sich ziehen; die Kommission sollte jedoch von Amts wegen eine Prüfung einleiten können, wenn ihr Informationen, auch seitens eines Mitgliedstaats, einer natürlichen oder juristischen Person oder einer Vereinigung, vorliegen, dass diese Unterauftragnehmer und Lieferanten möglicherweise drittstaatliche Subventionen erhalten haben könnten.

- (55) *Im Einklang mit den Richtlinien über die öffentliche Auftragsvergabe sollte die Bestimmung des aus der Sicht des öffentlichen Auftraggebers oder des Auftraggebers wirtschaftlich günstigsten Angebots anhand einer Bewertung auf der Grundlage des Preises oder der Kosten, mittels eines Kosten-Wirksamkeits-Ansatzes, wie der Lebenszykluskostenrechnung, erfolgen und kann das beste Preis-Leistungs-Verhältnis beinhalten, das auf der Grundlage von Kriterien – unter Einbeziehung qualitativer, umweltbezogener oder sozialer Aspekte – bewertet wird, die mit dem Auftragsgegenstand des betreffenden Auftrags in Verbindung stehen.*
- (56) *Im Rahmen von Rechtsbehelfen im Zusammenhang mit der Anwendung dieser Verordnung, insbesondere was die öffentliche Vergabeverfahren betrifft, kann bzw. – im in Artikel 267 AEUV vorgesehenen Fall – muss ein einzelstaatliches Gericht im Sinne des Artikels 267 AEUV, das eine Entscheidung über die Frage als erforderlich erachtet, um sein Urteil zu fällen, den Gerichtshof um Vorabentscheidung über die Auslegung des Unionsrechts, einschließlich dieser Verordnung, ersuchen. Jedoch darf nach ständiger Rechtsprechung des Gerichtshofs dieses einzelstaatliche Gericht den Gerichtshof nicht auf Antrag eines betroffenen Wirtschaftsteilnehmers, der die Gelegenheit hatte, eine Nichtigkeitsklage gegen diesen Beschluss zu erheben, mit einer Frage der Gültigkeit des Beschlusses der Kommission befassen, insbesondere wenn er unmittelbar und individuell von diesem Beschluss betroffen war, diese Gelegenheit jedoch nicht innerhalb der Frist gemäß Artikel 263 AEUV genutzt hatte.*

- (57) Angesichts der Merkmale des Vorabprüfungsmechanismus für Zusammenschlüsse und öffentliche Vergabeverfahren und mit Blick auf die für derartige Transaktionen erforderliche Rechtssicherheit sollten Zusammenschlüsse und öffentliche Vergabeverfahren, die nach den jeweils geltenden Verfahren angemeldet bzw. gemeldet und beurteilt wurden, von der Kommission nicht von Amts wegen erneut geprüft werden. Finanzielle Zuwendungen, über die die Kommission im Wege des Anmelde- bzw. Meldeverfahrens informiert wurde, können jedoch auch außerhalb dieses Prüfverfahrens für Zusammenschlüsse oder öffentliche Vergabeverfahren relevant sein.
- (58) ***Die Mitgliedstaaten sollten bei der Anwendung dieser Verordnung wirksam mit der Kommission zusammenarbeiten. Zur Erleichterung dieser Zusammenarbeit sollte die Kommission in der Lage sein, ein Verfahren für die Zusammenarbeit einzurichten.***
- (59) Um Informationen über **drittstaatliche** Subventionen **■** einzuholen, sollte die Kommission über die Möglichkeit verfügen, Untersuchungen für bestimmte Wirtschaftszweige, bestimmte Arten von Wirtschaftstätigkeiten oder in Bezug auf die Nutzung bestimmter Instrumente für drittstaatliche Subventionen einzuleiten. ***Die Kommission sollte die im Rahmen solcher Marktuntersuchungen erlangten Informationen verwenden können, um im Rahmen von Verfahren nach dieser Verordnung bestimmte Transaktionen zu überprüfen.***

- (60) *Wenn die Kommission das Vorliegen wiederholter den Binnenmarkt verzerrender drittstaatlicher Subventionen vermutet oder wenn bei mehreren Durchsetzungsmaßnahmen im Rahmen dieser Verordnung den Binnenmarkt verzerrende drittstaatliche Subventionen desselben Drittstaats festgestellt werden, sollte die Kommission die Möglichkeit haben, einen Dialog mit dem betreffenden Drittstaat aufzunehmen, um Optionen zu sondieren, die auf die Einstellung oder Änderung der den Binnenmarkt verzerrenden drittstaatlichen Subventionen im Hinblick darauf abzielen, deren verzerrende Auswirkungen auf den Binnenmarkt zu beseitigen. Ist in einem bilateralen Abkommen zwischen der Union und einem Drittstaat ein Konsultationsverfahren für den Binnenmarkt verzerrende drittstaatliche Subventionen vorgesehen, die in den Anwendungsbereich dieser Verordnung fallen, so könnte dieses Verfahren genutzt werden, um den Dialog mit Drittstaaten zu erleichtern. Der Dialog mit dem Drittstaat sollte die Kommission nicht daran hindern, Prüfungen nach dieser Verordnung einzuleiten oder laufende Prüfungen fortzusetzen. Die Kommission sollte das Europäische Parlament und den Rat regelmäßig über einschlägige Entwicklungen informieren.*
- (61) *Aus Gründen der Rechtssicherheit sollte der Zeitraum, in dem die Kommission eine drittstaatliche Subvention prüfen darf, auf zehn Jahre ab dem Tag der Gewährung dieser drittstaatlichen Subvention beschränkt sein.*

- (62) Aus denselben Gründen sollten Verjährungsfristen für die Verhängung und die Vollstreckung von Geldbußen oder Zwangsgeldern vorgesehen werden.
- (63) Im Interesse von Transparenz und Rechtssicherheit ist es angezeigt, **dass die Kommission** alle von **ihr** gemäß der vorliegenden Verordnung erlassenen Beschlüsse entweder im vollen Wortlaut oder als Zusammenfassung veröffentlicht **oder bekannt macht**.
- (64) Die Kommission sollte bei der Veröffentlichung ihrer Beschlüsse die Vorschriften über das Berufsgeheimnis nach Artikel 339 AEUV befolgen und insbesondere alle vertraulichen Informationen **und** Geschäftsgeheimnisse **■** schützen. **Die Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates¹² und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates¹³ erfolgen, je nachdem, welche Verordnung für die entsprechende Verarbeitung gilt.**

¹² 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).

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).

- (65) Für Fälle, in denen die von dem Unternehmen als vertraulich oder als Geschäftsgeheimnis gekennzeichneten Informationen nicht unter das Berufsgeheimnis zu fallen scheinen, sollte es ein Verfahren geben, nach dem die Kommission das Recht hat, zu entscheiden, inwieweit solche Informationen offengelegt werden können. Wenn die Kommission einen Antrag auf vertrauliche Behandlung zurückweist, sollte sie eine Frist angeben, nach deren Ablauf die Informationen offengelegt werden, sodass der Antragsteller jeden ihm zur Verfügung stehenden gerichtlichen Schutz einschließlich einer einstweiligen **Maßnahme** in Anspruch nehmen kann.
- (66) Die **Unternehmen, die Gegenstand einer Prüfung** nach dieser Verordnung **sind**, sollten Gelegenheit **erhalten, zu den Gründen, aus denen die Kommission einen Beschluss zu erlassen beabsichtigt, Stellung zu nehmen, und daher Recht auf Einsicht in die Akten haben**. Die Verteidigungsrechte der **Unternehmen, die Gegenstand einer Prüfung sind**, sind zu wahren, doch müssen auch Geschäftsgeheimnisse geschützt werden.

- (67) *Wenn der Bereitsteller der Informationen zustimmt, sollte die Kommission die im Rahmen dieser Verordnung erlangten Informationen auch bei der Anwendung anderer Rechtsakte der Union verwenden können.*
- (68) *Die Mitgliedstaaten und die Kommission sollten alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass Verschlusssachen geschützt werden, insbesondere gemäß dem Übereinkommen zwischen den im Rat vereinigten Mitgliedstaaten der Europäischen Union über den Schutz von Verschlusssachen, die im Interesse der Europäischen Union ausgetauscht werden¹⁴, dem Beschluss (EU, Euratom) 2015/443 der Kommission¹⁵ und dem Beschluss (EU, Euratom) 2015/444 der Kommission¹⁶.*
- (69) Die Durchführung dieser Verordnung durch die Union sollte mit dem Unionsrecht und dem WTO-Abkommen sowie mit den Zusagen im Rahmen anderer Handels- und Investitionsübereinkommen, zu deren Vertragsparteien die Union oder die Mitgliedstaaten zählen, im Einklang stehen. ***Diese Verordnung sollte die Bemühungen der Union zur Verbesserung der multilateralen Vorschriften für die Bewältigung verzerrender Subventionen ergänzen.***

¹⁴ Übereinkommen zwischen den im Rat vereinigten Mitgliedstaaten der Europäischen Union über den Schutz von Verschlusssachen, die im Interesse der Europäischen Union ausgetauscht werden (ABl. C 202 vom 8.7.2011, S. 13).

¹⁵ Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

¹⁶ Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

- (70) Einschränkungen der **Freiheiten nach** Artikel 34, 49, 56 und 63 AEUV können dadurch gerechtfertigt sein, dass unfaire Wettbewerbsbedingungen vermieden werden müssen, sofern solche Einschränkungen – wie andere Einschränkungen der Grundfreiheiten – mit den allgemeinen Grundsätzen des Unionsrechts, wie Verhältnismäßigkeit und Rechtssicherheit, sowie mit den Grundrechten im Einklang stehen.
- (71) **Es besteht die Möglichkeit, dass** es bei der Durchführung dieser Verordnung ■ zu Überschneidungen mit sektorspezifischen Vorschriften kommt, vor allem in den Bereichen Seeschifffahrt und Luftverkehr. Daher muss das Verhältnis dieser Verordnung zu sektorspezifischen Instrumenten, in denen es um drittstaatliche Subventionen geht, so insbesondere zu der Verordnung (EWG) Nr. 4057/86 des Rates¹⁷, der Verordnung (EU) 2016/1035 des Europäischen Parlaments und des Rates¹⁸ und der Verordnung (EU) 2019/712 des Europäischen Parlaments und des Rates¹⁹, geklärt werden.
-

¹⁷ Verordnung (EWG) Nr. 4057/86 des Rates vom 22. Dezember 1986 über unlautere Preisbildungspraktiken in der Seeschifffahrt (ABl. L 378 vom 31.12.1986, S. 14).

¹⁸ Verordnung (EU) 2016/1035 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz gegen schädigende Preisgestaltung im Schiffbau (ABl. L 176 vom 30.6.2016, S. 1).

¹⁹ Verordnung (EU) 2019/712 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Sicherstellung des Wettbewerbs im Luftverkehr und zur Aufhebung der Verordnung (EG) Nr. 868/2004 (ABl. L 123 vom 10.5.2019, S. 4).

- (72) *Alle auf der Grundlage dieser Verordnung erlassenen Rechtsakte der Kommission unterliegen im Einklang mit Artikel 263 AEUV der Überwachung durch den Gerichtshof. Gemäß Artikel 261 AEUV sollte der Gerichtshof die Befugnis zur unbeschränkten Ermessensnachprüfung im Hinblick auf die Beschlüsse erhalten, mit denen die Kommission Geldbußen oder Zwangsgelder auferlegt.*
- (73) *Um die Vorhersehbarkeit dieser Verordnung zu fördern, sollte die Kommission Leitlinien in Bezug auf Folgendes veröffentlichen und regelmäßig aktualisieren: die Kriterien für die Feststellung des Vorliegens einer durch eine drittstaatliche Subvention verursachten Verzerrung auf dem Binnenmarkt, die Anwendung der Abwägungsprüfung, die Anwendung ihrer Befugnis, die vorherige Anmeldung aller Zusammenschlüsse bzw. Meldung aller drittstaatlichen finanziellen Zuwendungen an einen Wirtschaftsteilnehmer im Rahmen eines öffentlichen Vergabeverfahrens zu verlangen, und die Beurteilung einer Verzerrung in einem öffentlichen Vergabeverfahren. Bei der Herausgabe dieser Leitlinien sollte die Kommission angemessene Konsultationen mit den Interessenträgern und Mitgliedstaaten durchführen. Um die Durchführung dieser Verordnung in der Anfangsphase ihrer Anwendung zu erleichtern, sollte sich die Kommission bemühen, vor der Veröffentlichung der Leitlinien Erläuterungen zur Anwendung dieser Bestimmungen zu veröffentlichen.*

- (74) Um für einheitliche Bedingungen für die Durchführung dieser Verordnung zu sorgen, sollten der Kommission nach Artikel 291 AEUV Durchführungsbefugnisse übertragen werden. *Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates²⁰ ausgeübt werden und Folgendes betreffen: Beschlüsse zur Einstellung der eingehenden Prüfungen, die Auferlegung einstweiliger Maßnahmen, Beschlüsse über Zusammenschlüsse, die unter Verstoß gegen die Anmeldepflicht oder unter Verstoß gegen einen Verpflichtungsbeschluss, einen Beschluss zur Untersagung eines Zusammenschlusses oder einen Beschluss zur Untersagung der Zuschlagserteilung bei einem öffentlichen Vergabeverfahren vollzogen wurden, den Widerruf bestimmter Beschlüsse sowie Durchführungsbefugnisse in Bezug auf die Form-, Inhalts- und Verfahrenseinzelheiten und die diesbezüglichen Aspekte im Zusammenhang mit der Vorprüfung und der eingehenden Prüfung.*
- (75) *Die Kommission sollte die Möglichkeit haben, ein vereinfachtes Verfahren einzuführen, nach dem sie bestimmte Zusammenschlüsse oder öffentliche Vergabeverfahren behandelt, die offenbar mit geringerer Wahrscheinlichkeit zu Verzerrungen auf dem Binnenmarkt durch drittstaatliche Subventionen führen.*

²⁰ 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).

- (76) Um auch langfristig **gleiche** Wettbewerbsbedingungen auf dem Binnenmarkt zu gewährleisten und sowohl Fälle, für die eine Anmeldung bzw. Meldung erfolgt ist, als auch von Amts wegen geprüfte Fälle angemessen abzudecken **und gleichzeitig einen übermäßigen Verwaltungsaufwand zu begrenzen**, sollte der Kommission nach Artikel 290 AEUV die Befugnis zum Erlass von Rechtsakten übertragen werden in Bezug auf die Änderung der Schwellenwerte für die Anmeldung von Zusammenschlüssen bzw. die Meldung bei öffentlichen Vergabeverfahren ■ sowie in Bezug auf die **Verkürzung** der Fristen für die Vorprüfung und die eingehende Prüfung angemeldeter Zusammenschlüsse bzw. gemeldeter finanzieller Zuwendungen im Zusammenhang mit einem öffentlichen Vergabeverfahren. **Unbeschadet der Möglichkeit, die Anmeldeschwellen für Zusammenschlüsse bzw. die Meldeschwellen für öffentliche Aufträge im Wege eines Gesetzgebungsvorschlags zu ändern, einschließlich im Zusammenhang mit der in dieser Verordnung vorgesehenen Überprüfung, können diese Schwellenwerte während des Zeitraums der Befugnisübertragung nach dieser Verordnung einmal im Wege eines delegierten Rechtsakts geändert werden.** Was finanzielle Zuwendungen im Zusammenhang mit einem öffentlichen Vergabeverfahren angeht, so sollte die Befugnis zum Erlass eines solchen Rechtsaktes in einer Weise ausgeübt werden, die auch den Interessen von KMU Rechnung trägt.

Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer vorbereitenden Arbeiten 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 Rechtsetzung²¹ 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.

- (77) Gilt für einen Zusammenschluss die Anmeldepflicht nach dieser Verordnung, sollten die finanziellen Zuwendungen, die gleich welchem der an dem Zusammenschluss beteiligten Unternehmen in den drei Jahren vor Geltungsbeginn dieser Verordnung gewährt wurden, in den Anwendungsbereich dieser Verordnung fallen. Im Zusammenhang mit einem öffentlichen Vergabeverfahren sollte diese Verordnung auch für finanzielle Zuwendungen gelten, die einem **Wirtschaftsteilnehmer** in den drei Jahren vor Geltungsbeginn dieser Verordnung gewährt wurden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

²¹ ABl. L 123 vom 12.5.2016, S. 1.

Kapitel 1
Allgemeine Bestimmungen

Artikel 1

Gegenstand und Anwendungsbereich

- (1) ***Zweck dieser Verordnung ist es, zum reibungslosen Funktionieren des Binnenmarkts beizutragen, indem ein harmonisierter Rahmen geschaffen wird, mit dem die Verzerrungen, die direkt oder indirekt durch drittstaatliche Subventionen verursacht werden, angegangen werden, um für gleiche Wettbewerbsbedingungen zu sorgen.*** Mit dieser Verordnung werden Regeln und Verfahren für die Prüfung drittstaatlicher Subventionen, die den Binnenmarkt verzerren, und für die Beseitigung solcher Verzerrungen festgelegt. Solche Verzerrungen können bei jeder wirtschaftlichen Tätigkeit auftreten, vor allem bei Zusammenschlüssen und öffentlichen Vergabeverfahren.
- (2) Diese Verordnung betrifft drittstaatliche Subventionen, die Unternehmen – ***einschließlich öffentlicher Unternehmen, die der direkten oder indirekten Kontrolle des Staates unterliegen*** – gewährt werden, welche eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausüben. ***Unter anderem*** gelten Unternehmen, die die Kontrolle über ein in der Union niedergelassenes Unternehmen erwerben oder mit einem solchen Unternehmen ***fusionieren***, und Unternehmen, die an einem öffentlichen Vergabeverfahren ***in der Union*** teilnehmen, als Unternehmen, die eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausüben.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. **„Unternehmen“, im Bereich öffentlicher Vergabeverfahren, Wirtschaftsteilnehmer im Sinne des Artikels 1 Nummer 14 der Richtlinie 2009/81/EG, des Artikels 5 Nummer 2 der Richtlinie 2014/23/EU, des Artikels 2 Nummer 10 der Richtlinie 2014/24/EU und des Artikels 2 Nummer 6 der Richtlinie 2014/25/EU;**
2. **„Auftrag“, im Bereich öffentlicher Vergabeverfahren und sofern nichts anderes bestimmt ist, einen „öffentlichen Auftrag“ im Sinne des Artikels 2 Nummer 5 der Richtlinie 2014/24/EU, einen „Auftrag“ im Sinne des Artikels 1 Nummer 2 der Richtlinie 2009/81/EG und „Liefer-, Bauleistungs- und Dienstleistungsauftrag“ im Sinne des Artikels 2 Nummer 1 der Richtlinie 2014/25/EU sowie eine „Konzession“ im Sinne des Artikels 5 Nummer 1 der Richtlinie 2014/23/EU;**
3. **„öffentliches Vergabeverfahren“**
 - a) **alle Arten von Vergabeverfahren nach der Richtlinie 2014/24/EU für den Abschluss eines öffentlichen Auftrags oder nach der Richtlinie 2014/25/EU für den Abschluss eines Liefer-, Bauleistungs- und Dienstleistungsauftrags** ,

- b) ein Verfahren zur Vergabe von Bau- oder Dienstleistungskonzessionen nach der Richtlinie 2014/23/EU ,
 - c) **Verfahren zur Vergabe von Aufträgen, die unter die Richtlinie 2009/81/EG fallen, sofern sie nicht von den Mitgliedstaaten auf der Grundlage von Artikel 346 AEUV ausgenommen wurden,**
 - d) Verfahren zur Vergabe von Aufträgen nach Artikel 10 Absatz 4 Buchstabe a der Richtlinie 2014/23/EU, Artikel 9 Absatz 1 Buchstabe a der Richtlinie 2014/24/EU oder Artikel 20 Absatz 1 Buchstabe a der Richtlinie 2014/25/EU;
4. „öffentlicher Auftraggeber“ im Bereich öffentlicher Vergabeverfahren einen öffentlichen Auftraggeber im Sinne des Artikels 6 der Richtlinie 2014/23/EU, Artikels 2 Absatz 1 der Richtlinie 2014/24/EU und Artikels 3 der Richtlinie 2014/25/EU
5. „Auftraggeber“ im Bereich öffentlicher Vergabeverfahren einen Auftraggeber im Sinne des Artikels 7 der Richtlinie 2014/23/EU und Artikels 4 der Richtlinie 2014/25/EU.
6. **„ein Verfahren mit mehreren Phasen“ ein öffentliches Vergabeverfahren im Sinne der Artikel 28 bis 32 der Richtlinie 2014/24/EU und der Artikel 46 bis 52 der Richtlinie 2014/25/EU – entweder als nichtoffenes Verfahren, Verhandlungsverfahren, Verhandlungsverfahren ohne vorherige Bekanntmachung, wettbewerblicher Dialog oder Innovationspartnerschaften – oder als ein gleichartiges Verfahren im Sinne der Richtlinie 2014/23/EU.**

Artikel 3

Vorliegen einer drittstaatlichen Subvention

- (1) Für die Zwecke dieser Verordnung liegt eine drittstaatliche Subvention vor, wenn ein Drittstaat **direkt oder indirekt** eine finanzielle Zuwendung gewährt, die einem Unternehmen, das eine wirtschaftliche Tätigkeit auf dem Binnenmarkt ausübt, einen Vorteil verschafft und die rechtlich oder faktisch auf ein einzelnes Unternehmen oder einen einzelnen Wirtschaftszweig oder mehrere Unternehmen oder Wirtschaftszweige beschränkt ist.

(2) Für die Zwecke dieser Verordnung umfasst der Begriff „finanzielle Zuwendung“ ***unter anderem***

- a) den Transfer von Geldern oder Verbindlichkeiten, wie etwa Kapitalzuführungen, Zuschüsse, Kredite, Kreditgarantien, Steueranreize, Ausgleich von Betriebsverlusten, den Ausgleich für von Behörden auferlegte finanzielle Belastungen, Schuldenerlass, Schuldenswaps oder eine Umschuldung,
- b) den Verzicht auf ansonsten fällige Einnahmen, ***wie etwa Steuerbefreiungen oder die Gewährung besonderer oder ausschließlicher Rechte an ein Unternehmen ohne angemessene Vergütung,*** oder
- c) die Bereitstellung oder den Erwerb von Waren oder Dienstleistungen.

Eine finanzielle Zuwendung eines Drittstaats umfasst eine finanzielle Zuwendung folgender Stellen:

- a) der Zentralregierung bzw. Behörden aller anderen Ebenen,

- b) **einer** drittstaatlichen öffentlichen **Einrichtung**, deren Handlungen – unter anderem angesichts der Merkmale der betreffenden Einrichtung, des rechtlichen und wirtschaftlichen Umfelds in dem Land, in dem die Einrichtung tätig ist, einschließlich der Rolle der Regierung in der Wirtschaft – dem Drittstaat zugerechnet werden können, oder
- c) einer privaten Einrichtung, deren Handlungen angesichts aller relevanten Umstände dem Drittstaat zugerechnet werden können.

Artikel 4

Verzerrungen auf dem Binnenmarkt

- (1) Eine Verzerrung auf dem Binnenmarkt liegt vor, wenn eine drittstaatliche Subvention geeignet ist, die Wettbewerbsposition **eines** Unternehmens auf dem Binnenmarkt zu verbessern, und die drittstaatliche Subvention dadurch den Wettbewerb auf dem Binnenmarkt tatsächlich oder potenziell beeinträchtigt. Eine Verzerrung auf dem Binnenmarkt wird anhand von Indikatoren ermittelt, **zu denen insbesondere das Folgende gehören kann:**

- a) die Höhe der drittstaatlichen Subvention,

- b) die Art der drittstaatlichen Subvention,
 - c) die Situation des Unternehmens, **einschließlich seiner Größe**, und der betreffenden Märkte **oder Sektoren**,
 - d) der Umfang **und die Entwicklung** der Wirtschaftstätigkeit des **■** Unternehmens auf dem Binnenmarkt,
 - e) der Zweck der drittstaatlichen Subvention, die mit ihr verbundenen Voraussetzungen sowie ihre Verwendung auf dem Binnenmarkt.
- (2) Wenn der Gesamtbetrag einer drittstaatlichen Subvention **für ein Unternehmen 4 Mio. EUR** in einem Zeitraum von drei aufeinanderfolgenden Geschäftsjahren nicht **übersteigt, so gilt es als unwahrscheinlich, dass** diese drittstaatliche Subvention zu Verzerrungen auf dem Binnenmarkt führt.

- (3) *Wenn der Gesamtbetrag einer drittstaatlichen Subvention für ein Unternehmen den Betrag einer De-minimis-Beihilfe im Sinne von Artikel 3 Absatz 2 Unterabsatz 1 der Verordnung (EU) Nr. 1407/2013 pro Drittstaat in einem Zeitraum von drei aufeinanderfolgenden Geschäftsjahren nicht übersteigt, so gilt diese drittstaatliche Subvention nicht als den Binnenmarkt verzerrend.*
- (4) *Eine drittstaatliche Subvention kann als nicht den Binnenmarkt verzerrend gelten, sofern sie darauf abzielt, einen von Naturkatastrophen oder außergewöhnlichen Ereignissen verursachten Schaden zu beheben.*

Artikel 5

Kategorien drittstaatlicher Subventionen, bei denen **mit größter Wahrscheinlichkeit** eine Verzerrung des Binnenmarkts stattfindet

- (1) Bei drittstaatlichen Subventionen ist die Wahrscheinlichkeit einer Verzerrung auf dem Binnenmarkt am größten, wenn sie unter eine der folgenden Kategorien fallen:
- a) drittstaatliche Subventionen, die einem notleidenden Unternehmen gewährt werden, d.h. einem Unternehmen, das seine Geschäftstätigkeit kurz- oder mittelfristig wahrscheinlich einstellen wird, wenn es keine Subvention erhält, es sei denn, es liegt ein Umstrukturierungsplan vor, der geeignet ist, die langfristige Rentabilität des Unternehmens wiederherzustellen und der einen erheblichen Eigenbeitrag des Unternehmens vorsieht,

- b) drittstaatliche Subventionen in Form einer unbegrenzten Garantie für Schulden oder Verbindlichkeiten des Unternehmens, d.h. einer Garantie, deren Höhe oder Laufzeit nicht begrenzt ist,
- c) *Ausführfinanzierungsmaßnahmen, die nicht im Einklang mit dem OECD-Übereinkommen über öffentlich unterstützte Exportkredite stehen,*
- d) drittstaatliche Subventionen, die einen Zusammenschluss unmittelbar erleichtern,
- e) *drittstaatliche Subventionen, die ein Unternehmen in die Lage versetzen, im Rahmen eines Vergabeverfahrens ein ungerechtfertigt günstiges Angebot abzugeben, auf dessen Grundlage das Unternehmen den Zuschlag für den entsprechenden Auftrag erhalten könnte.*

I

- (2) *Unternehmen, die Gegenstand einer Prüfung sind, wird die Möglichkeit eingeräumt, relevante Informationen darüber vorzulegen, dass eine drittstaatliche Subvention, die unter eine der in Absatz 1 bestimmten Kategorien fällt, den Binnenmarkt unter den besonderen Umständen des jeweiligen Falls nicht verzerrt.*

Artikel 6

Abwägungsprüfung

- (1) Die Kommission **kann** die negativen Auswirkungen einer drittstaatlichen Subvention in Form der Verzerrung auf dem Binnenmarkt **gemäß den Artikeln 4 und 5 auf der Grundlage der erhaltenen Informationen** gegen die positiven Auswirkungen der Subvention auf die Entwicklung der betreffenden **subventionierten** wirtschaftlichen Tätigkeit **auf dem Binnenmarkt** abwägen **und prüft dabei auch andere positive Auswirkungen der drittstaatlichen Subvention, wie etwa die umfassenderen positiven Auswirkungen in Bezug auf die einschlägigen politischen Ziele, insbesondere die der Union.**
- (2) Bei ihrer Entscheidung, ob sie Abhilfemaßnahmen auferlegt oder angebotene Verpflichtungszusagen annimmt, berücksichtigt die Kommission die Abwägung gemäß Absatz 1 sowie auch Art und Umfang der Abhilfemaßnahmen bzw. Verpflichtungszusagen.

Artikel 7

Verpflichtungszusagen und Abhilfemaßnahmen

- (1) ***Die Kommission kann Abhilfemaßnahmen auferlegen, um die tatsächlich oder potenziell durch eine drittstaatliche Subvention verursachte Verzerrung auf dem Binnenmarkt zu beseitigen, es sei denn, sie hat gemäß Absatz 2 Verpflichtungszusagen des Unternehmens, das Gegenstand der Prüfung ist, angenommen.***
- (2) ***Die Kommission kann Verpflichtungszusagen des Unternehmens, das Gegenstand der Prüfung ist, annehmen, wenn diese Verpflichtungszusagen die Verzerrung auf dem Binnenmarkt vollständig und wirksam beseitigen. Nimmt die Kommission solche Verpflichtungszusagen an, so erklärt sie die Verpflichtungen mittels eines Verpflichtungsbeschlusses nach Artikel 10 Absatz 3 für das Unternehmen, das Gegenstand der Prüfung ist, für bindend. Gegebenenfalls wird überwacht, ob das Unternehmen die vereinbarten Verpflichtungszusagen einhält.***

- (3) Die Verpflichtungszusagen bzw. Abhilfemaßnahmen müssen **verhältnismäßig sein und die tatsächlich oder potenziell** durch die drittstaatliche Subvention auf dem Binnenmarkt verursachte Verzerrung vollständig und wirksam beseitigen.
- (4) Die Verpflichtungen bzw. Abhilfemaßnahmen können **unter anderem**. Folgendes umfassen:
- a) Gewährung des Zugangs zu Infrastruktur – **einschließlich Forschungseinrichtungen, Produktionsmittel oder wesentlicher Einrichtungen** –, die durch die den Binnenmarkt verzerrenden drittstaatlichen Subventionen erworben oder gefördert wurde, zu fairen, **angemessenen** und diskriminierungsfreien Bedingungen, es sei denn, ein solcher Zugang ist bereits im Unionsrecht vorgesehen,
 - b) Verringerung der Kapazitäten oder der Marktpresenz, **auch durch vorübergehende Beschränkungen der Geschäftstätigkeit**,
 - c) Verzicht auf bestimmte Investitionen,
 - d) Lizenzvergabe zu fairen, angemessenen und diskriminierungsfreien Bedingungen für Vermögenswerte, die mithilfe drittstaatlicher Subventionen erworben oder entwickelt wurden,

- e) Veröffentlichung der Ergebnisse von Forschung und Entwicklung,
 - f) Veräußerung bestimmter Vermögenswerte,
 - g) an die ■ Unternehmen ergehende Anordnung, den betreffenden Zusammenschluss rückgängig zu machen,
 - h) Rückzahlung der drittstaatlichen Subvention, einschließlich einer angemessenen Verzinsung, **die anhand der in der Verordnung (EG) Nr. 794/2004 der Kommission²² dargelegten Methode berechnet wird,**
 - i) **an die beteiligten Unternehmen ergehende Anordnung, ihre Governance-Struktur anzupassen.**
- (5) Die Kommission **erlegt gegebenenfalls** Berichterstattungs- und Transparenzvorschriften, **einschließlich einer regelmäßigen Berichterstattung über die Umsetzung der in Absatz 4 aufgeführten Verpflichtungen und Abhilfemaßnahmen, auf.**
-

²² Verordnung (EG) Nr. 794/2004 der Kommission vom 21. April 2004 zur Durchführung der Verordnung (EU) 2015/1589 des Rates über besondere Vorschriften für die Anwendung von Artikel 108 des Vertrags über die Arbeitsweise der Europäischen Union (ABl. L 140 vom 30.4.2004, S. 1).

- (6) Schlägt das ■ Unternehmen, **das Gegenstand der Prüfung ist**, vor, die drittstaatliche Subvention einschließlich einer angemessenen Verzinsung zurückzuzahlen, so akzeptiert die Kommission die Rückzahlung **nur dann** als Verpflichtung, wenn sie feststellen kann, dass die Rückzahlung transparent, **überprüfbar** und wirksam ist, wobei sie dem Risiko einer Umgehung der Ziele dieser Verordnung Rechnung trägt.

Artikel 8

Informationen über künftige Zusammenschlüsse und öffentliche Vergabeverfahren

Bei Beschlüssen nach den Artikeln 11, 25 und 31 kann das Unternehmen, das Gegenstand der Prüfung ist, wenn dies angemessen und erforderlich ist, dazu verpflichtet sein, die Kommission für einen begrenzten Zeitraum über seine Teilnahme an Zusammenschlüssen oder öffentlichen Vergabeverfahren zu unterrichten. Diese Verpflichtung gilt unbeschadet der Anmelde- bzw. Meldepflichten gemäß Artikel 21 bzw. 29.

Kapitel 2

Von Amts wegen eingeleitete Prüfung **und allgemeine Bestimmungen** zur Prüfung drittstaatlicher Subventionen

Artikel 9

Von Amts wegen eingeleitete Prüfung drittstaatlicher Subventionen

- (1) Die Kommission kann auf eigene Initiative Informationen aus allen Quellen, **einschließlich Mitgliedstaaten, eine natürliche oder juristische Person oder eine Vereinigung**, über mutmaßlich den Binnenmarkt verzerrende drittstaatliche Subventionen prüfen.
- (2) **Von Amts wegen eingeleitete Prüfungen öffentlicher Vergabeverfahren sind auf vergebene Aufträge beschränkt.**

Diese Prüfungen dürfen nicht zur Aufhebung der Entscheidung über die Vergabe eines Auftrags oder zur Kündigung eines Auftrags führen.

Artikel 10

Vorprüfung

- (1) **Deuten die in Artikel 9 genannten Informationen nach Auffassung der Kommission darauf hin, dass eine den Binnenmarkt verzerrende drittstaatliche Subvention vorliegen könnte**, so holt die Kommission alle Informationen ein, die sie für erforderlich hält, um vorläufig zu beurteilen, ob die geprüfte finanzielle Zuwendung eine drittstaatliche Subvention darstellt und ob sie den Binnenmarkt verzerrt. Dazu kann die Kommission insbesondere
- a) Auskunft nach **Artikel 13** verlangen **und**
 - b) innerhalb und außerhalb der Union Nachprüfungen nach **Artikel 14** oder **Artikel 15** durchführen.
- (2) **Hat ein Mitgliedstaat der Kommission mitgeteilt, dass ein entsprechendes nationales Verfahren geplant ist oder eingeleitet wurde, so unterrichtet die Kommission diesen Mitgliedstaat über den Beginn der Vorprüfung. Insbesondere unterrichtet die Kommission die Mitgliedstaaten, die der Kommission ein nationales Verfahren gemäß der Verordnung (EU) 2019/452 notifiziert haben, über den Beginn der Vorprüfung. Wird die Vorprüfung im Zusammenhang mit einem öffentlichen Vergabeverfahren eingeleitet, so setzt die Kommission auch den betreffenden öffentlichen Auftraggeber bzw. den betreffenden Auftraggeber davon in Kenntnis.**

- (3) **Liegen** der Kommission auf der Grundlage der Vorprüfung ■ hinreichende Anhaltspunkte dafür **vor**, dass einem Unternehmen eine den Binnenmarkt verzerrende drittstaatliche Subvention gewährt wurde, so
- a) erlässt sie einen Beschluss zur Einleitung einer eingehenden Prüfung (im Folgenden „Beschluss zur Einleitung einer eingehenden Prüfung“), in dem die relevanten Tatbestands- und Rechtsfragen zusammengefasst sind und die vorläufige Beurteilung hinsichtlich des Vorliegens einer drittstaatlichen Subvention und der tatsächlichen oder potenziellen Verzerrung auf dem Binnenmarkt enthalten ist,
 - b) setzt sie das ■ Unternehmen, **das Gegenstand der Prüfung ist**, davon in Kenntnis,
 - c) **setzt sie die Mitgliedstaaten und, wenn die eingehende Prüfung im Zusammenhang mit einem öffentlichen Vergabeverfahren eingeleitet wird, den betreffenden öffentlichen Auftraggeber bzw. den Auftraggeber davon in Kenntnis** und

- d) veröffentlicht sie eine Bekanntmachung im *Amtsblatt der Europäischen Union* mit der Aufforderung, innerhalb einer von der Kommission bestimmten Frist schriftlich Stellung zu nehmen.
- (4) Gelangt die Kommission während einer Vorprüfung zu dem Schluss, dass keine hinreichenden Anhaltspunkte für die Einleitung einer eingehenden Prüfung vorliegen, weil entweder keine drittstaatliche Subvention vorliegt oder keine hinreichenden Anhaltspunkte für eine tatsächliche oder potenzielle Verzerrung auf dem Binnenmarkt vorliegen, schließt sie die Vorprüfung ab und setzt das ■ Unternehmen, das Gegenstand der Prüfung ist, ■ die ■ Mitgliedstaaten, **die gemäß Absatz 2 unterrichtet wurden, sowie – wenn die Vorprüfung im Zusammenhang mit einem öffentlichen Vergabeverfahren eingeleitet wurde – den betreffenden öffentlichen Auftraggeber bzw. den betreffenden Auftraggeber** davon in Kenntnis.

Artikel 11

Eingehende Prüfung

- (1) Im Rahmen der eingehenden Prüfung nimmt die Kommission eine genauere Beurteilung der ■ drittstaatlichen Subvention, die im Beschluss über die Einleitung einer eingehenden Prüfung bezeichnet wurde, vor und holt nach den **Artikeln 13, 14 und 15** alle Informationen ein, die sie für erforderlich hält.

- (2) Stellt die Kommission nach den Artikeln 4 bis 6 fest, dass eine drittstaatliche Subvention den Binnenmarkt verzerrt, so kann sie **einen Durchführungsrechtsakt in Form eines Beschlusses, mit dem** Abhilfemaßnahmen **auferlegt werden**, (im Folgenden „Beschluss zur Auferlegung von Abhilfemaßnahmen“) **erlassen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.**
- (3) Stellt die Kommission nach den Artikeln 4 bis 6 fest, dass eine drittstaatliche Subvention den Binnenmarkt verzerrt, und bietet das ■ Unternehmen, **das Gegenstand der Prüfung ist**, Verpflichtungen an, die die Kommission für geeignet und hinreichend hält, um die Verzerrung vollständig und wirksam zu beseitigen, so kann sie **einen Durchführungsrechtsakt in Form eines Beschlusses erlassen, um** die Verpflichtungszusagen ■ für das Unternehmen für bindend zu **erklären**, (im Folgenden „Verpflichtungsbeschluss“). Ein Beschluss, mit dem die Rückzahlung einer drittstaatlichen Subvention nach Artikel 7 Absatz 6 genehmigt wird, gilt als Verpflichtungsbeschluss. **Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.**

(4) Die Kommission erlässt einen **Durchführungsrechtsakt in Form eines Beschlusses**, keine Einwände zu erheben (im Folgenden „Beschluss, keine Einwände zu erheben“), wenn sie feststellt, dass

- a) sich die in ihrem Beschluss zur Einleitung einer eingehenden Prüfung dargelegte vorläufige Beurteilung nicht bestätigt oder
- b) positive Auswirkungen im Sinne des Artikels 6 schwerer wiegen als eine Verzerrung auf dem Binnenmarkt.

Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

(5) ***Die Kommission bemüht sich soweit wie möglich darum, einen Beschluss innerhalb von 18 Monaten nach Einleitung der eingehenden Prüfung zu erlassen.***

Artikel 12

Einstweilige Maßnahmen

(1) Um den Wettbewerb auf dem Binnenmarkt zu wahren und nicht wiedergutzumachenden Schaden abzuwenden, kann die Kommission **einen Durchführungsrechtsakt in Form eines Beschlusses zur Anordnung** einstweiliger Maßnahmen **erlassen**, wenn

- a)** es **hinreichende** Anhaltspunkte dafür gibt, dass eine finanzielle Zuwendung eine drittstaatliche Subvention darstellt und den Binnenmarkt verzerrt und
- b)** die **■** Gefahr eines **schweren** und nicht wiedergutzumachenden **Schadens** für den Wettbewerb auf dem Binnenmarkt besteht.

Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

(2) Die einstweiligen Maßnahmen können insbesondere, müssen aber nicht ausschließlich aus den in Artikel 7 Absatz 4 Buchstaben a, c und d genannten Maßnahmen bestehen. Im Zusammenhang mit öffentlichen Vergabeverfahren dürfen keine einstweiligen Maßnahmen ergriffen werden.

- (3) *Die einstweiligen Maßnahmen gelten entweder für einen bestimmten Zeitraum, der soweit erforderlich und angemessen verlängert werden kann, oder bis der endgültige Beschluss erlassen wurde.*

Artikel 13

Auskunftsverlangen

- (1) *Zur Erfüllung der ihr mit dieser Verordnung übertragenen Aufgaben kann die Kommission im Einklang dem vorliegenden Artikel Auskünfte verlangen.*
- (2) Die Kommission kann von einem ■ Unternehmen, *das Gegenstand der Prüfung ist*, alle erforderlichen Auskünfte verlangen, *einschließlich Auskünfte in Bezug auf sein Angebot im Rahmen eines öffentlichen Vergabeverfahrens.*
- (3) Die Kommission kann *diese Auskünfte, einschließlich Auskünfte in Bezug auf ihre Angebote im Rahmen öffentlicher Vergabeverfahren*, auch von anderen Unternehmen oder Unternehmensvereinigungen *verlangen, wobei dem Grundsatz der Verhältnismäßigkeit gebührend Rechnung zu tragen ist.*

- (4) Ein Auskunftsverlangen **gemäß Absatz 2 oder 3** enthält Folgendes:
- a) die Angabe der Rechtsgrundlage und des Zwecks des Auskunftsverlangens, eine Auflistung der benötigten Angaben und eine angemessene Frist für deren Übermittlung,
 - b) den Hinweis, dass bei Übermittlung unrichtiger, unvollständiger oder irreführender Angaben die Geldbußen oder Zwangsgelder nach **Artikel 17** verhängt werden können,
 - c) eine Erklärung, dass die Kommission **nach Artikel 16** bei mangelnder Bereitschaft ■ zur Kooperation ■ einen Beschluss auf der Grundlage der ihr verfügbaren Informationen erlassen kann.
- (5) Auf Aufforderung der Kommission erteilen die Mitgliedstaaten ihr alle Auskünfte, die sie zur Erfüllung der ihr mit dieser Verordnung übertragenen Aufgaben benötigt. **Absatz 4 Buchstabe a gilt entsprechend.**
- (6) Die Kommission kann auch **von ■ Drittstaaten alle erforderlichen Auskünfte verlangen. Absatz 4 Buchstaben a und c gilt entsprechend.**

- (7) *Die Kommission kann eine natürliche oder juristische Person befragen, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt. Findet eine Befragung nicht in den Räumlichkeiten der Kommission, telefonisch oder auf einem anderen elektronischen Weg statt, so*
- a) unterrichtet die Kommission vor der Befragung den Mitgliedstaat, in dessen Hoheitsgebiet die Befragung stattzufinden hat, oder*
 - b) holt die Kommission vor der Befragung die Zustimmung des Drittstaats, in dessen Hoheitsgebiet die Befragung stattzufinden hat, ein.*

Artikel 14

Nachprüfungen innerhalb der Union

- (1) *Zur Erfüllung der ihr mit dieser Verordnung übertragenen Aufgaben* kann die Kommission *bei Unternehmen und Unternehmensvereinigungen* die erforderlichen Nachprüfungen vornehmen.

- (2) Führt die Kommission eine solche Nachprüfung durch, so sind die von der Kommission mit der Durchführung der Nachprüfung beauftragten Bediensteten befugt,
- a) alle Räumlichkeiten, Grundstücke **und Transportmittel der Unternehmen oder Unternehmensvereinigungen** zu betreten,
 - b) die Bücher und sonstigen Geschäftsunterlagen, **unabhängig davon, in welcher Form sie gespeichert sind**, zu prüfen, **auf alle Informationen zuzugreifen, die der Einheit, die Gegenstand der Nachprüfung ist, zugänglich sind**, sowie Kopien oder Auszüge dieser Bücher oder Unterlagen anzufordern,
 - c) von allen Vertretern oder Beschäftigten des Unternehmens **oder der Unternehmensvereinigung** Erläuterungen zu Sachverhalten oder Unterlagen zu verlangen, die mit Gegenstand und Zweck der Nachprüfung in Zusammenhang stehen, und ihre Antworten aufzuzeichnen,
 - d) betriebliche Räumlichkeiten und Bücher oder Unterlagen jeder Art für die Dauer der Nachprüfung und in dem hierfür erforderlichen Ausmaß zu versiegeln.

- (3) Das ■ Unternehmen **oder die Unternehmensvereinigung** ist verpflichtet, von der Kommission durch Beschluss angeordnete Nachprüfungen zu dulden. Die mit einer Nachprüfung beauftragten Bediensteten der Kommission und die anderen von ihr ermächtigten Begleitpersonen üben ihre Befugnisse unter Vorlage eines Kommissionsbeschlusses aus, der Folgendes enthält:
- a) die Angabe von Gegenstand und Zweck der Nachprüfung,
 - b) eine Erklärung, dass die Kommission **nach Artikel 16** bei mangelnder Bereitschaft ■ zur Kooperation ■ einen Beschluss auf der Grundlage der ihr verfügbaren Informationen erlassen kann,
 - c) einen Hinweis, **dass nach Artikel 17** Geldbußen oder Zwangsgelder **verhängt werden können, und**
 - d) **einen Hinweis auf das Recht, den Beschluss gemäß Artikel 263 AEUV durch den Gerichtshof überprüfen zu lassen.**
- (4) Die Kommission unterrichtet den Mitgliedstaat, in dessen Hoheitsgebiet die Nachprüfung vorgenommen werden soll, rechtzeitig vor deren Beginn über den Prüfungsauftrag **und den Tag, an dem die Nachprüfung beginnt.**

- (5) Die von dem Mitgliedstaat, in dessen Hoheitsgebiet die Nachprüfung vorgenommen werden soll, ermächtigten oder benannten Bediensteten **und anderen Personen** unterstützen auf Anweisung des Mitgliedstaats oder auf Ersuchen der Kommission die Bediensteten der Kommission und die anderen von ihr ermächtigten Begleitpersonen aktiv. Sie verfügen hierzu über die in Absatz 2 genannten Befugnisse.
- (6) Stellen die beauftragten Bediensteten der Kommission oder die anderen von ihr ermächtigten Begleitpersonen fest, dass sich ein Unternehmen **oder eine Unternehmensvereinigung** einer Nachprüfung im Sinne dieses Artikels widersetzt, so leistet der ■ Mitgliedstaat, **in dessen Hoheitsgebiet die Nachprüfung vorgenommen werden soll**, die erforderliche Amtshilfe, gegebenenfalls unter Einsatz der Polizei oder anderer gleichwertiger Vollzugsorgane, damit die Nachprüfung durchgeführt werden kann. **Setzt die in diesem Absatz genannte Amtshilfe nach nationalem Recht eine gerichtliche Genehmigung voraus, so ist diese zu beantragen. Die Genehmigung kann auch vorsorglich beantragt werden.**

- (7) Auf Ersuchen der Kommission führt ein Mitgliedstaat in seinem Hoheitsgebiet Nachprüfungen oder andere Ermittlungsmaßnahmen nach seinem nationalen Recht durch, um festzustellen, ob eine drittstaatliche Subvention vorliegt, die den Binnenmarkt verzerrt.

Artikel 15

Nachprüfungen außerhalb der Union

Zur Erfüllung der ihr mit dieser Verordnung übertragenen Aufgaben kann die Kommission Nachprüfungen im Hoheitsgebiet eines Drittstaats durchführen, sofern ■ die Regierung dieses Drittstaats offiziell unterrichtet wurde und **keine Einwände gegen die Nachprüfung erhebt. Die Kommission kann auch das Unternehmen oder die Unternehmensvereinigung um Zustimmung zur Nachprüfung ersuchen.** Artikel 14 Absätze 1 und 2 und Absatz 3 Buchstaben a und b gelten entsprechend.

Artikel 16

Mangelnde Bereitschaft zur Kooperation

- (1) Die Kommission kann auf der Grundlage der verfügbaren Informationen einen Beschluss nach **Artikel 10, Artikel 11, Artikel 25 Absatz 3 oder Artikel 31 Absatz 2** erlassen, wenn ein ■ Unternehmen, **das Gegenstand der Prüfung ist**, oder ein Drittstaat, **der die drittstaatliche Subvention gewährt hat**,
- a) auf ein Auskunftsverlangen nach **Artikel 13** hin unvollständige, unrichtige oder irreführende Angaben macht,
 - b) die verlangten Auskünfte nicht innerhalb der von der Kommission gesetzten Frist erteilt,
 - c) sich weigert, eine von der Kommission nach **Artikel 14** oder **Artikel 15** angeordnete Nachprüfung innerhalb oder außerhalb der Union zu dulden oder
 - d) in anderer Weise die Vorprüfung oder die eingehende Prüfung behindert.
- (2) Hat ein Unternehmen oder eine Unternehmensvereinigung, ein Mitgliedstaat oder der Drittstaat gegenüber der Kommission unrichtige oder irreführende Angaben gemacht, so werden diese Angaben nicht berücksichtigt.

- (3) Erteilt ein ■ Unternehmen, bei dem es sich auch um ein unmittelbar oder mittelbar vom Staat kontrolliertes öffentliches Unternehmen handeln kann, nicht die Auskünfte, die erforderlich sind, um festzustellen, ob ihm durch eine finanzielle Zuwendung ein Vorteil entsteht, so kann davon ausgegangen werden, dass dem Unternehmen ein solcher Vorteil entstanden ist.
- (4) Bei Heranziehung der verfügbaren Informationen darf das Ergebnis des Verfahrens für das ■ Unternehmen ungünstiger ausfallen, als wenn es kooperiert hätte.

Artikel 17

Geldbußen und Zwangsgelder

- (1) Die Kommission kann durch Beschluss Geldbußen oder Zwangsgelder verhängen, wenn ein ■ Unternehmen oder eine Unternehmensvereinigung vorsätzlich oder fahrlässig
- a) auf ein Auskunftsverlangen nach **Artikel 13** hin unvollständige, unrichtige oder irreführende Angaben macht oder die Angaben nicht innerhalb der gesetzten Frist übermittelt,

- b) bei Nachprüfungen nach **Artikel 14** die angeforderten Bücher oder sonstigen Geschäftsunterlagen nicht vollständig vorlegt,
- c) bei der Beantwortung einer nach **Artikel 14** Absatz 2 Buchstabe c gestellten Frage
 - i) eine unrichtige oder irreführende Antwort erteilt,
 - ii) eine unrichtige, unvollständige oder irreführende Antwort eines Beschäftigten nicht innerhalb einer von der Kommission gesetzten Frist berichtet oder
 - iii) in Bezug auf Sachverhalte, die mit Gegenstand und Zweck einer durch einen Beschluss nach **Artikel 14** Absatz 3 angeordneten Nachprüfung in Zusammenhang stehen, keine vollständige Antwort erteilt oder eine vollständige Antwort verweigert,
- d) nach **Artikel 14** angeordnete Nachprüfungen nicht duldet oder nach **Artikel 14** Absatz 2 Buchstabe d angebrachte Siegel erbrochen hat, **oder**
- e) **die Bedingungen für die Akteneinsicht oder die von der Kommission auferlegten Bedingungen für die Offenlegung gemäß Artikel 42 Absatz 4 nicht einhält.**

- (2) Die Geldbußen, die gemäß Absatz 1 verhängt werden, betragen höchstens 1 % des Gesamtumsatzes des betreffenden Unternehmens oder der betreffenden Unternehmensvereinigung im vorangegangenen Geschäftsjahr.
- (3) Die Zwangsgelder, die gemäß Absatz 1 verhängt werden, betragen höchstens 5 % des von dem betreffenden Unternehmen oder der betreffenden Unternehmensvereinigung im vorangegangenen Geschäftsjahr erzielten durchschnittlichen täglichen Gesamtumsatzes für jeden Arbeitstag, um den die im Beschluss festgesetzte Frist überschritten wird, bis die von der Kommission verlangten Auskünfte vollständig und sachlich richtig erteilt wurden **oder bis eine Nachprüfung geduldet wird**.
- (4) Bevor die Kommission einen Beschluss nach Absatz 1 **Buchstabe a** erlässt, setzt sie eine letzte Frist von zwei Wochen, in der das ■ Unternehmen oder die ■ Unternehmensvereinigung die fehlenden Angaben machen kann.

- (5) Kommt ein ■ Unternehmen einem Verpflichtungsbeschluss nach **Artikel 11** Absatz 3, einem Beschluss zur Anordnung einstweiliger Maßnahmen nach **Artikel 12** oder einem Beschluss mit Abhilfemaßnahmen nach **Artikel 11** Absatz 2 nicht nach, so kann die Kommission durch Beschluss
- a) Geldbußen von höchstens 10 % des von dem betreffenden Unternehmen im vorangegangenen Geschäftsjahr erzielten Gesamtumsatzes verhängen oder
 - b) Zwangsgelder von höchstens 5 % des durchschnittlichen täglichen Gesamtumsatzes des betreffenden Unternehmens im vorangegangenen Geschäftsjahr für jeden Tag der Nichtbefolgung verhängen, beginnend mit dem Tag des Kommissionsbeschlusses zur Verhängung des Zwangsgelds bis zu dem Tag, an dem die Kommission feststellt, dass das betreffende Unternehmen dem Beschluss nachkommt.

Die Kommission kann diese Geldbußen oder Zwangsgelder auch verhängen, wenn das Unternehmen einen nach Artikel 11, 25 oder 31 erlassenen Beschluss nicht einhält, mit dem das Unternehmen gemäß Artikel 8 verpflichtet wurde, die Kommission über seine künftige Teilnahme an Zusammenschlüssen oder öffentlichen Vergabeverfahren zu unterrichten.

- (6) Bei der Festsetzung der Höhe der Geldbuße oder des Zwangsgelds trägt die Kommission der Art, der Schwere und der Dauer der Zuwiderhandlung sowie dem Grundsatz der Verhältnismäßigkeit und der Angemessenheit gebührend Rechnung.
- (7) *Wenn das betreffende Unternehmen oder die betreffende Unternehmensvereinigung der Verpflichtung nachgekommen ist, zu deren Erfüllung das Zwangsgeld festgesetzt worden war, kann die Kommission die endgültige Höhe des Zwangsgelds im Vergleich zu dem Betrag aus dem ursprünglichen Beschluss, mit dem das Zwangsgeld verhängt wurde, herabsetzen.*

Artikel 18

Widerruf

- (1) In den folgenden Fällen kann die Kommission einen Beschluss nach **Artikel 11** Absatz 2, 3 oder 4, **Artikel 25 Absatz 3 und Artikel 31 Absatz 1, 2 oder 3** aufheben und einen neuen **Durchführungsrechtsakt in Form eines** Beschlusses erlassen, **und zwar wenn**
- a) das ■ Unternehmen, *an das der ursprüngliche Beschluss gerichtet war, gegen die eingegangenen* Verpflichtungen oder die auferlegten Abhilfemaßnahmen *verstößt*,

b) der ursprüngliche Beschluss auf unvollständigen, unrichtigen oder irreführenden Angaben beruhte,

c) *die Verpflichtungen oder die Abhilfemaßnahmen nicht gewirkt haben.*

Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

(2) *Der Widerruf und die Annahme eines neuen Beschlusses durch die Kommission gemäß Absatz 1 berühren nicht die Entscheidung des öffentlichen Auftraggebers bzw. des Auftraggebers über die Vergabe eines Auftrags. Sie berühren auch keinen Auftrag, der nach einer solchen Entscheidung über die Vergabe bereits abgeschlossen worden war.*

Kapitel 3

Zusammenschlüsse

Artikel 19

Verzerrungen auf dem Binnenmarkt durch drittstaatliche Subventionen für Zusammenschlüsse

Bei der Beurteilung, ob eine drittstaatliche Subventionen für einen Zusammenschluss den Binnenmarkt im Sinne von Artikel 4 oder 5 verzerrt, ist die Beurteilung auf diesen Zusammenschluss beschränkt. Bei der Beurteilung werden ausschließlich drittstaatliche Subventionen berücksichtigt, die in den drei **Jahren** vor Vertragsabschluss, Veröffentlichung des Übernahmeangebots oder Erwerb einer die Kontrolle begründenden Beteiligung gewährt wurden.

Artikel 20

Zusammenschlüsse und Anmeldeschwellen

- (1) Für die Zwecke dieser Verordnung wird ein Zusammenschluss dadurch bewirkt, dass eine dauerhafte Veränderung der Kontrolle auf eine der beiden folgenden Arten stattfindet:
 - a) zwei oder mehr bisher voneinander unabhängige Unternehmen oder Unternehmensteile fusionieren oder

- b) eine oder mehrere Personen, die bereits mindestens ein Unternehmen kontrollieren, oder ein oder mehrere Unternehmen erwerben durch den Erwerb von Anteilsrechten oder Vermögenswerten, durch Vertrag oder in sonstiger Weise die unmittelbare oder mittelbare Kontrolle über die Gesamtheit oder über Teile eines oder mehrerer anderer Unternehmen.
- (2) Die Gründung eines Gemeinschaftsunternehmens, das auf Dauer alle Funktionen einer selbstständigen wirtschaftlichen Einheit erfüllt, stellt einen Zusammenschluss im Sinne des Absatzes 1 dar.
- (3) Für die Zwecke dieser Verordnung liegt ein „anmeldepflichtiger Zusammenschluss“ vor, wenn bei einem Zusammenschluss
- a) **■** mindestens eines der fusionierenden Unternehmen, **das erworbene Unternehmen** oder **das Gemeinschaftsunternehmen** in der Union niedergelassen ist und in der Union einen Gesamtumsatz von mindestens 500 Mio. EUR erzielt und
 - b) **die folgenden** Unternehmen in den drei **Jahren** vor Vertragsabschluss, Veröffentlichung des Übernahmeangebots oder Erwerb einer die Kontrolle begründenden Beteiligung von Drittstaaten finanzielle Zuwendungen von insgesamt mehr als 50 Mio. EUR erhalten haben:
 - i) bei einer Übernahme der oder die Erwerber und das erworbene Unternehmen,
 - ii) bei einer Fusion die fusionierenden Unternehmen,
 - iii) bei einem Gemeinschaftsunternehmens die Unternehmen, die das Gemeinschaftsunternehmen gründen und das Gemeinschaftsunternehmen.

(4) Ein Zusammenschluss wird nicht bewirkt, wenn

- a) Kreditinstitute, sonstige Finanzinstitute oder Versicherungsgesellschaften, deren normale Tätigkeit Geschäfte und den Handel mit Wertpapieren für eigene oder fremde Rechnung einschließt, vorübergehend Anteile an einem Unternehmen zum Zweck der Veräußerung erwerben, sofern sie die mit den Anteilen verbundenen Stimmrechte nicht ausüben, um das Wettbewerbsverhalten des Unternehmens zu bestimmen, oder sofern sie die Stimmrechte nur ausüben, um die Veräußerung der Gesamtheit oder von Teilen des Unternehmens oder seiner Vermögenswerte oder die Veräußerung der Anteile vorzubereiten, und sofern die Veräußerung innerhalb eines Jahres nach dem Zeitpunkt des Erwerbs erfolgt;**
- b) wenn der Träger eines öffentlichen Mandats aufgrund der Gesetzgebung eines Mitgliedstaats über die Auflösung von Unternehmen, die Insolvenz, die Zahlungseinstellung, den Vergleich oder ähnliche Verfahren die Kontrolle erwirbt;**

- c) wenn die in Absatz 1 Buchstabe b bezeichneten Handlungen von Beteiligungsunternehmen im Sinne von Artikel 2 Nummer 15 der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates²³ vorgenommen werden, mit der Einschränkung, dass die mit den erworbenen Anteilen verbundenen Stimmrechte, insbesondere wenn sie zur Ernennung der Mitglieder der geschäftsführenden oder aufsichtsführenden Organe der Unternehmen ausgeübt werden, an denen die Beteiligungsgesellschaften Anteile halten, nur zur Erhaltung des vollen Wertes der Investitionen und nicht dazu benutzt werden, unmittelbar oder mittelbar das Wettbewerbsverhalten dieser Unternehmen zu bestimmen.

Die in Unterabsatz 1 Buchstabe a genannte Frist von einem Jahr kann von der Kommission auf Antrag verlängert werden, wenn die genannten Institute oder Gesellschaften nachweisen, dass die Veräußerung innerhalb der vorgeschriebenen Frist unzumutbar war.

²³ 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).

- (5) Die Kontrolle wird durch Rechte, Verträge oder andere Mittel begründet, die einzeln oder zusammen unter Berücksichtigung aller tatsächlichen oder rechtlichen Umstände die Möglichkeit gewähren, einen bestimmenden Einfluss auf die Tätigkeit eines Unternehmens auszuüben, insbesondere durch
- a) Eigentums- oder Nutzungsrechte an der Gesamtheit oder an Teilen des Vermögens des Unternehmens,
 - b) Rechte oder Verträge, die einen bestimmenden Einfluss auf die Zusammensetzung, die Beratungen oder Beschlüsse der Organe des Unternehmens gewähren.
- (6) Die Kontrolle wird für die Personen oder Unternehmen begründet,
- a) die aus diesen Rechten oder Verträgen selbst berechtigt sind, oder
 - b) die, obwohl sie aus diesen Rechten oder Verträgen nicht selbst berechtigt sind, die Befugnis haben, die sich daraus ergebenden Rechte auszuüben.

Artikel 21

Vorherige Anmeldung von Zusammenschlüssen

- (1) Anmeldepflichtige Zusammenschlüsse werden nach Vertragsabschluss, Veröffentlichung des Übernahmeangebots oder Erwerb einer die Kontrolle begründenden Beteiligung vor ihrem Vollzug bei der Kommission angemeldet.
- (2) Die beteiligten Unternehmen können den geplanten Zusammenschluss auch anmelden, wenn sie der Kommission gegenüber glaubhaft machen, dass sie gewillt sind, einen Vertrag zu schließen, oder im Fall eines Übernahmeangebots öffentlich ihre Absicht zur Abgabe eines solchen Angebots bekundet haben, sofern der beabsichtigte Vertrag oder das beabsichtigte Angebot zu einem anmeldepflichtigen Zusammenschluss nach Absatz 1 führen würde.
- (3) Zusammenschlüsse in Form einer Fusion im Sinne des **Artikels 20** Absatz 1 Buchstabe a oder in Form des Erwerbs der gemeinsamen Kontrolle im Sinne des **Artikels 20** Absatz 1 Buchstabe b werden von den an der Fusion oder dem Erwerb der gemeinsamen Kontrolle Beteiligten gemeinsam angemeldet. In allen anderen Fällen wird die Anmeldung von der Person oder dem Unternehmen vorgenommen, die bzw. das die Kontrolle über die Gesamtheit oder über Teile eines oder mehrerer Unternehmen erwirbt.

- (4) Kommen die beteiligten Unternehmen ihrer Anmeldepflicht nicht nach, so kann die Kommission die Anmeldung eines anmeldepflichtigen Zusammenschlusses verlangen und ihn nach Maßgabe dieser Verordnung prüfen. In diesem Fall ist die Kommission nicht an die in **Artikel 24** Absätze 1 und 4 genannten Fristen gebunden.
- (5) Die Kommission kann die vorherige Anmeldung eines Zusammenschlusses, bei dem es sich nicht um einen anmeldepflichtigen Zusammenschluss im Sinne des **Artikels 20** handelt, vor dem Vollzug des Zusammenschlusses jederzeit verlangen, wenn sie vermutet, dass die beteiligten Unternehmen in den drei Jahren vor dem Zusammenschluss ■ drittstaatliche Subventionen **erhalten** haben könnten. Dieser Zusammenschluss gilt für die Zwecke dieser Verordnung als anmeldepflichtiger Zusammenschluss.

Artikel 22

Berechnung des Umsatzes

- (1) Der Gesamtumsatz umfasst die Umsätze, welche die beteiligten Unternehmen im vorangegangenen Geschäftsjahr mit Waren und Dienstleistungen erzielt haben und die dem normalen geschäftlichen Tätigkeitsbereich der Unternehmen zuzuordnen sind, unter Abzug von Erlösschmälerungen, der Mehrwertsteuer und anderer unmittelbar auf den Umsatz bezogener Steuern. Der Gesamtumsatz eines beteiligten Unternehmens enthält nicht den Verkauf von Waren und die Erbringung von Dienstleistungen zwischen den in Absatz 4 genannten Unternehmen.

Der in der **Union** erzielte Umsatz umfasst den Verkauf von Waren und die Erbringung von Dienstleistungen für Unternehmen oder Verbraucher in der Union.

- (2) Wird der Zusammenschluss durch den Erwerb von Teilen eines oder mehrerer Unternehmen bewirkt, so ist unabhängig davon, ob diese Teile eigene Rechtspersönlichkeit besitzen, abweichend von Absatz 1 aufseiten des Veräußerers bzw. der Veräußerer nur der Umsatz zu berücksichtigen, der auf die veräußerten Teile entfällt.

Zwei oder mehr Erwerbsvorgänge im Sinne des Unterabsatzes 1 dieses Absatzes, die innerhalb von zwei Jahren zwischen denselben Personen oder Unternehmen getätigt werden, werden hingegen als ein einziger Zusammenschluss behandelt, der zum Zeitpunkt des letzten Erwerbsvorgangs stattfindet.

(3) An die Stelle des Umsatzes tritt

- a) bei Kredit- und sonstigen Finanzinstituten die Summe der folgenden in der Richtlinie 86/635/EWG des Rates²⁴ definierten Ertragsposten gegebenenfalls nach Abzug der Mehrwertsteuer und sonstiger direkt auf diese Erträge erhobener Steuern:
 - i) Zinserträge und ähnliche Erträge,

²⁴ Richtlinie 86/635/EWG des Rates vom 8. Dezember 1986 über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten (ABl. L 372 vom 31.12.1986, S. 1).

- ii) Erträge aus Wertpapieren:
 - Erträge aus Aktien, anderen Anteilsrechten und nicht festverzinslichen Wertpapieren,
 - Erträge aus Beteiligungen,
 - Erträge aus Anteilen an verbundenen Unternehmen,
 - iii) Provisionserträge,
 - iv) Nettoerträge aus Finanzgeschäften,
 - v) sonstige betriebliche Erträge,
- b) bei Versicherungsunternehmen die Summe der Bruttoprämien; diese Summe umfasst alle vereinnahmten sowie alle noch zu vereinnahmenden Prämien aufgrund von Versicherungsverträgen, die von diesen Unternehmen oder für ihre Rechnung abgeschlossen worden sind, einschließlich etwaiger Rückversicherungsprämien und abzüglich der aufgrund des Betrags der Prämie oder des gesamten Prämienvolumens berechneten Steuern und sonstigen Abgaben.

Für die Zwecke des Buchstaben a besteht für ein Kreditinstitut oder für ein Finanzinstitut der Umsatz in der Union aus den unter Buchstabe a genannten Ertragsposten, die die in der Union niedergelassene Zweig- oder Geschäftsstelle des Instituts verbucht.

Für die Zwecke des Buchstaben b besteht für ein Versicherungsunternehmen der Umsatz in der Union aus den von in der Union ansässigen Personen enthaltenen Bruttoprämien.

- (4) Der Gesamtumsatz eines beteiligten Unternehmens setzt sich unbeschadet des Absatzes 2 zusammen aus den Umsätzen
- a) des beteiligten Unternehmens,
 - b) der Unternehmen, in denen das beteiligte Unternehmen unmittelbar oder mittelbar entweder
 - i) mehr als die Hälfte des Kapitals oder des Betriebsvermögens besitzt oder
 - ii) über mehr als die Hälfte der Stimmrechte verfügt oder
 - iii) mehr als die Hälfte der Mitglieder des Aufsichtsrats, des Verwaltungsrats oder der zur gesetzlichen Vertretung berufenen Organe bestellen kann oder
 - iv) das Recht hat, die Geschäfte dieser Unternehmen zu führen,

- c) der Unternehmen, die in dem beteiligten Unternehmen die unter Buchstabe b bezeichneten Rechte oder Einflussmöglichkeiten haben,
 - d) der Unternehmen, in denen ein unter Buchstabe c genanntes Unternehmen die unter Buchstabe b bezeichneten Rechte oder Einflussmöglichkeiten hat,
 - e) der Unternehmen, in denen mehrere der unter den Buchstaben a bis d genannten Unternehmen jeweils gemeinsam die in Buchstabe b genannten Rechte oder Einflussmöglichkeiten haben.
- (5) Haben beteiligte Unternehmen gemeinsam die in Absatz 4 Buchstabe b bezeichneten Rechte oder Einflussmöglichkeiten, so gilt für die Berechnung des Gesamtumsatzes der beteiligten Unternehmen folgende Regelung:
- a) Zu berücksichtigen sind die Umsätze mit Waren und Dienstleistungen zwischen dem gemeinsamen Unternehmen und jedem dritten Unternehmen; diese Umsätze sind den beteiligten Unternehmen zu gleichen Teilen zuzurechnen.

- b) Nicht zu berücksichtigen sind die Umsätze mit Waren und Dienstleistungen zwischen dem gemeinsamen Unternehmen und jedem der beteiligten Unternehmen oder mit einem Unternehmen, das mit diesen im Sinne des Absatzes 4 Buchstaben b bis e verbunden ist.

Artikel 23

Zusammenrechnung finanzieller Zuwendungen

Der Gesamtbetrag der finanziellen Zuwendungen für ein beteiligtes Unternehmen setzt sich zusammen aus allen finanziellen Zuwendungen, die **Drittstaaten allen** in **Artikel 22** Absatz 2 und Artikel 22 Absatz 4 Buchstaben a bis e genannten Unternehmen **gewährt** haben.

Artikel 24

Aufschub des Vollzugs von Zusammenschlüssen und Fristen

- (1) Ein anmeldepflichtiger Zusammenschluss darf nicht vor seiner Anmeldung vollzogen werden.

Darüber hinaus

- a) darf der Zusammenschluss während eines Zeitraums von 25 Arbeitstagen nach Eingang dieser Anmeldung nicht vollzogen werden, sofern bei der Kommission eine vollständige Anmeldung eingeht.

- b) darf der Zusammenschluss während eines Zeitraums von 90 Arbeitstagen nach Einleitung der eingehenden Prüfung nicht vollzogen werden, sofern die Kommission spätestens 25 Arbeitstage nach Eingang der vollständigen Anmeldung eine eingehende Prüfung einleitet. Diese Frist verlängert sich um 15 Arbeitstage, wenn die beteiligten Unternehmen nach Artikel 7 Verpflichtungszusagen unterbreiten, um die Verzerrung auf dem Binnenmarkt zu beseitigen.
- c) darf **der Zusammenschluss** danach vollzogen werden, nachdem **die Kommission** einen Beschluss nach **Artikel 25** Absatz 3 Buchstabe a oder b **erlassen** hat.

Die unter den Buchstaben a und b genannte Frist beginnt an dem auf den Eingang der vollständigen Anmeldung oder den Erlass des einschlägigen Kommissionsbeschlusses folgenden Arbeitstag.

- (2) Absatz 1 steht der Verwirklichung von Vorgängen nicht entgegen, bei denen die Kontrolle von mehreren Veräußerern entweder im Wege eines öffentlichen Übernahmeangebots oder im Wege einer Reihe von Rechtsgeschäften mit Wertpapieren, einschließlich solchen, die in andere zum Handel an einer Börse oder an einem ähnlichen Markt zugelassene Wertpapiere konvertierbar sind, erworben wird, sofern
 - a) der Zusammenschluss nach **Artikel 21** unverzüglich bei der Kommission angemeldet wird und

- b) der Erwerber die mit den Anteilen verbundenen Stimmrechte nicht ausübt oder nur zur Erhaltung des vollen Wertes seiner Investition aufgrund einer von der Kommission nach Absatz 3 dieses Artikels erteilten Freistellung ausübt.
- (3) Die Kommission kann auf Antrag eine Freistellung von den in Absatz 1 oder 2 bezeichneten Auflagen erteilen. In einem Antrag auf Erteilung einer Freistellung sind die Gründe für diesen Antrag anzugeben. Die Kommission beschließt über den Antrag unter besonderer Berücksichtigung der möglichen Auswirkungen des Aufschubs des Vollzugs auf ein oder mehrere an dem Zusammenschluss beteiligte Unternehmen bzw. auf Dritte sowie des Risikos einer durch den Zusammenschluss bewirkten Verzerrung auf dem Binnenmarkt. Die Freistellung kann an bestimmte Bedingungen und Auflagen geknüpft werden, um auszuschließen, dass es zu Verzerrungen auf dem Binnenmarkt kommt. Sie kann jederzeit, auch vor der Anmeldung oder nach Abschluss des Rechtsgeschäfts, beantragt und erteilt werden.

- (4) Die Fristen nach Absatz 1 Buchstabe b des vorliegenden Artikels verlängern sich, wenn die beteiligten Unternehmen dies spätestens 15 Arbeitstage nach Einleitung der eingehenden Prüfung gemäß Artikel 10 beantragen. Die beteiligten Unternehmen dürfen eine solche Fristverlängerung nur einmal beantragen.

Die Kommission kann die Fristen nach Absatz 1 Buchstabe b des vorliegenden Artikels jederzeit nach Einleitung der eingehenden Prüfung mit Zustimmung der beteiligten Unternehmen verlängern.

Die Gesamtdauer aller etwaigen Fristverlängerungen nach diesem Absatz darf 20 Arbeitstage nicht übersteigen.

- (5) Die Kommission kann die Fristen nach Absatz 1 ausnahmsweise aussetzen, wenn die Unternehmen die von ihr nach **Artikel 13** angeforderten Auskünfte nicht vollständig erteilt haben oder sich weigern, eine durch Beschluss nach **Artikel 14** angeordnete Nachprüfung zu dulden.

- (6) Die Kommission kann einen Beschluss nach **Artikel 25** Absatz 3 erlassen, ohne an die in den Absätzen 1 und 4 des vorliegenden Artikels genannten Fristen gebunden zu sein, wenn
- a) sie feststellt, dass ein Zusammenschluss unter Verstoß gegen die Verpflichtungen vollzogen wurde, die mit einem nach **Artikel 25** Absatz 3 Buchstabe a erlassenen Beschluss verbunden sind, **■** oder
 - b) ein Beschluss nach **Artikel 25** Absatz 1 aufgehoben wurde.
- (7) Jedes unter Verstoß gegen Absatz 1 vollzogene Rechtsgeschäft gilt erst nach Erlass eines Beschlusses nach **Artikel 25** Absatz 3 als gültig.
- (8) Dieser Artikel berührt nicht die Wirksamkeit von Rechtsgeschäften mit Wertpapieren, einschließlich solcher, die in andere zum Handel an einer Börse oder an einem ähnlichen Markt zugelassene Wertpapiere konvertierbar sind, es sei denn, dass den Veräußerern und Erwerbern bewusst war oder bewusst hätte sein müssen, dass das betreffende Rechtsgeschäft unter Verstoß gegen Absatz 1 vollzogen wurde.

Artikel 25

Verfahrensvorschriften für die Vorprüfung und die eingehende Prüfung angemeldeter Zusammenschlüsse

- (1) **Artikel 10, Artikel 11** Absätze 1, 3 und 4 sowie die **Artikel 12 bis 16 und 18** gelten für angemeldete Zusammenschlüsse.
- (2) Die Kommission kann spätestens 25 Arbeitstage nach Eingang einer vollständigen Anmeldung eine eingehende Prüfung nach **Artikel 10 Absatz 3** einleiten.
- (3) Im Anschluss an die eingehende Prüfung erlässt die Kommission einen **Durchführungsrechtsakt in Form eines** der folgenden Beschlüsse:
 - a) einen Verpflichtungsbeschluss nach **Artikel 11** Absatz 3,
 - b) einen Beschluss, keine Einwände zu erheben, nach **Artikel 11** Absatz 4, oder

- c) einen Beschluss zur Untersagung eines Zusammenschlusses, wenn die Kommission feststellt, dass eine drittstaatliche Subvention den Binnenmarkt nach den Artikeln 4 bis 6 verzerrt.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

- (4) Beschlüsse nach Absatz 3 werden innerhalb von 90 Arbeitstagen nach Einleitung der eingehenden Prüfung erlassen; diese Frist kann gegebenenfalls nach **Artikel 24** Absatz 1 Buchstabe b, Absatz 4 und Absatz 5 verlängert werden. Hat die Kommission bei Fristablauf noch keinen Beschluss erlassen, so dürfen die beteiligten Unternehmen den Zusammenschluss vollziehen.
- (5) In jedem Auskunftsverlangen an ein Unternehmen gibt die Kommission an, ob die Fristen nach **Artikel 24** Absatz 5 ausgesetzt werden, falls das Unternehmen nicht innerhalb der gesetzten Frist vollständige Auskünfte erteilt.

- (6) Wenn die Kommission feststellt, dass ein Zusammenschluss, der ***nach Artikel 21 Absatz 1 anmeldepflichtig ist oder nach Artikel 21 Absatz 5 auf Aufforderung der Kommission angemeldet wurde***, bereits vollzogen worden ist ***und dass die drittstaatlichen Subventionen im Zusammenhang mit diesem Zusammenschluss den Binnenmarkt gemäß den Artikeln 4, 5 und 6 verzerren***, kann sie eine der folgenden Maßnahmen ergreifen:
- a) Sie kann den beteiligten Unternehmen aufgeben, den Zusammenschluss rückgängig zu machen, insbesondere durch die Auflösung der Fusion oder die Veräußerung aller erworbenen Anteile oder Vermögenswerte, um den Zustand vor dem Vollzug des Zusammenschlusses wiederherzustellen, oder, wenn die Wiederherstellung durch Rückgängigmachung des Zusammenschlusses nicht möglich ist, jede andere geeignete Maßnahme treffen, um diesen Zustand soweit wie möglich wiederherzustellen.
 - b) Sie kann jede andere geeignete Maßnahme anordnen, um sicherzustellen, dass die beteiligten Unternehmen den Zusammenschluss rückgängig machen oder andere Maßnahmen zur Wiederherstellung des früheren Zustands nach Maßgabe ihres Beschlusses ergreifen.

Die Kommission kann die unter den Buchstaben a und b des vorliegenden Absatzes genannten Maßnahmen entweder durch einen Beschluss nach Absatz 3 Buchstabe c dieses Artikels oder durch einen gesonderten Beschluss auferlegen.

Die Kommission kann mittels **eines Durchführungsrechtsakts in Form eines Beschlusses über eine** der unter den Buchstaben a und b des vorliegenden Absatzes genannten Maßnahmen ergreifen, wenn sie feststellt, dass ein Zusammenschluss unter Verstoß gegen einen Beschluss nach Absatz 3 Buchstabe a des vorliegenden Artikels, in dem festgestellt wurde, dass der Zusammenschluss ohne die Verpflichtungen das Kriterium des Absatzes 3 Buchstabe c des vorliegenden Artikels erfüllen würde, vollzogen wurde.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

- (7) Die Kommission kann auch **einen Durchführungsrechtsakt in Form eines Beschlusses zur Anordnung** einstweiliger Maßnahmen nach **Artikel 12 erlassen**, wenn
- a) ein Zusammenschluss unter Verstoß gegen **Artikel 21** vollzogen wurde,

- b) ein Zusammenschluss unter Verstoß gegen einen Verpflichtungsbeschluss nach Absatz 3 Buchstabe a des vorliegenden Artikels vollzogen wurde.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.

Artikel 26

Geldbußen und Zwangsgelder bei Zusammenschlüssen

- (1) Die Kommission kann Geldbußen oder Zwangsgelder nach **Artikel 17** verhängen.
- (2) Die Kommission kann durch Beschluss gegen die beteiligten Unternehmen auch Geldbußen von höchstens 1 % ihres im vorangegangenen Geschäftsjahr erzielten Gesamtumsatzes verhängen, wenn diese Unternehmen in einer Anmeldung nach **Artikel 21** oder in einer Ergänzung einer solchen Anmeldung vorsätzlich oder fahrlässig unrichtige oder irreführende Angaben gemacht haben.

- (3) **Die Kommission kann durch Beschluss gegen die beteiligten Unternehmen auch Geldbußen von höchstens 10 % ihres im vorangegangenen Geschäftsjahr erzielten Gesamtumsatzes verhängen, wenn diese Unternehmen vorsätzlich oder fahrlässig**
- a) **einen anmeldepflichtigen Zusammenschluss vor seinem Vollzug nicht nach *Artikel 21* anmelden, es sei denn, dies ist nach *Artikel 24* ausdrücklich zulässig,**
 - b) **einen angemeldeten Zusammenschluss unter Verstoß gegen *Artikel 24* vollziehen,**
 - c) **einen angemeldeten Zusammenschluss vollziehen, der nach *Artikel 25* Absatz 3 Buchstabe c untersagt wurde,**
 - d) ***die Anmeldepflichten nach Artikel 39 Absatz 3 umgangen haben oder versucht haben, diese zu umgehen.***

Kapitel 4

Öffentliche Vergabeverfahren

Artikel 27

Verzerrungen auf dem Binnenmarkt durch den Binnenmarkt verzerrende drittstaatliche Subventionen im Rahmen öffentlicher Vergabeverfahren

Als drittstaatliche Subventionen, die ein öffentliches Vergabeverfahren verzerren oder zu verzerren drohen, sind **drittstaatliche** Subventionen ■ zu verstehen, die **einen Wirtschaftsteilnehmer** in die Lage versetzen, ein in Bezug auf die betreffenden Bauleistungen, Lieferungen oder Dienstleistungen ungerechtfertigt günstiges Angebot einzureichen. Die Beurteilung nach Artikel 4, ob eine Verzerrung auf dem Binnenmarkt vorliegt und ob ein Angebot in Bezug auf die betreffenden Bauleistungen, Lieferungen oder Dienstleistungen ungerechtfertigt günstig ist, beschränkt sich auf das jeweilige öffentliche Vergabeverfahren. Bei der Beurteilung werden nur drittstaatliche Subventionen berücksichtigt, die in den drei Jahren vor der Meldung gewährt wurden.

Artikel 28

Schwellenwerte für die Meldung in öffentlichen Vergabeverfahren

- (1) Für die Zwecke **dieser Verordnung** liegt eine meldepflichtige drittstaatliche finanzielle Zuwendung im Rahmen eines öffentlichen Vergabeverfahrens vor, wenn
- a) der geschätzte Wert des Auftrags **oder der Rahmenvereinbarung ohne Mehrwertsteuer, der gemäß den Bestimmungen von Artikel 8 der Richtlinie 2014/23/EU, Artikel 5 der Richtlinie 2014/24/EU und Artikel 16 der Richtlinie 2014/25/EU berechnet wird, oder einer einzelnen Auftragsvergabe über das dynamische Beschaffungssystem** mindestens 250 Mio. EUR beträgt **und**
 - b) **dem Wirtschaftsteilnehmer, einschließlich seiner wirtschaftlich unselbständigen Tochtergesellschaften, seiner Beteiligungsgesellschaften und gegebenenfalls seiner Hauptunterauftragnehmer und Hauptlieferanten, die an demselben Angebot im Rahmen des öffentlichen Vergabeverfahrens beteiligt sind, in den drei Jahren vor der Meldung oder gegebenenfalls der aktualisierten Meldung finanzielle Zuwendungen von insgesamt mindestens 4 Mio. EUR pro Drittstaat gewährt wurden.**

- (2) *Beschließt der öffentliche Auftraggeber bzw. der Auftraggeber, den Auftrag in Lose zu unterteilen, so liegt eine meldepflichtige drittstaatliche finanzielle Zuwendung im Rahmen eines öffentlichen Vergabeverfahrens vor, wenn der geschätzte Wert des Auftrags ohne Mehrwertsteuer den in Absatz 1 Buchstabe a genannten Schwellenwert übersteigt und der Wert des Loses oder der Gesamtwert aller Lose, um die sich der Bieter bewirbt, mindestens 125 Mio. EUR beträgt und die drittstaatliche finanzielle Zuwendung mindestens dem in Absatz 1 Buchstabe b genannten Schwellenwert entspricht.*
- (3) Dieses Kapitel gilt nicht für Verfahren zur Vergabe von Aufträgen, die in den Anwendungsbereich der Richtlinie 2009/81/EG  fallen.
- (4) *Die Verfahren zur Vergabe von Aufträgen nach Artikel 32 Absatz 2 Buchstabe c der Richtlinie 2014/24/EU und Artikel 50 Buchstabe d der Richtlinie 2014/25/EU fallen unter die Bestimmungen von Kapitel 2 dieser Verordnung und sind von der Anwendung von Kapitel 4 dieser Verordnung ausgenommen.*

- (5) *Können die Bauleistungen, Lieferungen oder Dienstleistungen gemäß Artikel 31 Absatz 4 der Richtlinie 2014/23/EU, Artikel 32 Absatz 2 Buchstabe b der Richtlinie 2014/24/EU und Artikel 50 Buchstabe c der Richtlinie 2014/25/EU nur von einem bestimmten Wirtschaftsteilnehmer erbracht bzw. bereitgestellt werden und beträgt der geschätzte Wert des Auftrags mindestens den in Absatz 1 Buchstabe a des vorliegenden Artikels festgelegten Wert, so informieren die Wirtschaftsteilnehmer, die ein Angebot oder einen Teilnahmeantrag einreichen, abweichend von Artikel 29 Absatz 1 die Kommission über alle drittstaatlichen finanziellen Zuwendungen, sofern die Bedingung gemäß Absatz 1 Buchstabe b des vorliegenden Artikels erfüllt ist. Unbeschadet der Möglichkeit zur Einleitung einer Prüfung nach Kapitel 2 der vorliegenden Verordnung gilt die Übermittlung solcher Informationen nicht als Meldung und ist nicht Gegenstand von Prüfungen nach dem vorliegenden Kapitel.*

- (6) *Die öffentlichen Auftraggeber bzw. die Auftraggeber geben in der Auftragsbekanntmachung oder – im Fall eines Verfahrens ohne vorherige Bekanntmachung – in den Auftragsunterlagen an, dass die Wirtschaftsteilnehmer der Meldepflicht nach Artikel 29 unterliegen. Das Fehlen einer solchen Erklärung berührt jedoch nicht die Anwendung dieser Verordnung auf Aufträge, die in ihren Anwendungsbereich fallen.*

Artikel 29

Vorherige Meldung oder Erklärung drittstaatlicher finanzieller Zuwendungen im
Zusammenhang mit öffentlichen Vergabeverfahren

- (1) ***Sind die Bedingungen für die Meldung finanzieller Zuwendungen gemäß Artikel 28 Absätze 1 und 2 erfüllt, so melden die Wirtschaftsteilnehmer, die an einem öffentlichen Vergabeverfahren teilnehmen, dem öffentlichen Auftraggeber bzw. dem Auftraggeber alle drittstaatlichen finanziellen Zuwendungen nach Artikel 28 Absatz 1 Buchstabe b. In allen anderen Fällen führen die Wirtschaftsteilnehmerin einer Erklärung alle erhaltenen drittstaatlichen finanziellen Zuwendungen auf und bestätigen, dass die erhaltenen drittstaatlichen finanziellen Zuwendungen keiner Meldepflicht nach Artikel 28 Absatz 1 Buchstabe b unterliegen. Bei einem offenen Verfahren ist die Meldung oder die Erklärung nur einmal gemeinsam mit dem Angebot einzureichen. Bei einem Verfahren mit mehreren Phasen ist die Meldung oder die Erklärung zweimal einzureichen, zunächst zusammen mit dem Teilnahmeantrag und danach als aktualisierte Meldung oder aktualisierte Erklärung zusammen mit dem eingereichten Angebot oder dem endgültigen Angebot.***

- (2) *Sobald die Meldung oder die Erklärung eingereicht wurde, leitet der öffentliche Auftraggeber bzw. der Auftraggeber die Meldung oder die Erklärung unverzüglich an die Kommission weiter.*
- (3) *Fehlt eine Meldung oder Erklärung im Teilnahmeantrag oder im Angebot, so kann der öffentliche Auftraggeber bzw. der Auftraggeber die betreffenden Wirtschaftsteilnehmer auffordern, das entsprechende Dokument innerhalb von zehn Arbeitstagen vorzulegen. Angebote oder Teilnahmeanträge von Wirtschaftsteilnehmern, die den Bedingungen dieses Artikels unterliegen und denen trotz einer Aufforderung des öffentlichen Auftraggebers bzw. des Auftraggebers nach dem vorliegenden Absatz letztlich keine Meldung oder Erklärung gemäß Absatz 1 beigefügt wird, werden vom öffentlichen Auftraggeber bzw. dem Auftraggeber für nicht ordnungsgemäß erklärt und abgelehnt. Der öffentliche Auftraggeber bzw. der Auftraggeber informiert die Kommission über diese Ablehnung.*

- (4) *Die Kommission prüft den Inhalt der eingegangenen Meldung unverzüglich. Stellt die Kommission fest, dass die Meldung unvollständig ist, so teilt sie dem öffentlichen Auftraggeber bzw. dem Auftraggeber und dem betreffenden Wirtschaftsteilnehmer ihre Feststellungen mit und fordert den Wirtschaftsteilnehmer auf, die Meldung innerhalb von zehn Arbeitstagen zu vervollständigen. Ist eine Meldung, die einem Angebot oder einem Teilnahmeantrag beigefügt ist, trotz einer Aufforderung der Kommission gemäß diesem Absatz weiterhin unvollständig, so erlässt die Kommission einen Beschluss, mit dem das Angebot für nicht ordnungsgemäß erklärt wird. In diesem Beschluss fordert die Kommission auch den öffentlichen Auftraggeber bzw. den Auftraggeber auf, eine Entscheidung zur Ablehnung eines solchen nicht ordnungsgemäßen Angebots oder Teilnahmeantrags zu treffen.*
- (5) Die Pflicht zur vorherigen Meldung drittstaatlicher finanzieller Zuwendungen nach diesem Artikel gilt für Wirtschaftsteilnehmer, Gruppen von Wirtschaftsteilnehmern nach Artikel 26 Absatz 2 der Richtlinie 2014/23/EU, Artikel 19 Absatz 2 der Richtlinie 2014/24/EU und Artikel 37 Absatz 2 der Richtlinie 2014/25/EU sowie für die Hauptunterauftragnehmer und die Hauptlieferanten, **die zum Zeitpunkt der Einreichung der vollständigen Meldung oder Erklärung bzw. der vollständigen aktualisierten Meldung oder Erklärung bekannt sind.** Für die Zwecke dieser Verordnung gilt ein Unterauftragnehmer oder Lieferant als Hauptunterauftragnehmer oder Hauptlieferant, wenn seine Teilnahme wesentliche Elemente der Auftragserfüllung gewährleistet bzw. immer dann, wenn der wirtschaftliche Anteil seines Beitrags 20 % des **Werts des eingereichten Angebots** übersteigt.

- (6) *Der Hauptauftragnehmer im Sinne der Richtlinien 2014/24/EU und 2014/25/EU oder der Konzessionsnehmer im Sinne der Richtlinie 2014/23/EU stellt im Namen von Gruppen von Wirtschaftsteilnehmern, den Hauptunterauftragnehmern und den Hauptlieferanten sicher, dass die Meldung oder die Erklärung eingereicht wird. Für die Zwecke des Artikels 33 ist der Hauptauftragnehmer oder Konzessionsnehmer nur für die Richtigkeit der Daten im Zusammenhang mit seinen eigenen drittstaatlichen finanziellen Zuwendungen verantwortlich.*
- (7) *Vermutet der öffentliche Auftraggeber bzw. der Auftraggeber bei der Prüfung von Angeboten, dass drittstaatliche Subventionen vorliegen, obwohl eine Erklärung eingereicht wurde, so teilt er der Kommission unverzüglich seine Vermutungen mit. Unbeschadet der in den Richtlinien 2014/24/EU und 2014/25/EU festgelegten Befugnisse der öffentlichen Auftraggeber bzw. der Auftraggeber zu überprüfen, ob ein Angebot ungewöhnlich niedrig ist, nimmt der öffentliche Auftraggeber bzw. der Auftraggeber keine Beurteilung dessen vor, ob ein Angebot ungewöhnlich niedrig ist, wenn diese Beurteilung nur aufgrund der Vermutung des Vorliegens drittstaatlicher Subventionen eingeleitet würde. Gelangt die Kommission zu dem Schluss, dass kein ungerechtfertigt günstiges Angebot im Sinne dieser Verordnung vorliegt, so informiert sie den betreffenden öffentlichen Auftraggeber bzw. den betreffenden Auftraggeber. Sonstige natürliche oder juristische Personen können der Kommission alle Informationen im Zusammenhang mit den Binnenmarkt verzerrenden drittstaatlichen Subventionen melden und jede Vermutung einer möglichen falschen Erklärung mitteilen.*

- (8) Wenn die Kommission vermutet, dass ein Wirtschaftsteilnehmer in den drei Jahren vor Einreichung des Angebots oder des Antrags auf Teilnahme am öffentlichen Vergabeverfahren möglicherweise von drittstaatlichen **Subventionen** profitiert hat, **■** kann sie – **unbeschadet ihrer Möglichkeit, ein Verfahren von Amts wegen einzuleiten** – vor Vergabe des Auftrags die Meldung der drittstaatlichen finanziellen Zuwendungen verlangen, die der **Wirtschaftsteilnehmer** im Rahmen öffentlicher Vergabeverfahren von **Drittstaaten** erhalten hat und die nicht nach **Artikel 28 Absatz 1** meldepflichtig sind oder **■** in den Anwendungsbereich von **Artikel 30 Absatz 4** fallen. **Wenn** die Kommission die Meldung einer solchen drittstaatlichen finanziellen Zuwendung verlangt hat, gilt diese finanzielle Zuwendung als meldepflichtige drittstaatliche finanzielle Zuwendung im Rahmen eines öffentlichen Vergabeverfahrens **und unterliegt den Bestimmungen des Kapitels 4.**

Artikel 30

Verfahrensvorschriften für die Vorprüfung und die eingehende Prüfung gemeldeter finanzieller Zuwendungen im Rahmen öffentlicher Vergabeverfahren

- (1) **Artikel 10, Artikel 11** Absätze 1, 3 und 4 sowie die **Artikel 13, 14, 15, 16, 18 und 23** gelten für gemeldete finanzielle Zuwendungen im Rahmen öffentlicher Vergabeverfahren.
- (2) Die Kommission führt spätestens **20 Arbeitstage** nach Eingang einer **vollständigen** Meldung eine Vorprüfung durch. **In hinreichend begründeten Fällen kann die Kommission diese Frist einmal um zehn Arbeitstage verlängern.**
- (3) Die Kommission entscheidet vor Ablauf der Frist für den Abschluss der Vorprüfung über die Einleitung einer eingehenden Prüfung und unterrichtet den betreffenden Wirtschaftsteilnehmer und den öffentlichen Auftraggeber bzw. den Auftraggeber unverzüglich entsprechend.

- (4) *Wenn die Kommission eine Vorprüfung abgeschlossen hat, ohne einen Beschluss zu erlassen, und neue Informationen erhält, die den Verdacht begründen, dass eine eingereichte Meldung oder Erklärung unvollständig war, oder wenn eine solche Meldung oder Erklärung nicht an die Kommission weitergeleitet wird, kann sie im Einklang mit Artikel 29 Absatz 4 zusätzliche Informationen verlangen. Die Kommission kann auf der Grundlage dieser neuen Informationen eine Vorprüfung wieder aufnehmen. Wird unbeschadet der Möglichkeit, gegebenenfalls eine Vorprüfung gemäß Kapitel 2 einzuleiten, eine Vorprüfung gemäß dem vorliegenden Kapitel eingeleitet, so entspricht der Beginn für die Festlegung der Dauer der Vorprüfung dem Zeitpunkt, an dem die neue Meldung oder Erklärung bei der Kommission eingegangen ist.*
- (5) Die Kommission kann einen Beschluss zum Abschluss der eingehenden Prüfung bis spätestens **110 Arbeitstage** nach Eingang einer **vollständigen** Meldung erlassen. *In hinreichend begründeten Ausnahmefällen, einschließlich der in Absatz 6 genannten Prüfungen oder der in Artikel 16 Absatz 1 Buchstaben a und b genannten Fälle, kann dieser Zeitraum* nach Konsultation des  öffentlichen Auftraggebers bzw. des Auftraggebers **einmalig um 20 Arbeitstage** verlängert werden.

- (6) *Handelt es sich bei dem öffentlichen Vergabeverfahren um ein Verfahren mit mehreren Phasen, so prüft die Kommission abweichend von Absatz 2 die zusammen mit dem Teilnahmeantrag eingereichte vollständige Meldung innerhalb von 20 Arbeitstagen nach Eingang der Meldung, ohne die Vorprüfung abzuschließen oder einen Beschluss zur Einleitung einer eingehenden Prüfung zu fassen. Nach dem Ablauf der Frist von 20 Arbeitstagen wird die Vorprüfung ausgesetzt, bis ein endgültiges Angebot oder im Fall eines nichtoffenen Verfahrens ein Angebot eingereicht wird. Sobald das Angebot oder das endgültige Angebot mit einer vollständigen aktualisierten Meldung eingereicht worden ist, wird die Vorprüfung fortgesetzt und die Kommission verfügt über eine Frist von 20 Arbeitstagen, um sie unter Berücksichtigung etwaiger zusätzlicher Informationen abzuschließen. Die Kommission erlässt innerhalb von 90 Arbeitstagen nach Übermittlung der vollständigen aktualisierten Meldung einen Beschluss über den Abschluss etwaiger nachfolgender eingehender Prüfungen.*

Artikel 31

Beschlüsse der Kommission

- (1) Stellt die Kommission nach einer eingehenden Prüfung fest, dass ein Wirtschaftsteilnehmer von einer drittstaatlichen Subvention profitiert, die nach den Artikeln 4, 5 und 6 den Binnenmarkt verzerrt, und bietet das betreffende Wirtschaftsteilnehmer Verpflichtungen an, die die Verzerrung auf dem Binnenmarkt vollständig und wirksam beseitigen, erlässt sie **einen Durchführungsrechtsakt in Form** eines Verpflichtungsbeschlusses nach **Artikel 11** Absatz 3. **Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.**
- (2) Bietet der betreffende Wirtschaftsteilnehmer keine Verpflichtungen an oder ist die Kommission der Auffassung, dass die in Absatz 1 genannten Verpflichtungen weder geeignet noch hinreichend sind, um die Verzerrung vollständig und wirksam zu beseitigen, so erlässt die Kommission einen **Durchführungsrechtsakt in Form** eines Beschlusses, mit dem die Vergabe des Auftrags an den betreffenden Wirtschaftsteilnehmer untersagt wird („Beschluss zur Untersagung der Zuschlagserteilung“). **Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen. Infolge dieses Beschlusses lehnt der öffentliche Auftraggeber bzw. der Auftraggeber das Angebot ab.**

- (3) Stellt die Kommission nach einer eingehenden Prüfung nicht fest, dass ein Wirtschaftsteilnehmer von einer den Binnenmarkt verzerrenden drittstaatlichen Subvention profitiert, so erlässt sie einen **Durchführungsrechtsakt in der Form eines** Beschlusses nach **Artikel 11** Absatz 4. **Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 48 Absatz 2 genannten Beratungsverfahren erlassen.**
- (4) Die Beurteilung nach Artikel 6 darf nicht zu einer mit dem Unionsrecht unvereinbaren Änderung des ■ von dem **Wirtschaftsteilnehmer** eingereichten Angebots **oder endgültigen Angebots** führen.

Artikel 32

Angebotsbewertungen im Rahmen öffentlicher Vergabeverfahren mit Meldung und Vergabeaussetzung

- (1) Während der Vorprüfung und der eingehenden Prüfung **können alle Verfahrensschritte** im Rahmen **des** öffentlichen Vergabeverfahrens **mit Ausnahme der** Zuschlagserteilung fortgesetzt werden.
- (2) Beschließt die Kommission die Einleitung einer eingehenden Prüfung nach **Artikel 30** Absatz 3, so darf der Auftrag erst dann an einen **Wirtschaftsteilnehmer**, der eine Meldung nach **Artikel 29** eingereicht hat, vergeben werden, wenn die Kommission einen Beschluss nach **Artikel 31** Absatz 3 gefasst hat oder die **Fristen** nach **Artikel 30 Absatz 5 oder 6** verstrichen sind. Hat die Kommission **innerhalb der geltenden Frist** keinen Beschluss erlassen, so darf der Auftrag an jeden **Wirtschaftsteilnehmer** vergeben werden, auch an den Wirtschaftsteilnehmer, der eine Meldung eingereicht hat.

- (3) *Wenn der öffentliche Auftraggeber bzw. der Auftraggeber feststellt, dass das wirtschaftlich günstigste Angebot von einem Wirtschaftsteilnehmer abgegeben wurde, der eine Erklärung gemäß Artikel 29 eingereicht hat, und wenn die Kommission keine Prüfung im Einklang mit Artikel 29 Absatz 8, Artikel 30 Absatz 3 oder Artikel 30 Absatz 4 eingeleitet hat, kann der Auftrag an den Wirtschaftsteilnehmer vergeben werden, der ein solches Angebot abgegeben hat, bevor die Kommission einen der Beschlüsse nach Artikel 31 erlassen hat, die Fristen nach Artikel 30 Absatz 2, Artikel 30 Absatz 5 oder Artikel 30 Absatz 6 verstrichen sind oder die Kommission einen der Beschlüsse nach Artikel 31 in Bezug auf andere Angebote, die Gegenstand einer Prüfung sind, erlassen hat.*
- (4) Erlässt die Kommission in Bezug auf das *Angebot, das nach Auffassung des öffentlichen Auftraggebers bzw. des Auftraggebers das wirtschaftlich günstigste Angebot ist*, einen Beschluss nach **Artikel 31** Absatz 2, so darf der Auftrag an den *Wirtschaftsteilnehmer* vergeben werden, der nicht Gegenstand eines Beschlusses nach **Artikel 31** Absatz 2 ist und das nächstbeste Angebot abgegeben hat.

- (5) Erlässt die Kommission einen Beschluss nach **Artikel 31** Absatz 1 oder 3, so darf der Auftrag an jeden **Wirtschaftsteilnehmer** vergeben werden, der das wirtschaftlich günstigste Angebot abgegeben hat, einschließlich an den Wirtschaftsteilnehmer, der eine Meldung nach **Artikel 29** eingereicht hat.
- (6) **Der** öffentliche Auftraggeber bzw. der Auftraggeber unterrichtet die Kommission **unverzüglich** über jeden Beschluss im Zusammenhang mit **der Beendigung des öffentlichen Vergabeverfahrens, der Ablehnung des Angebots oder des Teilnahmeantrags des betreffenden Wirtschaftsteilnehmers, der Vorlage eines neuen Angebots des betreffenden Wirtschaftsteilnehmers oder der Vergabe des Auftrags**.

- (7) Die für die öffentlichen **Vergabeverfahren** geltenden Grundsätze, einschließlich der Grundsätze der Verhältnismäßigkeit, Nichtdiskriminierung, Gleichbehandlung, Transparenz **und Wettbewerb**, werden in Bezug auf alle an dem öffentlichen Vergabeverfahren beteiligten **Wirtschaftsteilnehmer** eingehalten. Die Prüfung drittstaatlicher Subventionen nach dieser Verordnung darf nicht dazu führen, dass der öffentliche Auftraggeber bzw. der Auftraggeber den betreffenden **Wirtschaftsteilnehmer** in einer gegen diese Grundsätze verstoßenden Weise behandelt. **Umwelt-, sozial- und arbeitsrechtliche Vorschriften gelten für Wirtschaftsteilnehmer gemäß den Richtlinien 2014/23/EU, 2014/24/EU und 2014/25/EU sowie anderem Unionsrecht.**
- (8) Jede Frist beginnt an dem auf den Eingang der Meldung bzw. den Erlass des einschlägigen Kommissionsbeschlusses folgenden Arbeitstag.

Artikel 33

Geldbußen und Zwangsgelder bei finanziellen Zuwendungen im Zusammenhang mit öffentlichen Vergabeverfahren

- (1) Die Kommission kann Geldbußen oder Zwangsgelder nach **Artikel 17** verhängen.

- (2) Die Kommission kann durch Beschluss gegen die betreffenden **Wirtschaftsteilnehmer** auch Geldbußen von höchstens 1 % ihres im vorangegangenen Geschäftsjahr erzielten Gesamtumsatzes verhängen, wenn diese **Wirtschaftsteilnehmer** in einer Meldung oder Erklärung nach **Artikel 29** oder in einer Ergänzung zu einer solchen Meldung oder Erklärung vorsätzlich oder fahrlässig unrichtige oder irreführende Angaben gemacht haben.
- (3) Die Kommission kann durch Beschluss gegen die beteiligten **Wirtschaftsteilnehmer** Geldbußen von höchstens 10 % ihres im vorangegangenen Geschäftsjahr erzielten Gesamtumsatzes verhängen, wenn **diese** Wirtschaftsteilnehmer vorsätzlich oder fahrlässig
- a) **eine drittstaatliche finanzielle Zuwendung** während des öffentlichen Vergabeverfahrens nach **Artikel 29 nicht gemeldet haben,**
 - b) **die Meldepflichten nach Artikel 39 Absatz 3 umgangen haben oder versucht haben, diese zu umgehen.**

Kapitel 5
Gemeinsame Verfahrensvorschriften

Artikel 34

Verhältnis zwischen Verfahren

- (1) Eine finanzielle Zuwendung, die im Zusammenhang mit einem Zusammenschluss nach **Artikel 21 oder einem öffentlichen Vergabeverfahren nach Artikel 29 angemeldet bzw.** gemeldet wird, kann auch in Bezug auf eine andere wirtschaftliche Tätigkeit relevant sein und im Rahmen dieser Verordnung darauf geprüft werden.
- (2) *Eine finanzielle Zuwendung, die im Zusammenhang mit einem Verfahren von Amts wegen nach Artikel 10 oder Artikel 11 in Bezug auf eine bestimmte wirtschaftliche Tätigkeit geprüft wird, kann auch in Bezug auf eine andere wirtschaftliche Tätigkeit relevant sein und im Rahmen dieser Verordnung darauf geprüft werden.*

Artikel 35

Übermittlung von Informationen

- (1) *Ist ein Mitgliedstaat der Auffassung, dass eine drittstaatliche Subvention vorliegt und den Binnenmarkt verzerren könnte, so übermittelt er diese Informationen der Kommission. Die Kommission kann auf der Grundlage dieser Informationen beschließen, eine Vorprüfung nach Artikel 10 einzuleiten oder eine Anmeldung nach Artikel 21 Absatz 5 bzw. eine Meldung nach Artikel 29 Absatz 8 verlangen.*

- (2) *Natürliche oder juristische Personen oder Vereinigungen können der Kommission alle ihnen zur Verfügung stehenden Informationen über drittstaatliche Subventionen, die den Binnenmarkt verzerren könnten, übermitteln. Die Kommission kann auf der Grundlage dieser Informationen beschließen, eine Vorprüfung nach Artikel 10 einzuleiten oder eine Anmeldung nach Artikel 21 Absatz 5 bzw. eine Meldung nach Artikel 29 Absatz 8 verlangen.*
- (3) *Die Kommission macht den Mitgliedstaaten und den betreffenden öffentlichen Auftraggebern bzw. den betreffenden Auftraggebern in einer eigens dafür eingerichteten Datenbank die nichtvertraulichen Fassungen aller gemäß dieser Verordnung erlassenen Beschlüsse zugänglich.*

Artikel 36

Marktuntersuchung

- (1) Wenn aufgrund der der Kommission vorliegenden Informationen ein begründeter Verdacht besteht, dass drittstaatliche Subventionen in einem bestimmten Wirtschaftszweig, für eine bestimmte Art von Wirtschaftstätigkeit oder auf der Grundlage eines bestimmten Subventionsinstruments den Binnenmarkt verzerren könnten, kann die Kommission in Bezug auf den betreffenden Wirtschaftszweig, die bestimmte Art der Wirtschaftstätigkeit oder den Einsatz des betreffenden Subventionsinstruments eine Marktuntersuchung durchführen. Im Rahmen dieser Marktuntersuchung kann die Kommission von den betreffenden Unternehmen oder Unternehmensvereinigungen die notwendigen Auskünfte verlangen und die notwendigen Nachprüfungen vornehmen. Die Kommission kann auch Auskunftsverlangen an die betreffenden **Mitgliedstaaten** oder **den** betreffenden Drittstaat richten.
- (2) Die Kommission **veröffentlicht gegebenenfalls** einen Bericht über die Ergebnisse ihrer Marktuntersuchung in Bezug auf bestimmte Wirtschaftszweige, bestimmte Arten von Wirtschaftstätigkeiten oder bestimmte Subventionsinstrumente **■** und **holt Stellungnahmen ein**.
- (3) Die Kommission kann die über solche Marktuntersuchungen erlangten Informationen im Rahmen von Verfahren nach dieser Verordnung verwenden.
- (4) Die **Artikel 13, 14, 15 und 17** finden Anwendung.

Artikel 37

Dialog mit Drittstaaten

- (1) Wenn die Kommission im Anschluss an eine Marktuntersuchung nach Artikel 36 das Vorliegen wiederholter den Binnenmarkt verzerrender drittstaatlicher Subventionen vermutet oder wenn bei mehreren Durchsetzungsmaßnahmen im Rahmen dieser Verordnung den Binnenmarkt verzerrende drittstaatliche Subventionen desselben Drittstaats festgestellt werden, kann die Kommission einen Dialog mit dem betreffenden Drittstaat aufnehmen, um Optionen zu sondieren, die auf die Einstellung oder Änderung dieser Subventionen abzielen, um deren verzerrende Auswirkungen auf den Binnenmarkt zu beseitigen. Die Kommission unterrichtet das Europäische Parlament und den Rat von allen einschlägigen Entwicklungen.*
- (2) Der Dialog mit dem Drittstaat hindert die Kommission nicht daran, nach dieser Verordnung tätig zu werden. Im Rahmen dieser Verordnung angenommene Einzelmaßnahmen werden in dem Dialog nicht behandelt.*

Artikel 38

Verjährungsfristen

- (1) Für die Befugnisse der Kommission nach den **Artikeln 10 und 11** gilt eine Verjährungsfrist von zehn Jahren ab dem Tag, an dem einem  Unternehmen eine drittstaatliche Subvention gewährt wurde. Jede Maßnahme der Kommission nach **Artikel 10, 13, 14 oder 15** in Bezug auf eine drittstaatliche Subvention führt zur Unterbrechung der Verjährungsfrist. Nach jeder Unterbrechung beginnt die Verjährungsfrist von zehn Jahren erneut.
- (2) Für die Befugnisse der Kommission zur Verhängung von Geldbußen oder Zwangsgeldern nach den **Artikeln 17, 26 und 33** gilt eine Verjährungsfrist von drei Jahren ab dem Tag, an dem die Zuwiderhandlung nach **Artikel 17, 26 oder 33** stattgefunden hat. Bei fortgesetzten oder wiederholten Zuwiderhandlungen beginnt die Frist an dem Tag, an dem die Zuwiderhandlung eingestellt wird. Jede Maßnahme, die die Kommission in Bezug auf eine Zuwiderhandlung nach **Artikel 17, 26 oder 33** ergreift, führt zur Unterbrechung der Verjährungsfrist für die Verhängung von Geldbußen bzw. Zwangsgeldern. Nach jeder Unterbrechung beginnt die Verjährungsfrist von drei Jahren erneut.

- (3) Für die Befugnisse der Kommission, Beschlüsse zur Verhängung von Geldbußen oder Zwangsgeldern nach **den Artikeln 17, 26 und 33** durchzusetzen, gilt eine Verjährungsfrist von fünf Jahren ab dem Tag, an dem der Beschluss der Kommission zur Verhängung von Geldbußen bzw. Zwangsgeldern erlassen wurde. Jede Maßnahme, die die Kommission oder ein Mitgliedstaat auf Antrag der Kommission ergreift, um die Zahlung der Geldbuße bzw. des Zwangsgelds durchzusetzen, führt zur Unterbrechung dieser Verjährungsfrist. Nach jeder Unterbrechung beginnt die Verjährungsfrist von fünf Jahren erneut.
- (4) *Die Verjährungsfrist läuft spätestens an dem Tag aus, an dem die doppelte Zeitspanne dieser Verjährungsfrist verstrichen ist, sofern nicht die Kommission*
- a) einen Beschluss nach Artikel 10 oder 11 in einem Fall nach Absatz 1 des vorliegenden Artikels erlassen hat oder*
 - b) eine Geldbuße oder ein Zwangsgeld in einer Situation nach Absatz 2 des vorliegenden Artikels verhängt hat.*
- (5) *Die Verjährungsfrist wird gehemmt, solange der Beschluss der Kommission Gegenstand eines vor dem Gerichtshof der Europäischen Union anhängigen Verfahrens ist.*

Artikel 39

Umgehungsverbot

- (1) Unternehmen dürfen keine Finanzgeschäfte oder -kontrakte abschließen, um die Anmeldepflichten nach Artikel 21 Absätze 1 und 5 bzw. die Meldepflichten nach Artikel 29 Absätze 1, 5 und 8 zu umgehen.**
- (2) Vermutet die Kommission, dass ein Unternehmen die in Absatz 1 genannten Praktiken angewandt hat oder anwendet, so kann sie von diesem Unternehmen alle Auskünfte verlangen, die die Kommission als erforderlich erachtet, um festzustellen, ob das Unternehmen die in Absatz 1 genannten Praktiken angewandt hat oder anwendet, und sie kann eine Prüfung gemäß Artikel 21 Absatz 4 oder Artikel 30 Absatz 4 einleiten.**

Artikel 40

Veröffentlichung von Beschlüssen

- (1) Die Kommission veröffentlicht eine Zusammenfassung der Beschlüsse nach Artikel 10 Absatz 3 Buchstabe a und gibt allen natürlichen und juristischen Personen, Mitgliedstaaten oder dem Drittstaat, der die drittstaatliche Subvention gewährt hat, Gelegenheit zur Stellungnahme.**

- (2) Die Kommission veröffentlicht die nach **Artikel 11** Absätze 2, 3 und 4, **Artikel 25 Absätze 3 und 6** sowie **Artikel 31** Absätze 1, 2 und 3 erlassenen Beschlüsse im *Amtsblatt der Europäischen Union*.
- (3) Bei der Veröffentlichung von Zusammenfassungen und Beschlüssen trägt die Kommission dem berechtigten Interesse der Unternehmen am Schutz ihrer Geschäftsgeheimnisse und anderer vertraulicher Informationen gebührend Rechnung.

Artikel 41

Adressaten der Beschlüsse

- (1) Die Kommission **setzt Unternehmen oder Unternehmensvereinigungen** unverzüglich **über an sie gerichtete Beschlüsse in Kenntnis** und bietet **diesen Unternehmen oder Unternehmensvereinigungen** Gelegenheit, der Kommission mitzuteilen, welche **im Beschluss enthaltenen** Angaben sie als vertraulich erachten.

- (2) Die Kommission **unterrichtet** den betreffenden öffentlichen Auftraggeber bzw. den betreffenden Auftraggeber **über nach Artikel 31 Absätze 1 und 3 angenommene Beschlüsse**, die an einen Wirtschaftsteilnehmer gerichtet sind, das an einem öffentlichen Vergabeverfahren teilnimmt.
- (3) Beschlüsse nach Artikel 29 Absatz 4 und **Artikel 31** Absatz 2 werden an den betreffenden öffentlichen Auftraggeber bzw. den betreffenden Auftraggeber gerichtet. Die Kommission unterrichtet den Wirtschaftsteilnehmer, für das die Zuschlagserteilung untersagt wird, mittels einer Kopie des einschlägigen Beschlusses.

Artikel 42

Offenlegung und Verteidigungsrechte

- (1) Vor dem Erlass von Beschlüssen nach **Artikel 11, Artikel 12, Artikel 17, Artikel 18, Artikel 25 Absatz 3, Artikel 26, Artikel 31 oder Artikel 33** gibt die Kommission dem **Unternehmen, das Gegenstand der Prüfung ist**, Gelegenheit, zu den Gründen, aus denen die Kommission den Beschluss zu erlassen beabsichtigt, Stellung zu nehmen.
- (2) **Abweichend von Absatz 1 kann ein Beschluss nach Artikel 11 vorläufig erlassen werden, ohne dass dem Unternehmen, das Gegenstand der Prüfung ist, vorher Gelegenheit gegeben wurde, zu den Gründen Stellung zu nehmen, sofern die Kommission ihm diese Gelegenheit so bald wie möglich nach Erlass ihres Beschlusses gibt.**

- (3) Die Kommission stützt ihre Beschlüsse ausschließlich auf Gründe, zu denen die betreffenden Unternehmen Gelegenheit zur Stellungnahme erhalten haben.
- (4) *Um von seinem Recht nach Absatz 1 Gebrauch machen zu können, hat das Unternehmen, das Gegenstand der Prüfung ist, das Recht auf Einsicht in die Akten der Kommission. Von der Akteneinsicht ausgenommen sind vertrauliche Informationen sowie interne Schriftstücke der Kommission oder der Mitgliedstaaten und insbesondere die Korrespondenz zwischen der Kommission und den Mitgliedstaaten.*

Das Recht auf Akteneinsicht unterliegt dem berechtigten Interesse der Unternehmen oder der Unternehmensvereinigungen am Schutz ihrer Geschäftsgeheimnisse und anderer vertraulicher Informationen. Die Kommission kann das Unternehmen, das Gegenstand der Prüfung ist, und die Unternehmen oder Unternehmensvereinigungen, die der Kommission Informationen bereitgestellt haben, auffordern, sich auf Bedingungen zur Offenlegung dieser Informationen zu einigen. Falls die Unternehmen oder Unternehmensvereinigungen zu keiner Einigung kommen, ist die Kommission befugt, Bedingungen zur Offenlegung der Informationen aufzuerlegen.

Dieser Absatz hindert die Kommission in keiner Weise daran, sofern erforderlich Informationen, die das Vorliegen einer den Binnenmarkt verzerrenden drittstaatlichen Subvention belegen, zu verwenden und offenzulegen.

Artikel 43

Berufsgeheimnis *und* Vertraulichkeit

- (1) Im Rahmen dieser Verordnung erlangte Informationen dürfen nur zu dem Zweck verwendet werden, zu dem sie erlangt wurden, ***es sei denn, der Bereitsteller der Informationen stimmt etwas anderem zu.***
- (2) ***Die Mitgliedstaaten und*** die Kommission, ihre Bediensteten und andere ihrer Aufsicht unterstehende Personen ***stellen im Einklang mit den geltenden Bestimmungen sicher, dass die im Rahmen der Anwendung dieser Verordnung erlangten vertraulichen Informationen geschützt werden. Hierzu*** legen sie unter das Berufsgeheimnis fallende Informationen, die sie im Rahmen dieser Verordnung erlangt haben, nicht offen.
- (3) Die Absätze 1 und 2 stehen der Veröffentlichung von Statistiken und Berichten, die keine Angaben enthalten, anhand derer bestimmte Unternehmen oder Unternehmensvereinigungen erkannt werden können, nicht entgegen.
- (4) ***Die Offenlegung von Informationen, die im Rahmen dieser Verordnung übermittelt werden, darf nicht die wesentlichen Sicherheitsinteressen der Mitgliedstaaten berühren.***

Kapitel 6

Verhältnis zu anderen Rechtsinstrumenten

Artikel 44

Verhältnis zu anderen Rechtsinstrumenten

- (1) Die vorliegende Verordnung lässt die Anwendung der Artikel 101, 102, 106, 107 und 108 AEUV sowie der Verordnung (EG) Nr. 1/2003 des Rates²⁵ und der Verordnung (EG) Nr. 139/2004 unberührt.
- (2) Die vorliegende Verordnung lässt die Anwendung der Verordnung (EU) 2016/1037 des Europäischen Parlaments und des Rates²⁶ unberührt.
- (3) Die vorliegende Verordnung lässt die Anwendung der Verordnung (EU) 2019/452²⁷ unberührt.

²⁵ Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln (ABl. L 1 vom 4.1.2003, S. 1).

²⁶ Verordnung (EU) 2016/1037 des Europäischen Parlaments und des Rates über den Schutz gegen subventionierte Einfuhren aus nicht zur Europäischen Union gehörenden Ländern (ABl. L 176 vom 30.6.2016, S. 55).

- (4) *Die vorliegende Verordnung lässt die Anwendung der Verordnung (EU) 2022/1031 des Europäischen Parlaments und des Rates²⁷ unberührt.*
- (5) Die vorliegende Verordnung hat Vorrang vor der Verordnung (EU) 2016/1035 **■**, bis jene Verordnung gemäß ihrem Artikel 18 angewendet wird. Fällt nach diesem Zeitpunkt eine drittstaatliche Subvention in den Anwendungsbereich sowohl der Verordnung (EU) 2016/1035 als auch der vorliegenden Verordnung, hat die Verordnung (EU) 2016/1035 Vorrang. Die Bestimmungen der vorliegenden Verordnung, die auf die öffentliche Auftragsvergabe und Zusammenschlüsse Anwendung finden, haben jedoch Vorrang vor der Verordnung (EU) 2016/1035.
- (6) Die vorliegende Verordnung hat Vorrang vor der Verordnung (EWG) Nr. 4057/86 **■**.
- (7) Die vorliegende Verordnung lässt die Anwendung der Verordnung (EU) 2019/712 **■** unberührt. **■** Zusammenschlüsse im Sinne des **Artikels 20** der vorliegenden Verordnung, an denen Luftfahrtunternehmen beteiligt sind, unterliegen den Bestimmungen des Kapitels 3 der vorliegenden Verordnung. Öffentliche Vergabeverfahren, an denen Luftfahrtunternehmen beteiligt sind, unterliegen den Bestimmungen des Kapitels 4 der vorliegenden Verordnung.

²⁷ *Verordnung (EU) 2022/1031 des Europäischen Parlaments und des Rates vom 23. Juni 2022 über den Zugang von Wirtschaftsteilnehmern, Waren und Dienstleistungen aus Drittländern zum Unionsmarkt für öffentliche Aufträge und Konzessionen und über die Verfahren zur Unterstützung von Verhandlungen über den Zugang von Wirtschaftsteilnehmern, Waren und Dienstleistungen aus der Union zu den Märkten für öffentliche Aufträge und Konzessionen von Drittländern (Instrument betreffend das internationale Beschaffungswesen – IPI) (ABl. L 173 vom 30.6.2022, S. 1).*

- (8) *Die vorliegende Verordnung ist im Einklang mit den Richtlinien 2009/81/EG, 2014/23/EU, 2014/24/EU und 2014/25/EU sowie den Richtlinien 89/665/EWG²⁸ und 92/13/EWG²⁹ des Rates auszulegen.*
- (9) Die vorliegende Verordnung hindert die Union nicht daran, die Rechte auszuüben und die Verpflichtungen zu erfüllen, die ihr aus völkerrechtlichen Übereinkünften erwachsen. Es wird keine Prüfung nach der vorliegenden Verordnung durchgeführt und keine Maßnahme verhängt oder aufrechterhalten, wenn diese Prüfung oder Maßnahme den Verpflichtungen der Union aus einschlägigen völkerrechtlichen Übereinkünften, zu dessen Vertragsparteien sie gehört, zuwiderlaufen würde. Insbesondere werden im Rahmen dieser Verordnung keine Maßnahmen ergriffen, die einer spezifischen Maßnahme gegen eine Subvention im Sinne des Artikels 32.1 des Übereinkommens über Subventionen und Ausgleichsmaßnahmen, **die von einem Drittstaat gewährt wurde, der Mitglied der Welthandelsorganisation ist,** gleichkämen.

²⁸ *Richtlinie 89/665/EWG des Rates vom 21. Dezember 1989 zur Koordinierung der Rechts- und Verwaltungsvorschriften für die Anwendung der Nachprüfungsverfahren im Rahmen der Vergabe öffentlicher Liefer- und Bauaufträge (ABl. L 395 vom 30.12.1989, S. 33).*

²⁹ *Richtlinie 92/13/EWG des Rates vom 25. Februar 1992 zur Koordinierung der Rechts- und Verwaltungsvorschriften für die Anwendung der Gemeinschaftsvorschriften über die Auftragsvergabe durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie im Telekommunikationssektor (ABl. L 76 vom 23.3.1992, S. 14).*

Kapitel 7
Übergangs- und Schlussbestimmungen



Artikel 45

Überwachung durch den Gerichtshof

Nach Artikel 261 AEUV hat der Gerichtshof der Europäischen Union die Befugnis zu unbeschränkter Ermessensnachprüfung von Beschlüssen, mit denen die Kommission Geldbußen oder Zwangsgelder verhängt hat. Er kann die verhängten Geldbußen oder Zwangsgelder aufheben, herabsetzen oder erhöhen.

Artikel 46

Leitlinien

- (1) *Die Kommission veröffentlicht spätestens am ... [drei Jahre nach dem Tag des Inkrafttretens dieser Verordnung] Leitlinien in Bezug auf Folgendes und aktualisiert diese danach regelmäßig:***
- a) die Anwendung der Kriterien für die Feststellung des Vorliegens einer Verzerrung nach Artikel 4 Absatz 1,***
 - b) die Anwendung der Abwägungsprüfung nach Artikel 6,***

- c) *die Anwendung ihrer Befugnis, die vorherige Anmeldung jedes Zusammenschlusses nach Artikel 21 Absatz 5 bzw. die vorherige Meldung jeder drittstaatlichen finanziellen Zuwendung an einen Wirtschaftsteilnehmer im Rahmen eines öffentlichen Vergabeverfahrens nach Artikel 29 Absatz 8 zu verlangen, und*
 - d) *die Beurteilung einer Verzerrung in einem öffentlichen Vergabeverfahren nach Artikel 27.*
- (2) *Vor der Herausgabe der Leitlinien nach Absatz 1 führt die Kommission angemessene Konsultationen mit den Interessenträgern und Mitgliedstaaten durch. Die Leitlinien stützen sich auf die Erfahrungen, die bei der Durchführung und Durchsetzung dieser Verordnung gesammelt wurden.*

Artikel 47

■ Durchführungsrechtsakte

- (1) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, die Folgendes betreffen:
- a) *Form, Inhalt und andere Verfahrenseinzelheiten in Bezug auf die Anmeldung von Zusammenschlüssen nach Artikel 21, einschließlich eines möglichen vereinfachten Verfahrens, wobei dem Ziel, den Verwaltungsaufwand im Rahmen von Artikel 21 dieser Verordnung und Artikel 4 der Verordnung (EG) Nr. 139/2004 für die Anmelder zu begrenzen, besonders Rechnung zu tragen ist,*

- b) Form, Inhalt und andere Verfahrenseinzelheiten in Bezug auf die Meldung drittstaatlicher finanzieller Zuwendungen **und die Erklärung, dass keine drittstaatliche finanzielle Zuwendung erhalten wurde**, im Rahmen öffentlicher Vergabeverfahren **nach Artikel 29, einschließlich eines möglichen vereinfachten Verfahrens**,
- c) **Verfahrenseinzelheiten für mündliche Erklärungen nach Artikel 13 Absatz 7, Artikel 14 Absatz 2 Buchstabe c und Artikel 15**,
- d) Einzelheiten in Bezug auf die Offenlegung nach **Artikel 42 und das Berufsgeheimnis nach Artikel 43**,
- e) Form, Inhalt und andere Verfahrenseinzelheiten in Bezug auf Transparenzanforderungen,
- f) genaue Vorschriften zur Berechnung von Fristen,
- g) die **Verfahrenseinzelheiten** und Fristen für die Unterbreitung von Verpflichtungszusagen nach den **Artikeln 25 und 31**,

- h)** genaue Vorschriften zu den in den **Artikeln 29 bis 32** dargelegten Verfahrensschritten in Bezug auf Untersuchungen im Rahmen öffentlicher Vergabeverfahren.
- (2) Durchführungsrechtsakte gemäß Absatz 1 werden nach dem Beratungsverfahren, auf das in **Artikel 48** Absatz 2 Bezug genommen wird, erlassen.
- (3) *Vor dem Erlass von Maßnahmen nach Absatz 1 veröffentlicht die Kommission einen Entwurf dieser Maßnahmen und holt innerhalb der Frist Stellungnahmen ein. Diese Frist wird von der Kommission gesetzt und beträgt mindestens vier Wochen.*
- (4) *Die ersten Durchführungsrechtsakte nach Absatz 1 werden am ... [Tag des Geltungsbeginns dieser Verordnung] erlassen.*

Artikel 48

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 4 der Verordnung (EU) Nr. 182/2011.

Artikel 49

Delegierte Rechtsakte

- (1) Der Kommission wird die Befugnis übertragen, einen delegierten Rechtsakt ***im Einklang mit Artikel 50 zu erlassen, um erforderlichenfalls den Schwellenwert für die Anmeldung von Zusammenschlüssen nach Artikel 20 Absatz 3 Buchstabe a zu ändern, indem der Schwellenwert um bis zu 20 % erhöht oder um bis zu 20 % herabgesetzt wird, nachdem***
 - a) ***dieser Schwellenwert unter Berücksichtigung der Erfahrung, die bei der Durchführung und Durchsetzung dieser Verordnung gesammelt wurde, bewertet wurde und***

- b) die Notwendigkeit festgestellt wurde, diesen Schwellenwert zu ändern, um
 - i) sicherzustellen, dass die in Kapitel 3 vorgesehenen Anmeldeverfahren die genaue Ermittlung den Binnenmarkt verzerrender drittstaatlicher Subventionen ermöglichen,*
 - ii) für einen vertretbaren Verwaltungsaufwand für die Kommission und die betreffenden Unternehmen zu sorgen und*
 - iii) die Wirksamkeit der Anwendung dieser Verordnung zu verbessern.**
- (2) Für die Zwecke der Beurteilung, ob der Schwellenwert für die Anmeldungen nach Absatz 1 geändert werden muss, führt die Kommission ihre Bewertung für einen bestimmten Zeitraum, der nicht kürzer als zwei Jahre sein darf, insbesondere auf der Grundlage der folgenden objektiven Kriterien durch:*
- a) des Anteils der Anmeldungen nach Artikel 21 Absatz 1, die dazu geführt haben, dass die Kommission entweder die Vorprüfung nach Artikel 10 Absatz 4 abgeschlossen oder einen Beschluss, keine Einwände zu erheben, nach Artikel 25 Absatz 3 Buchstabe b erlassen hat,*

- b) *des Anteils der Anmeldungen nach Artikel 21 Absatz 1, die dazu geführt haben, dass die Kommission entweder einen Beschluss zur Untersagung eines Zusammenschlusses nach Artikel 25 Absatz 3 Buchstabe c oder einen Verpflichtungsbeschluss nach Artikel 25 Absatz 3 Buchstabe a erlassen hat,*
- c) *des Anteils der Anmeldungen nach Artikel 21 Absatz 5, die dazu geführt haben, dass die Kommission entweder einen Beschluss zur Untersagung eines Zusammenschlusses nach Artikel 25 Absatz 3 Buchstabe c oder einen Verpflichtungsbeschluss nach Artikel 25 Absatz 3 Buchstabe a erlassen hat,*
- d) *des Anteils der nach Artikel 9 von Amts wegen eingeleiteten Prüfungen im Zusammenhang mit Zusammenschlüssen, die keine anmeldepflichtigen Zusammenschlüsse im Sinne des Artikels 20 darstellen, die entweder zu einem Beschluss zur Auferlegung von Abhilfemaßnahmen nach Artikel 11 Absatz 2 oder zu einem Verpflichtungsbeschluss nach Artikel 11 Absatz 3 führten,*

- e) *des Vergleichs zwischen dem Schwellenwert nach Artikel 20 Absatz 3 Buchstabe a und dem durchschnittlichen Gesamtumsatz oberhalb dieses Schwellenwertes in Fällen, in denen entweder ein Beschluss zur Untersagung eines Zusammenschlusses nach Artikel 25 Absatz 3 Buchstabe c oder ein Verpflichtungsbeschluss nach Artikel 25 Absatz 3 Buchstabe a erlassen wurde,*
 - f) *der Anzahl der Anmeldungen nach Artikel 21 Absatz 1 und die Entwicklung dieser Anzahl.*
- (3) *Um die Schwellenwerte in Artikel 20 Absatz 3 Buchstabe a erhöhen zu können, ist in der in Absatz 2 genannten Bewertung nachzuweisen, dass*
- a) *ein Großteil der Beschlüsse zur Untersagung eines Zusammenschlusses nach Artikel 25 Absatz 3 Buchstabe c oder der Verpflichtungsbeschlüsse nach Artikel 25 Absatz 3 Buchstabe a Fälle betraf, in denen der in Artikel 20 Absatz 3 Buchstabe a genannte Gesamtumsatz erheblich über diesem Schwellenwert lag, oder*

- b) *ein Großteil der Anmeldungen nach Artikel 21 Absatz 1 dazu geführt hat, dass die Kommission entweder die Vorprüfung nach Artikel 10 Absatz 4 abgeschlossen oder einen Beschluss, keine Einwände zu erheben, nach Artikel 25 Absatz 3 Buchstabe b erlassen hat.*
- (4) *Um die Schwellenwerte in Artikel 20 Absatz 3 Buchstabe a herabsetzen zu können, ist in der in Absatz 2 genannten Bewertung nachzuweisen, dass*
- a) *ein Großteil der Anmeldungen nach Artikel 21 Absatz 5 dazu geführt hat, dass die Kommission entweder einen Beschluss zur Untersagung eines Zusammenschlusses nach Artikel 25 Absatz 3 Buchstabe c oder einen Verpflichtungsbeschluss nach Artikel 25 Absatz 3 Buchstabe a erlassen hat, oder*
 - b) *ein Großteil der von Amts wegen eingeleiteten Prüfungen drittstaatlicher Subventionen im Zusammenhang mit Zusammenschlüssen, die keine anmeldepflichtigen Zusammenschlüsse im Sinne des Artikels 20 darstellten, dazu geführt hat, dass die Kommission entweder einen Beschluss zur Auferlegung von Abhilfemaßnahmen nach Artikel 11 Absatz 2 oder einen Verpflichtungsbeschluss nach Artikel 11 Absatz 3 erlassen hat.*

- (5) *Der Kommission wird die Befugnis übertragen, einen delegierten Rechtsakt im Einklang mit Artikel 50 zu erlassen, um erforderlichenfalls die Schwellenwerte für die Meldungen nach Artikel 28 Absatz 1 Buchstabe a und Artikel 28 Absatz 2 für öffentliche Vergabeverfahren zu ändern, indem sie um bis zu 20 % erhöht oder um bis zu 20 % herabgesetzt werden, nachdem*
- a) diese Schwellenwerte unter Berücksichtigung ihrer Erfahrung, die bei der Durchführung und Durchsetzung dieser Verordnung gesammelt wurde bewertet wurden und*
 - b) die Notwendigkeit festgestellt wurde, diesen Schwellenwert zu ändern, um*
 - i) sicherzustellen, dass die in Kapitel 4 vorgesehenen Anmeldeverfahren die genaue Ermittlung den Binnenmarkt verzerrender drittstaatlicher Subventionen ermöglichen,*
 - ii) für einen vertretbaren Verwaltungsaufwand für die Kommission und die betreffenden Wirtschaftsteilnehmer zu sorgen und*
 - iii) die Wirksamkeit der Anwendung dieser Verordnung zu verbessern.*

- (6) *Für die Zwecke der Beurteilung, ob der Schwellenwert für die Meldungen nach Absatz 5 geändert werden muss, führt die Kommission ihre Bewertung in Bezug auf einen bestimmten Zeitraum, der nicht kürzer als zwei Jahre sein darf, insbesondere auf der Grundlage der folgenden objektiven Kriterien durch:*
- a) *des Anteils der Meldungen nach Artikel 29 Absatz 1, die dazu geführt haben, dass die Kommission entweder die Vorprüfung nach Artikel 10 Absatz 4 abgeschlossen oder einen Beschluss, keine Einwände zu erheben, nach Artikel 31 Absatz 3 Buchstabe b erlassen hat,*
 - b) *des Anteils der Meldungen nach Artikel 29 Absatz 1, die dazu geführt haben, dass die Kommission entweder einen Beschluss zur Untersagung der Zuschlagserteilung nach Artikel 31 Absatz 2 oder einen Verpflichtungsbeschluss nach Artikel 31 Absatz 1 erlassen hat,*
 - c) *des Anteils der Meldungen nach Artikel 29 Absatz 8, die dazu geführt haben, dass die Kommission entweder einen Beschluss zur Untersagung der Zuschlagserteilung nach Artikel 31 Absatz 2 oder einen Verpflichtungsbeschluss nach Artikel 31 Absatz 1 erlassen hat,*

- d) *der Anzahl der Beschlüsse zur Auferlegung von Abhilfemaßnahmen nach Artikel 11 Absatz 2 und der Verpflichtungsbeschlüsse nach Artikel 11 Absatz 3 im Anschluss an eine nach Artikel 9 von Amts wegen eingeleitete Prüfung im Zusammenhang mit einer drittstaatlichen finanziellen Zuwendung im Rahmen eines öffentlichen Vergabeverfahrens, die keiner Meldepflicht im Sinne des Artikels 28 Absatz 1 unterlag oder in den Anwendungsbereich von Artikel 30 Absatz 4 fiel, im Verhältnis zur Gesamtzahl der nach Artikel 9 von Amts wegen eingeleiteten Prüfungen im Zusammenhang mit einer drittstaatlichen finanziellen Zuwendung im Rahmen eines öffentlichen Vergabeverfahrens, die keiner Meldepflicht im Sinne des Artikels 28 Absatz 2 unterlag oder in den Anwendungsbereich von Artikel 30 Absatz 4 fiel,*
- e) *des Vergleichs zwischen den jeweiligen Schwellenwerten nach Artikel 28 Absatz 1 Buchstabe a und Artikel 28 Absatz 2 und dem durchschnittlichen geschätzten Wert des Auftrags oder des durchschnittlichen Werts des Loses oberhalb des jeweiligen Schwellenwerts, in denen entweder ein Beschluss zur Untersagung der Zuschlagserteilung nach Artikel 31 Absatz 2 oder ein Verpflichtungsbeschluss nach Artikel 31 Absatz 1 erlassen wurde,*
- f) *der Anzahl der Meldungen nach Artikel 29 Absatz 1 und die Entwicklung dieser Anzahl.*

- (7) *Um die Schwellenwerte der Meldungen erhöhen zu können, ist in der in Absatz 6 genannten Bewertung nachzuweisen, dass*
- a) *ein Großteil der Beschlüsse zur Untersagung der Zuschlagserteilung nach Artikel 31 Absatz 2 und Verpflichtungsbeschlüsse nach Artikel 31 Absatz 1 Fälle betraf, in denen der in Artikel 28 Absatz 1 Buchstabe a genannte geschätzte Wert des Auftrags oberhalb des Schwellenwerts oder der in Artikel 28 Absatz 2 genannte geschätzte Wert der Lose, für die ein Angebot abgegeben wurde, oberhalb des Schwellenwerts erheblich über den jeweiligen Schwellenwerten nach Artikel 28 Absatz 1 Buchstabe a und Artikel 28 Absatz 2 lag, oder*
 - b) *ein Großteil der Meldungen nach Artikel 29 Absatz 1 dazu geführt hat, dass die Kommission entweder die Vorprüfung nach Artikel 10 Absatz 4 abgeschlossen oder einen Beschluss, keine Einwände zu erheben, nach Artikel 31 Absatz 3 erlassen hat.*

- (8) *Um die Schwellenwerte herabsetzen zu können, ist in der in Absatz 6 genannten Bewertung nachzuweisen, dass*
- a) *ein Großteil der Meldungen nach Artikel 29 Absatz 8 dazu geführt hat, dass die Kommission entweder einen Verpflichtungsbeschluss nach Artikel 31 Absatz 1 oder einen Beschluss zur Untersagung der Zuschlagserteilung nach Artikel 31 Absatz 2 erlassen hat, oder*
 - b) *ein Großteil der von Amts wegen eingeleiteten Prüfungen drittstaatlicher Subventionen im Zusammenhang mit drittstaatlichen finanziellen Zuwendungen im Rahmen eines öffentlichen Vergabeverfahrens, die keiner Meldepflicht im Sinne des Artikels 28 Absatz 1 unterlagen oder in den Anwendungsbereich von Artikel 30 Absatz 4 fielen, dazu geführt hat, dass die Kommission entweder einen Beschluss zur Auferlegung von Abhilfemaßnahmen nach Artikel 11 Absatz 2 oder einen Verpflichtungsbeschluss nach Artikel 11 Absatz 3 erlassen hat.*

- (9) *Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte im Einklang mit Artikel 50 zu erlassen, um die zeitlichen Vorgaben für Vorprüfungen und eingehende Prüfungen nach Artikel 25 Absatz 2 und Absatz 4 für angemeldete Zusammenschlüsse und nach Artikel 30 Absatz 2, 5 und 6 für gemeldete finanzielle Zuwendungen im Rahmen öffentlicher Vergabeverfahren zu verkürzen. Die Kommission kann diese delegierten Rechtsakte erlassen, um die zeitlichen Vorgaben von Artikel 25 Absatz 2 und 4 und Artikel 30 Absatz 2, 6 und 6 zu verkürzen, wenn die praktische Erfahrung der Kommission bei der Anwendung dieser Verordnung zeigt, dass die Bewertung durch die Kommission in einem kürzeren Zeitraum durchgeführt werden kann.*

Artikel 50

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 nach Artikel 49 Absätze 1 und 5 wird der Kommission für einen Zeitraum von fünf Jahren ab dem ... [zwei Jahre nach dem Tag des Inkrafttretens dieser Verordnung] übertragen.*

- (3) *Die Befugnis zum Erlass delegierter Rechtsakte nach Artikel 49 Absatz 9 wird der Kommission für einen Zeitraum von fünf Jahren ab dem ... [zwei Jahre nach dem Tag des Inkrafttretens dieser Verordnung] 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.*
- (4) Die Befugnisübertragung gemäß **Artikel 49 Absätze 1, 5 und 9** 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.

- (5) 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.
- (6) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.
- (7) Ein delegierter Rechtsakt, der gemäß **Artikel 49 Absätze 1, 5 und 9** 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 51

Gesonderte delegierte Rechtsakte für die jeweiligen übertragenen Befugnisse

Die Kommission erlässt einen gesonderten delegierten Rechtsakt für jede einzelne ihr gemäß dieser Verordnung übertragene Befugnis.

Artikel 52

Berichterstattung und Überprüfung

- (1) Die Kommission legt dem Europäischen Parlament und dem Rat einen jährlichen Bericht über die Anwendung und Durchführung dieser Verordnung vor.***
- (2) Die Kommission überprüft bis zum ... [drei Jahre nach dem Tag des Geltungsbeginns dieser Verordnung] und danach alle drei Jahre ihre Praxis zur Durchführung und Durchsetzung dieser Verordnung, insbesondere in Bezug auf die Anwendung der Artikel 4, 5, 6 und 8 sowie die Anmelde- bzw. Meldeschwellen nach Artikel 20 Absatz 3, Artikel 28 Absatz 1 und Absatz 2, und legt dem Europäischen Parlament und dem Rat ■ einen Bericht ■ vor, dem sie, sofern sie dies für angemessen hält, einschlägige Gesetzgebungsvorschläge beifügt. Im Rahmen ihrer Überprüfung erstattet die Kommission Bericht über die Entwicklungen in den internationalen Beziehungen in Bezug auf die Subventionskontrollsysteme von Drittstaaten.***

(3) *Hält die Kommission es für angemessen, den Bericht mit einschlägigen Gesetzgebungsvorschlägen zu kombinieren, so könnten diese Vorschläge Folgendes umfassen:*

- a) Änderungen der Schwellenwerte für Anmeldungen bzw. Meldungen nach den Artikeln 20 und 28,*
- b) Freistellung bestimmter Gruppen betroffener Unternehmen von der Anmeldepflicht nach Artikel 21 bzw. der Meldepflicht nach Artikel 29, insbesondere wenn die Praxis der Kommission es ermöglicht, wirtschaftliche Tätigkeiten zu ermitteln, bei denen Verzerrungen auf dem Binnenmarkt durch drittstaatliche Subventionen unwahrscheinlich sind,*
- c) Festlegung spezifischer Schwellenwerte für die Anmeldung bzw. Meldung für bestimmte Wirtschaftszweige oder differenzierter Schwellenwerte für verschiedene Arten öffentlicher Aufträge, insbesondere wenn die Praxis der Kommission es ermöglicht, wirtschaftliche Tätigkeiten zu ermitteln, bei denen Verzerrungen auf dem Binnenmarkt durch drittstaatliche Subventionen wahrscheinlicher sind, auch in Bezug auf strategische Sektoren und kritische Infrastrukturen,*
- d) Änderungen der zeitlichen Vorgaben für Vorprüfungen und eingehende Prüfungen nach den Artikeln 25 und 30,*
- e) Aufhebung der vorliegenden Verordnung, wenn die Kommission der Auffassung ist, dass multilaterale Regelungen zur Verhinderung von den Binnenmarkt verzerrenden Subventionen die vorliegende Verordnung vollständig überflüssig gemacht haben.*

Artikel 53

Übergangsbestimmungen

- (1) Diese Verordnung gilt für drittstaatliche Subventionen, die in den **fünf Jahren** vor **dem ... [Tag des Geltungsbeginns dieser Verordnung]** gewährt wurden, wenn diese drittstaatlichen Subventionen den Binnenmarkt nach ... [Tag des Geltungsbeginns dieser Verordnung] verzerren.
- (2) **Abweichend von Absatz 1 gilt** diese Verordnung **■** für drittstaatliche finanzielle Zuwendungen, die in den drei Jahren vor **dem ... [Tag des Geltungsbeginns dieser Verordnung]** gewährt wurden, wenn die drittstaatlichen finanziellen Zuwendungen einem Unternehmen gewährt wurden, das nach dieser Verordnung einen Zusammenschluss anmeldet oder finanzielle Zuwendungen im Zusammenhang mit einem öffentlichen Vergabeverfahren meldet.
- (3) Diese Verordnung gilt nicht für Zusammenschlüsse, für die bereits vor **dem ... [Tag des Geltungsbeginns dieser Verordnung]** der entsprechende Vertrag geschlossen, das öffentliche Übernahmeangebot angekündigt oder eine die Kontrolle begründende Beteiligung erworben wurde.
- (4) Diese Verordnung gilt nicht für öffentliche Aufträge oder öffentliche Vergabeverfahren, die vor **dem ... [Tag des Geltungsbeginns dieser Verordnung]** vergeben bzw. eingeleitet wurden.

Artikel 54

Inkrafttreten und Geltungsbeginn

- (1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.
- (2) Sie gilt ab dem ... [**sechs Monate nach dem Tag des Inkrafttretens dieser Verordnung**].
- (3) **Abweichend von Absatz 2 des vorliegenden Artikels gelten die Artikel 47 und 48 ab dem ... [Tag des Inkrafttretens dieser Verordnung] und Artikel 14 Absatz 5, 6 und 7 ab dem ... [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].**
- (4) **Abweichend von Absatz 2 des vorliegenden Artikels gelten die Artikel 21 und 29 ab dem ... [neun Monate nach dem Tag des Inkrafttretens dieser Verordnung].**

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu ... am ...

Im Namen des Europäischen Parlaments
Die Präsidentin

Im Namen des Rates
Der Präsident/Die Präsidentin

Zu diesem Rechtsakt wurden drei Erklärungen abgegeben, welche in ... [Durch das Amt für Veröffentlichungen einzufügen: ABl. C XXX vom XXX, S. XX] wiedergegeben sind und unter dem folgenden Link abgerufen werden können: [ABl.: Bitte Link(s) zu den Erklärungen einfügen].

ANLAGE ZUR LEGISLATIVEN ENTSCHLIESSUNG

Gemeinsame Erklärung des Europäischen Parlaments, des Rates und der Kommission

Die Union tritt weiterhin für ein offenes und regelbasiertes multilaterales Handelssystem, in dessen Mittelpunkt eine modernisierte WTO steht, und für eine weitere Verbesserung der Wirksamkeit des multilateralen Rahmens für Subventionen ein. Sie bekräftigt ihre Entschlossenheit, die Modernisierung der WTO-Regeln zu unterstützen, um Handels- und Wettbewerbsverzerrungen zu beseitigen. Die Union wird sich insbesondere dafür einsetzen, die Regeln für Industriesubventionen zu modernisieren, um das ordnungsgemäße Funktionieren des WTO-Übereinkommens über Subventionen und Ausgleichsmaßnahmen zu verbessern und die Einhaltung und Durchsetzung zu fördern.

Erklärung der Europäischen Kommission zu den Erläuterungen in Bezug auf die Anwendung
der Verordnung ...* gemäß Artikel 46

Die Kommission verpflichtet sich, die Anwendung von Artikel 4 Absatz 1 der Verordnung [Veröffentlichungsnummer von Verfahren 2021/0114(COD) einfügen] über das Vorliegen einer durch eine drittstaatliche Subvention verursachten Verzerrung auf dem Binnenmarkt, die Anwendung der Abwägungsprüfung nach Artikel 6 dieser Verordnung und die Beurteilung einer Verzerrung in einem öffentlichen Vergabeverfahren nach Artikel 27 Absatz 1 dieser Verordnung zu erläutern.

Die Kommission wird diese ersten Erläuterungen spätestens zwölf Monate nach dem Geltungsbeginn dieser Bestimmungen veröffentlichen.

Die gemäß Artikel 46 der Verordnung [Veröffentlichungsnummer des Verfahrens 2021/0114(COD) einfügen] herausgegebenen Leitlinien können diese ersten Erläuterungen ersetzen.

* ABl.: Bitte die Veröffentlichungsnummer des Verfahrens in 2021/0114(COD) und eine Fußnote mit der Amtsblattfundstelle einfügen.

Erklärung der Europäischen Kommission zu multilateralen Regelungen zur Verhinderung
verzerrender drittstaatlicher Subventionen anlässlich der Annahme der Verordnung

...*

Das Europäische Parlament, der Rat und die Europäische Kommission erzielten am 30. Juni 2022 eine Einigung über die Verordnung über den Binnenmarkt verzerrende drittstaatliche Subventionen³⁰. Diese Verordnung ergänzt die europäischen und internationalen Regelwerke für Subventionen und Subventionskontrolle. Sie betrifft Verzerrungen, die durch drittstaatliche Subventionen auf dem Binnenmarkt der Union verursacht werden.

Subventionen können sich negativ auf den internationalen Handel auswirken und zu Wettbewerbsverzerrungen sowohl in traditionellen Wirtschaftszweigen als auch im Bereich neuer Technologien führen. In manchen Fällen können unkontrollierte Subventionen auch zu Überkapazitäten führen, was die gesunde Marktdynamik beeinträchtigt. Die EU muss weiterhin von den internationalen Chancen profitieren und gleichzeitig Instrumente entwickeln, um unlautere Handelspraktiken sowohl intern als auch extern anzugehen³¹. Mit dieser Verordnung soll ein Beitrag dazu geleistet werden, die Resilienz des EU-Binnenmarkts zu verbessern, insbesondere wenn es darum geht, den Binnenmarkt vor Verzerrungen durch drittstaatliche Subventionen zu schützen. Auf diesem Weg ergänzt die Union ihr Instrumentarium im Hinblick auf die Verwirklichung der Ziele in Bezug auf die offene strategische Autonomie der Union.

Zur Bewältigung der negativen Auswirkungen von Subventionen und in Anerkennung der Tatsache, dass die WTO-Regeln möglicherweise nicht wirksam genug sind, um den negativen Spillover-Effekten staatlicher Eingriffe in die Wirtschaft, auch in bestimmten Industriesektoren, entgegenzuwirken, setzt sich die Europäische Kommission weiterhin dafür ein, den multilateralen Rahmen für Subventionen noch wirksamer zu gestalten, und ist entschlossen, mit Nachdruck auf einen Rechtsrahmen hinzuarbeiten, der geeignet ist,

* ABl.: Bitte die Veröffentlichungsnummer des Verfahrens in 2021/0114(COD) und eine Fußnote mit der Amtsblattfundstelle einfügen.

³⁰ Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über den Binnenmarkt verzerrende drittstaatliche Subventionen, COM(2021)0223.

³¹ Mitteilung der Kommission vom 18. Februar 2021 zum Thema „Überprüfung der Handelspolitik – Eine offene, nachhaltige und entschlossene Handelspolitik“, COM(2021)0066.

Handels- und Wettbewerbsverzerrungen anzugehen und gleiche Wettbewerbsbedingungen sicherzustellen³². Die Kommission ist insbesondere entschlossen, die Regeln für Industriesubventionen zu modernisieren, um das ordnungsgemäße Funktionieren des WTO-Übereinkommens über Subventionen und Ausgleichsmaßnahmen zu verbessern und seine Einhaltung zu fördern. In diesem Zusammenhang weist die Europäische Kommission auf ihre laufende trilaterale Zusammenarbeit mit Japan und den Vereinigten Staaten hin.

Die Regeln für Subventionen sind insbesondere im WTO-Übereinkommen über Subventionen und Ausgleichsmaßnahmen festgelegt, in dem bestimmte Subventionen und Maßnahmen verboten werden, um die nachteiligen Auswirkungen von Subventionen im Warenverkehr zu bekämpfen. In der Union werden diese Regeln, soweit sie eine anfechtbare Subventionierung betreffen, im Rahmen der Verordnung (EU) 2016/1037 über den Schutz gegen subventionierte Einfuhren aus nicht zur Europäischen Union gehörenden Ländern durchgeführt³³. Der Anwendungsbereich der Verordnung (EU) 2016/1037 wird durch den Anwendungsbereich des WTO-Übereinkommens über Subventionen und Ausgleichsmaßnahmen bestimmt.

Die Verordnung über den Binnenmarkt verzerrende drittstaatliche Subventionen steht im Einklang mit den völkerrechtlichen Verpflichtungen der Union, insbesondere auch denjenigen, die sich aus dem WTO-Übereinkommen über Subventionen und Ausgleichsmaßnahmen ergeben. Die Europäische Kommission wird sicherstellen, dass alle in Anwendung dieser Verordnung getroffenen Maßnahmen mit ihren völkerrechtlichen Verpflichtungen im Einklang stehen.

Die Kommission beabsichtigt, die Möglichkeiten dieser neuen Verordnung, durch drittstaatliche Subventionen verursachte Verzerrungen auf dem Binnenmarkt anzugehen, in vollem Umfang zu nutzen.

³² Mitteilung der Kommission vom 18. Februar 2021 zum Thema „Überprüfung der Handelspolitik – Eine offene, nachhaltige und entschlossene Handelspolitik“, COM(2021)0066.

³³ Verordnung (EU) 2016/1037 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz gegen subventionierte Einfuhren aus nicht zur Europäischen Union gehörenden Ländern (ABl. L 176 vom 30.6.2016, S. 55).



ANGENOMMENE TEXTE

P9_TA(2022)0380

Richtlinie hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 2013/34/EU, 2004/109/EG und 2006/43/EG und der Verordnung (EU) Nr. 537/2014 hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen (COM(2021)0189 – C9-0147/2021 – 2021/0104(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2021)0189),
- gestützt auf Artikel 294 Absatz 2 sowie Artikel 50 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage dem Parlament der Vorschlag der Kommission unterbreitet wurde (C9-0147/2021),
- gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 7. September 2021³⁴,
- unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 22. September 2021³⁵,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 29. Juni 2022 gemachte Zusage, den Standpunkt des Parlaments gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,
- gestützt auf Artikel 59 seiner Geschäftsordnung,

³⁴ ABl. C 446 vom 3.11.2021, S. 2.

³⁵ ABl. C 517 vom 22.12.2021, S. 51.

- unter Hinweis auf die Stellungnahmen des Ausschusses für Wirtschaft und Währung, des Ausschusses für Beschäftigung und soziale Angelegenheiten, des Ausschusses für Umweltfragen, öffentliche Gesundheit und Lebensmittelsicherheit, des Ausschusses für auswärtige Angelegenheiten, des Entwicklungsausschusses und des Ausschusses für die Rechte der Frau und die Gleichstellung der Geschlechter,
 - unter Hinweis auf das Schreiben des Ausschusses für Industrie, Forschung und Energie,
 - unter Hinweis auf den Bericht des Rechtsausschusses (A9-0059/2022),
1. legt den folgenden Standpunkt in erster Lesung fest;
 2. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;
 3. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 10. November 2022 im Hinblick auf den Erlass der Richtlinie (EU) 2022/... des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen

(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 die Artikel 50 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

■

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses³⁶,

gemäß dem ordentlichen Gesetzgebungsverfahren³⁷,

³⁶ ABl. C 517 vom 22.12.2021, S. 51.

³⁷ Standpunkt des Europäischen Parlaments vom 10. November 2022.

in Erwägung nachstehender Gründe:

- (1) In ihrer Mitteilung vom 11. Dezember 2019 mit dem Titel „Der europäische Grüne Deal“ verpflichtete sich die Europäische Kommission, die die nichtfinanzielle Berichterstattung betreffenden Bestimmungen der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates³⁸ zu überprüfen. Der Grüne Deal ist die neue Wachstumsstrategie der Union. Er zielt darauf ab, die Union bis 2050 zu einer modernen, ressourcenschonenden und wettbewerbsfähigen Wirtschaft ohne Netto-Treibhausgasemissionen zu machen. Außerdem soll er das Naturkapital der Union schützen, bewahren und verbessern und die Gesundheit und das Wohlergehen der Unionsbürgerinnen und -bürger vor umweltbedingten Risiken und Auswirkungen schützen. Der Grüne Deal ist ferner darauf ausgerichtet, das Wirtschaftswachstum von der Ressourcennutzung zu entkoppeln und sicherzustellen, dass alle Regionen und Unionsbürgerinnen und -bürger an einem sozial gerechten Übergang zu einem nachhaltigen Wirtschaftssystem teilhaben, **sodass niemand zurückgelassen und kein Standort abgehängt wird**. Er wird zu den Zielen beitragen, eine Wirtschaft im Dienste der Menschen aufzubauen, die soziale Marktwirtschaft der Union zu stärken und sicherzustellen, dass diese zukunftsfähig ist und Stabilität, Arbeitsplätze, Wachstum und **nachhaltige** Investitionen schafft.

³⁸ 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).

Diese Ziele sind insbesondere angesichts der durch die COVID-19-Pandemie entstandenen sozioökonomischen Schäden und der Notwendigkeit einer nachhaltigen, inklusiven und fairen Erholung von besonderer Bedeutung. **Mit der Verordnung (EU) 2021/1119 des Europäischen Parlaments und des Rates³⁹** wird das Ziel der Klimaneutralität bis 2050 in der Union verbindlich gemacht. **Darüber hinaus verpflichtet sich die Kommission in ihrer Mitteilung vom 20. Mai 2020 mit dem Titel „EU-Biodiversitätsstrategie für 2030 – Mehr Raum für die Natur in unserem Leben“, dafür zu sorgen, dass bis 2050 alle Ökosysteme weltweit wiederhergestellt, widerstandsfähig und angemessen geschützt sind. Ziel dieser Strategie ist es, die biologische Vielfalt in Europa bis 2030 auf einen Pfad der Erholung zu bringen.**

³⁹ **Verordnung (EU) 2021/1119 des Europäischen Parlaments und des Rates vom 30. Juni 2021 zur Schaffung des Rahmens für die Verwirklichung der Klimaneutralität und zur Änderung der Verordnungen (EG) Nr. 401/2009 und (EU) 2018/1999 („Europäisches Klimagesetz“) (ABl. L 243 vom 9.7.2021, S. 1).**

- (2) In ihrer Mitteilung vom 8. März 2018 mit dem Titel „Aktionsplan: Finanzierung nachhaltigen Wachstums“ (im Folgenden "Aktionsplan zur Finanzierung nachhaltigen Wachstums") legte die Kommission Maßnahmen dar, mit denen folgende Ziele erreicht werden sollen: Umlenkung der Kapitalflüsse auf nachhaltige Investitionen, um ein nachhaltiges und inklusives Wachstum zu erreichen, Bewältigung finanzieller Risiken, die sich aus dem Klimawandel, der Ressourcenknappheit, der Umweltzerstörung und sozialen Problemen ergeben, und Förderung von Transparenz und Langfristigkeit in der Finanz- und Wirtschaftstätigkeit. Eine Grundvoraussetzung für die Erreichung dieser Ziele ist, dass Unternehmen **bestimmte Kategorien** relevanter, vergleichbarer und zuverlässiger Nachhaltigkeitsinformationen offenlegen. Im Zuge der Umsetzung des Aktionsplans zur Finanzierung nachhaltigen Wachstums haben das Europäische Parlament und der Rat eine Reihe von Rechtsakten angenommen. So regelt die Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates⁴⁰, wie Finanzmarktteilnehmer und Finanzberater Nachhaltigkeitsinformationen gegenüber Endanlegern und Eigentümern von Vermögenswerten offenzulegen haben.

⁴⁰ Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27. November 2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor (ABl. L 317 vom 9.12.2019, S. 1).

Mit der Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates⁴¹ wird ein Klassifikationssystem für ökologisch nachhaltige Wirtschaftstätigkeiten geschaffen, um nachhaltige Investitionen zu fördern und gegen das „Greenwashing“ von zu Unrecht als nachhaltig dargestellten Finanzprodukten vorzugehen. Mit der Verordnung (EU) 2019/2089 des Europäischen Parlaments und des Rates⁴², ergänzt durch die Delegierten Verordnungen (EU) 2020/1816⁴³, (EU) 2020/1817⁴⁴ und (EU) 2020/1818⁴⁵ der Kommission, werden Offenlegungsanforderungen für Referenzwert-Administratoren im Hinblick auf Umwelt-, Sozial- und Governance-Faktoren (ESG) sowie Mindeststandards für EU-Referenzwerte für den klimabedingten Wandel und für Paris-abgestimmte EU-Referenzwerte eingeführt.

⁴¹ Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088 (ABl. L 198 vom 22.6.2020, S. 13).

⁴² Verordnung (EU) 2019/2089 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Verordnung (EU) 2016/1011 hinsichtlich EU-Referenzwerten für den klimabedingten Wandel, hinsichtlich auf das Übereinkommen von Paris abgestimmter EU-Referenzwerte sowie hinsichtlich nachhaltigkeitsbezogener Offenlegungen für Referenzwerte (ABl. L 317 vom 9.12.2019, S. 17).

⁴³ Delegierte Verordnung (EU) 2020/1816 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates hinsichtlich der Erläuterung in der Referenzwert-Erklärung, wie Umwelt-, Sozial- und Governance-Faktoren in den einzelnen Referenzwerten, die zur Verfügung gestellt und veröffentlicht werden, berücksichtigt werden (ABl. L 406 vom 3.12.2020, S. 1).

⁴⁴ Delegierte Verordnung (EU) 2020/1817 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates hinsichtlich des Mindestinhalts der Erläuterung, wie Umwelt-, Sozial- und Governance-Faktoren in der Referenzwert-Methodik berücksichtigt werden (ABl. L 406 vom 3.12.2020, S. 12).

⁴⁵ Delegierte Verordnung (EU) 2020/1818 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates im Hinblick auf Mindeststandards für EU-Referenzwerte für den klimabedingten Wandel und für Paris-abgestimmte EU-Referenzwerte (ABl. L 406 vom 3.12.2020, S. 17).

Nach der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates⁴⁶ müssen große Institute, die zum Handel an einem geregelten Markt zugelassene Wertpapiere emittiert haben, ab dem 28. Juni 2022 Informationen zu ESG-Risiken offenlegen. Der mit der Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates⁴⁷ und der Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates⁴⁸ geschaffene Aufsichtsrahmen für Wertpapierfirmen enthält Bestimmungen zur Einbeziehung von ESG-Risiken in den Prozess der aufsichtlichen Überprüfung und Bewertung (Supervisory Review and Evaluation Process, SREP) durch die zuständigen Behörden sowie Anforderungen bezüglich der Offenlegung von ESG-Risiken durch Wertpapierfirmen, die ab dem 26. Dezember 2022 gelten. Am 6. Juli 2021 verabschiedete die Kommission außerdem einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische grüne Anleihen, womit dem Aktionsplan zur Finanzierung nachhaltigen Wachstums Folge geleistet werden soll.

⁴⁶ 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).

⁴⁷ 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).

⁴⁸ 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).

- (3) *In ihrer Mitteilung vom 17. Juni 2019 mit dem Titel „Leitlinien für die Berichterstattung über nichtfinanzielle Informationen: Nachtrag zur klimabezogenen Berichterstattung“ (im Folgenden „Leitlinien für die klimabezogene Berichterstattung“) hat die Kommission die Vorteile hervorgehoben, die die Berichterstattung über klimabezogene Informationen für Unternehmen mit sich bringt, insbesondere durch die stärkere Sensibilisierung und das bessere Verständnis hinsichtlich klimabezogener Risiken und Chancen innerhalb des Unternehmens, die Diversifizierung der Anlegerbasis, die Senkung der Kapitalkosten und die Verbesserung des konstruktiven Dialogs mit allen Interessenträgern. Des Weiteren könnte sich Vielfalt in Leitungsorganen von Unternehmen auf die Entscheidungsfindung, die Unternehmensführung und die Widerstandsfähigkeit auswirken.*
- (4) In seinen Schlussfolgerungen vom 5. Dezember 2019 zur Vertiefung der Kapitalmarktunion betonte der Rat die Bedeutung zuverlässiger, vergleichbarer und relevanter Informationen zu Risiken, Chancen und Auswirkungen von Nachhaltigkeit und forderte die Kommission auf, die Entwicklung eines europäischen Standards für die nichtfinanzielle Berichterstattung in Erwägung zu ziehen.

- (5) In seiner Entschließung vom 29. Mai 2018 zu einem nachhaltigen Finanzwesen⁴⁹ forderte das Europäische Parlament die Weiterentwicklung der Anforderungen an die nichtfinanzielle Berichterstattung im Rahmen der Richtlinie 2013/34/EU. In seiner Entschließung vom 17. Dezember 2020 zu der nachhaltigen Unternehmensführung⁵⁰ begrüßte das Europäische Parlament die Zusage der Kommission zur Überarbeitung der Richtlinie 2013/34/EU und wies darauf hin, dass ein umfassender Unionsrahmen für die Angabe nichtfinanzieller Informationen geschaffen werden müsse, der verpflichtende Standards der Union für die Berichterstattung über nichtfinanzielle Informationen enthält. Das Europäische Parlament forderte ferner eine Erweiterung des Geltungsbereichs der Berichterstattungsanforderungen auf weitere Unternehmenskategorien sowie die Einführung einer Prüfungspflicht.

⁴⁹ ABl. C 76 vom 9.3.2020, S. 23.

⁵⁰ ABl. C 445 vom 29.10.2021, S. 94.

- (6) In seiner Resolution vom 25. September 2015 mit dem Titel „Transformation unserer Welt: Agenda 2030 für nachhaltige Entwicklung“ (im Folgenden „Agenda 2030“) verabschiedete die Generalversammlung der Vereinten Nationen einen neuen globalen Rahmen zur nachhaltigen Entwicklung. Die Agenda 2030 hat als Kernstück die Ziele der Vereinten Nationen für nachhaltige Entwicklung und deckt die drei Dimensionen der Nachhaltigkeit ab: die wirtschaftliche, soziale und die Umweltdimension. In der Mitteilung der Kommission vom 22. November 2016 mit dem Titel „Auf dem Weg in eine nachhaltige Zukunft – Europäische Nachhaltigkeitspolitik“ wurden die Ziele für nachhaltige Entwicklung mit dem politischen Rahmen der Union verbunden, um sicherzustellen, dass bei allen innen- und außenpolitischen Maßnahmen und Initiativen der Union diese Ziele von Beginn an mitberücksichtigt werden. In seinen Schlussfolgerungen vom 20. Juni 2017 mit dem Titel „Eine nachhaltige Zukunft für Europa: Reaktion der EU auf die Agenda 2030 für nachhaltige Entwicklung“ bekräftigte der Rat die Entschlossenheit der Union und ihrer Mitgliedstaaten, die Agenda 2030 vollständig, kohärent, umfassend, integrativ und wirksam sowie in enger Zusammenarbeit mit den Partnern und anderen Akteuren umzusetzen.

- (7) Mit der Richtlinie 2014/95/EU des Europäischen Parlaments und des Rates⁵¹ wurde die Richtlinie 2013/34/EU im Hinblick auf die Offenlegung nichtfinanzieller Informationen durch bestimmte große Unternehmen und Gruppen geändert. Mit der Richtlinie 2014/95/EU wurden Unternehmen verpflichtet, mindestens über Umwelt-, Sozial-, und Arbeitnehmerbelange, die Achtung der Menschenrechte und die Bekämpfung von Korruption und Bestechung Bericht zu erstatten und dabei Informationen zu folgenden Berichterstattungsbereichen offenzulegen: Geschäftsmodell; Konzepte, einschließlich der Due-Diligence-Prozesse; Ergebnisse dieser Konzepte; Risiken und deren Handhabung sowie wichtigste Leistungsindikatoren, die für die betreffende Geschäftstätigkeit von Bedeutung sind.

⁵¹ Richtlinie 2014/95/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2014 zur Änderung der Richtlinie 2013/34/EU im Hinblick auf die Angabe nichtfinanzieller und die Diversität betreffender Informationen durch bestimmte große Unternehmen und Gruppen (ABl. L 330 vom 15.11.2014, S. 1).

- (8) Viele Interessenträger halten den Begriff „nichtfinanziell“ für unzutreffend, insbesondere, weil er impliziert, dass betreffende Informationen in finanzieller Hinsicht nicht von Relevanz sind. Allerdings haben solche Informationen zunehmend sehr wohl finanzielle Relevanz. Viele einschlägige Organisationen, Initiativen und Fachleute im Bereich Nachhaltigkeitsberichterstattung verwenden den Begriff „Nachhaltigkeitsinformationen“. Deshalb sollte anstelle des Begriffs „nichtfinanzielle Informationen“ vorzugsweise der Begriff „Nachhaltigkeitsinformationen“ verwendet werden. Daher sollte die Richtlinie 2013/34/EU geändert werden, um dieser neuen Terminologie Rechnung zu tragen.

- (9) Wenn Unternehmen eine bessere Nachhaltigkeitsberichterstattung durchführen würden, würde dies letztendlich Bürgerinnen und Bürgern und Sparern, ***einschließlich Gewerkschaften und Arbeitnehmervertretern***, zugutekommen, ***indem sie angemessen informiert wären und sich so besser in den sozialen Dialog einbringen könnten***. Sparer, die nachhaltig investieren wollen, werden fortan die Möglichkeit haben, dies zu tun, während von einem stabilen, nachhaltigen und inklusiven Wirtschaftssystem alle Bürgerinnen und Bürger profitieren würden. Damit sich diese Vorteile auch verwirklichen, müssen die in den Jahresberichten der Unternehmen offengelegten Nachhaltigkeitsinformationen zunächst zwei Hauptnutzergruppen erreichen. Bei der ersten Gruppe von Nutzern handelt es sich um Anleger, einschließlich Vermögensverwalter, die die Risiken und Chancen von Nachhaltigkeitsfragen für ihre Investitionen sowie die Auswirkungen entsprechender Investitionen auf Mensch und Umwelt besser verstehen wollen. Bei der zweiten Gruppe handelt es sich um ***Akteure der Zivilgesellschaft***, einschließlich Nichtregierungsorganisationen und Sozialpartner, die Unternehmen im Hinblick auf ihre Auswirkungen auf Mensch und Umwelt stärker in die Verantwortung nehmen wollen. Die in den Jahresberichten offengelegten Nachhaltigkeitsinformationen könnten auch von anderen Interessenträgern genutzt werden, ***insbesondere zur Erhöhung der Vergleichbarkeit zwischen Marktsektoren und innerhalb von Marktsektoren***. So könnten Geschäftspartner von Unternehmen, einschließlich Kunden, sich auf Nachhaltigkeitsinformationen stützen, um ihre Nachhaltigkeitsrisiken und -auswirkungen über die gesamte Wertschöpfungskette hinweg zu verstehen und gegebenenfalls darüber Bericht zu erstatten. Politische Entscheidungsträger und Umweltagenturen können diese Informationen – insbesondere in aggregierter Form – nutzen, um ökologische und soziale Entwicklungen zu überwachen, die umweltökonomische Gesamtrechnung zu fördern und die öffentliche Politik zu informieren. Zwar konsultieren nur wenige Bürgerinnen und Bürger und Verbraucher die Jahresberichte von Unternehmen direkt, doch könnten sie die darin enthaltenen Nachhaltigkeitsinformationen indirekt nutzen, z. B. bei der Prüfung von Empfehlungen oder Stellungnahmen von Finanzberatern oder Nichtregierungsorganisationen. Viele Anleger und Vermögensverwalter erwerben Nachhaltigkeitsinformationen von externen Datenanbietern, die diese verschiedenen Quellen, unter anderem öffentlichen

Unternehmensberichten, entnehmen und sammeln.

- (10) *Der Markt für Nachhaltigkeitsinformationen wächst schnell, und angesichts neuer Verpflichtungen, die Anleger und Vermögensverwalter erfüllen müssen, gewinnt die Rolle der Drittanbieter von Daten an Bedeutung. Da zunehmend aufgeschlüsselte Daten zur Verfügung stehen, dürften Nachhaltigkeitsinformationen kostengünstiger werden. Mit den in dieser Änderungsrichtlinie vorgesehenen Änderungen der Richtlinie 2013/34/EU wird darauf abgezielt, die Vergleichbarkeit von Daten zu erhöhen und Standards anzugleichen. Es wird erwartet, dass sich die Verfahren der Drittanbieter von Daten verbessern werden und die Sachkenntnis in diesem Bereich zunehmen wird, was Potenzial für die Schaffung neuer Arbeitsplätze birgt.*

- (11) Die Nachfrage nach Nachhaltigkeitsinformationen von Unternehmen ist in den letzten Jahren sehr stark gestiegen, insbesondere seitens der Anleger. Dieser Anstieg bei der Nachfrage ergibt sich daraus, dass sich die Art der Risiken für Unternehmen im Wandel befindet und das Bewusstsein der Anleger für die finanziellen Auswirkungen jener Risiken zunimmt. Dies gilt insbesondere für klimabezogene finanzielle Risiken. Es gibt auch ein wachsendes Bewusstsein für Risiken **und Chancen**, die sich für Unternehmen und Investitionen im Zusammenhang mit sonstigen Umweltfragen, **etwa was den Verlust der biologischen Vielfalt anbelangt, sowie** Gesundheitsfragen **und sozialen Fragen, einschließlich der Kinder- und der Zwangsarbeit**, ergeben. Der Anstieg bei der Nachfrage nach Nachhaltigkeitsinformationen wird auch durch die Zunahme von Anlageprodukten angetrieben, deren erklärtes Ziel es ist, bestimmte Nachhaltigkeitsstandards zu erfüllen oder bestimmte Nachhaltigkeitsziele zu erreichen **und für Kohärenz mit den Zielen des am 12. Dezember 2015 angenommenen Übereinkommens von Paris im Rahmen des Rahmenübereinkommens der Vereinten Nationen über Klimaänderungen (im Folgenden „Übereinkommen von Paris“), des Übereinkommens der Vereinten Nationen über die biologische Vielfalt und der Politik der Union zu sorgen**. Zum Teil ist dieser Anstieg die logische Konsequenz zuvor erlassener Rechtsvorschriften der Union, insbesondere der Verordnungen (EU) 2019/2088 und (EU) 2020/852. Angesichts des raschen Wandels im öffentlichen Bewusstsein, bei Verbraucherpräferenzen und Marktpraktiken wäre ein Teil dieses Anstiegs jedoch in jedem Fall eingetreten. Die COVID-19-Pandemie hat dazu geführt, dass der Informationsbedarf der Nutzer weiter zunimmt, zumal sie die Schwachstellen im Hinblick auf Arbeitnehmer sowie auf Wertschöpfungsketten von Unternehmen offengelegt hat. Informationen zu Umweltauswirkungen sind auch mit Blick auf die Abmilderung künftiger Pandemien relevant, da das Auftreten und die Ausbreitung von Krankheiten zunehmend mit menschenverursachten Störungen von Ökosystemen in Verbindung stehen.

- (12) Auch den Unternehmen selbst kommt eine qualitativ hochwertige Berichterstattung zu Nachhaltigkeitsaspekten zugute. Die wachsende Zahl der auf Nachhaltigkeitsziele ausgerichteten Anlageprodukte zeigt, dass Unternehmen durch eine gute Nachhaltigkeitsberichterstattung einen besseren Zugang zu Finanzkapital erlangen können. Die Nachhaltigkeitsberichterstattung kann es Unternehmen erleichtern, die eigenen Risiken und Chancen im Zusammenhang mit Nachhaltigkeitsaspekten zu ermitteln und zu steuern. Sie kann ferner als Grundlage für einen besseren Dialog und eine bessere Kommunikation zwischen Unternehmen und ihren Interessenträgern dienen und Unternehmen zu einem besseren Ruf verhelfen.

Darüber hinaus würde eine einheitliche Grundlage für die Nachhaltigkeitsberichterstattung in Form von Standards für die Nachhaltigkeitsberichterstattung dazu führen, dass relevante und ausreichende Informationen bereitgestellt werden und somit die Zahl von Ad-hoc-Auskunftsersuchen erheblich verringern.

- (13) Im Bericht der Kommission vom 21. April 2021 über die Überprüfungsklausel der Richtlinien 2013/34/EU, 2014/95/EU und 2013/50/EU und in der dazugehörigen Eignungsprüfung der Berichterstattung von Unternehmen (im Folgenden „Bericht der Kommission über die Überprüfungsklauseln und die dazugehörige Eignungsprüfung“) wurden Probleme hinsichtlich der Wirksamkeit der Richtlinie 2014/95/EU aufgezeigt. Es gibt deutliche Hinweise darauf, dass viele Unternehmen nicht zu allen wichtigen Nachhaltigkeitsthemen wesentliche Informationen offenlegen, **einschließlich Informationen im Zusammenhang mit dem Klima, etwa zu allen Treibhausgasemissionen und Faktoren, die die Biodiversität beeinträchtigen.** In dem Bericht wurden auch die begrenzte Vergleichbarkeit und Zuverlässigkeit von Nachhaltigkeitsinformationen als erhebliche Probleme ausgemacht. Darüber hinaus sind viele Unternehmen, deren Nachhaltigkeitsinformationen Nutzer benötigen würden, nicht zur Berichterstattung über Informationen verpflichtet. **Dementsprechend besteht ein eindeutiger Bedarf an einem soliden und erschwinglichen Rahmen für die Berichterstattung, der mit wirksamen Prüfverfahren einhergeht, um die Zuverlässigkeit der Daten zu gewährleisten und „Greenwashing“ sowie Doppelzählung zu verhindern.**

- (14) Ohne ein politisches Handeln dürfte die Kluft zwischen dem Informationsbedarf der Nutzer und den von den Unternehmen bereitgestellten Nachhaltigkeitsinformationen wachsen. Diese Kluft hat erhebliche negative Auswirkungen. So sind Anleger nicht in der Lage, Risiken und Chancen im Zusammenhang mit Nachhaltigkeitsfragen bei ihren Anlageentscheidungen hinreichend zu berücksichtigen. Gebündelt können eine Vielzahl von Anlageentscheidungen, bei denen Nachhaltigkeitsrisiken nicht angemessen Rechnung getragen wird, potenziell zu systemischen Risiken und somit zu einer Gefährdung der Finanzstabilität führen. Die Europäische Zentralbank (EZB) und internationale Organisationen wie der Rat für Finanzstabilität haben auf diese Systemrisiken hingewiesen, insbesondere in Bezug auf Klimafragen. Darüber hinaus ist es so für Anleger schwieriger, Finanzmittel in Unternehmen und Wirtschaftstätigkeiten zu investieren, die soziale und ökologische Probleme nicht verschärfen, sondern zu ihrer Lösung beitragen, wodurch die Ziele des Grünen Deals, des Aktionsplans zur Finanzierung nachhaltigen Wachstums **und des Übereinkommens von Paris** untergraben werden. Nichtregierungsorganisationen, Sozialpartner, von den Tätigkeiten der Unternehmen betroffene Gemeinschaften und andere Interessenträger sind weniger in der Lage, Unternehmen im Hinblick auf ihre Auswirkungen auf Mensch und Umwelt in die Verantwortung zu nehmen. Dies führt zu einem Mangel an Rechenschaftspflicht und könnte bewirken, dass Bürgerinnen und Bürger weniger Vertrauen in Unternehmen haben, was wiederum negative Auswirkungen auf das reibungslose Funktionieren der sozialen Marktwirtschaft haben könnte. Überdies macht es der Mangel an allgemein anerkannten Parametern und Methoden für die Messung, Bewertung und Bewältigung von Nachhaltigkeitsrisiken für Unternehmen schwieriger, ihre Geschäftsmodelle und Tätigkeiten nachhaltig zu gestalten. **Der Mangel an von Unternehmen bereitgestellten Nachhaltigkeitsinformationen schränkt zudem die Fähigkeit der Interessenträger ein, darunter die Akteure der Zivilgesellschaft, die Gewerkschaften und die Arbeitnehmervertreter, mit den Unternehmen einen Dialog über Nachhaltigkeitsaspekte aufzunehmen.**

- (15) Im Bericht der Kommission über die Überprüfungsklauseln und in der dazugehörigen Eignungsprüfung wurde zudem eine erhebliche Zunahme der an Unternehmen gerichteten Ersuchen um Informationen zu Nachhaltigkeitsaspekten, die darauf abzielen, die bestehende Informationslücke zwischen dem Informationsbedarf der Nutzer und den vorhandenen Nachhaltigkeitsinformationen von Unternehmen zu schließen, aufgezeigt. Darüber hinaus dürften die vorherrschenden Erwartungen gegenüber Unternehmen, eine Vielzahl unterschiedlicher Rahmen und Standards zu verwenden, anhalten und sich möglicherweise sogar noch verstärken, da immer mehr Wert auf Nachhaltigkeitsinformationen gelegt wird. Ohne ein politisches Handeln zur Bildung eines Konsenses über die von den Unternehmen bereitzustellenden Informationen werden die Kosten und der Aufwand für Bericht erstattende Unternehmen und die Nutzer solcher Informationen erheblich steigen.
- (16) Die bestehende Informationslücke erhöht die Wahrscheinlichkeit, dass einzelne Mitgliedstaaten zunehmend voneinander abweichende nationale Vorschriften oder Standards einführen werden. Unterschiedliche Berichterstattungsanforderungen in den einzelnen Mitgliedstaaten könnten zu zusätzlichen Kosten und mehr Komplexität für grenzüberschreitend tätige Unternehmen führen und somit den Binnenmarkt sowie das Niederlassungsrecht und den freien Kapitalverkehr in der gesamten Union untergraben. Diese unterschiedlichen Berichterstattungsanforderungen könnten auch dazu führen, dass Informationen, über die Bericht erstattet wurde, grenzübergreifend weniger gut vergleichbar sind, was eine Beeinträchtigung der Kapitalmarktunion zur Folge hat.

- (17) Die Artikel 19a und 29a der Richtlinie 2013/34/EU gelten für große Unternehmen von öffentlichem Interesse mit einer durchschnittlichen Mitarbeiterzahl von mehr als 500 bzw. für Unternehmen von öffentlichem Interesse, bei denen es sich um Mutterunternehmen einer großen Gruppe mit einer durchschnittlichen Mitarbeiterzahl von mehr als 500 auf konsolidierter Basis handelt. Angesichts des wachsenden Bedarfs der Nutzer an Nachhaltigkeitsinformationen sollten zusätzliche Kategorien von Unternehmen zur Berichterstattung über Nachhaltigkeitsinformationen verpflichtet werden. Daher sollten sämtliche großen Unternehmen sowie sämtliche Unternehmen – mit Ausnahme von Kleinstunternehmen –, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, dazu verpflichtet werden, Nachhaltigkeitsinformationen bereitzustellen. ***In den Bestimmungen dieser Änderungsrichtlinie, mit denen die Artikel 19a und 29a der Richtlinie 2013/34/EU geändert werden, wird der Umfang der Berichterstattungsanforderungen unter Bezugnahme auf die Artikel 2 und 3 der Richtlinie 2013/34/EU ausdrücklich festgelegt. Daher stellen sie keine Vereinfachung oder Änderung einer anderen Anforderung dar, und die Einschränkung der Befreiungen für Unternehmen von öffentlichem Interesse gemäß Artikel 40 der Richtlinie 2013/34/EU findet keine Anwendung. Insbesondere sollten Unternehmen von öffentlichem Interesse für die Zwecke der Anwendung der Anforderungen an die Nachhaltigkeitsberichterstattung nicht als große Unternehmen behandelt werden. Dementsprechend sollten kleine und mittlere Unternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind und bei denen es sich um Unternehmen von öffentlichem Interesse handelt, gemäß den Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen Bericht erstatten dürfen.*** Darüber hinaus sollten alle Unternehmen, die Mutterunternehmen einer großen Gruppe sind, Nachhaltigkeitsberichte auf Gruppenebene erstellen. ***Da in Artikel 8 der Verordnung (EU) 2020/852 zudem auf Artikel 19a und Artikel 29a der Richtlinie 2013/34/EU Bezug genommen wird, werden die Unternehmen, die in den Anwendungsbereich der Anforderungen der Nachhaltigkeitsberichterstattung aufgenommen wurden, auch Artikel 8 der Verordnung (EU) 2020/852 einhalten müssen.***

- (18) Die Anforderung dieser Änderungsrichtlinie, dass auch große Unternehmen, deren Wertpapiere nicht zum Handel auf einem geregelten Markt in der Union zugelassen sind, Informationen zu Nachhaltigkeitsaspekten offenlegen sollten, liegt in erster Linie in Bedenken hinsichtlich der Auswirkungen und der Rechenschaftspflicht solcher Unternehmen, auch im Hinblick auf ihre Wertschöpfungsketten, begründet. Für sämtliche großen Unternehmen sollten demnach dieselben Anforderungen zur öffentlichen Berichterstattung über Nachhaltigkeitsinformationen gelten. Darüber hinaus benötigen auch Finanzmarktteilnehmer Informationen von solchen großen Unternehmen, deren Wertpapiere nicht zum Handel auf einem geregelten Markt **in der Union** zugelassen sind.
- (19) Mit der Anforderung dieser Änderungsrichtlinie, dass auch Drittlandsunternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, Informationen zu Nachhaltigkeitsaspekten offenlegen sollten, soll dem Umstand Rechnung getragen werden, dass Finanzmarktteilnehmer die Informationen solcher Unternehmen benötigen, um die Risiken und Auswirkungen ihrer Investitionen verstehen und ihre in der Verordnung (EU) 2019/2088 festgelegten Offenlegungspflichten erfüllen zu können.

- (20) *Drittlandsunternehmen, die in erheblichem Umfang im Hoheitsgebiet der Union tätig sind, sollten ebenfalls verpflichtet werden, Nachhaltigkeitsinformationen vorzulegen, insbesondere über ihre Auswirkungen auf soziale und ökologische Belange, um sicherzustellen, dass Drittlandsunternehmen für ihre Auswirkungen auf Mensch und Umwelt verantwortlich sind und dass für die im Binnenmarkt tätigen Unternehmen gleiche Wettbewerbsbedingungen herrschen. Daher sollten Drittlandsunternehmen, die in der Union einen Nettoumsatz von mehr als 150 Mio. EUR erzielen und über ein Tochterunternehmen oder eine Zweigniederlassung im Gebiet der Union verfügen, den Anforderungen der Union an die Nachhaltigkeitsberichterstattung unterliegen. Um die Verhältnismäßigkeit und Durchsetzbarkeit solcher Anforderungen zu gewährleisten, sollte der Schwellenwert eines Nettoumsatzes von mehr als 40 Mio. EUR auch für die Zweigniederlassungen von Unternehmen aus Drittländern gelten, und die Schwellenwerte in Bezug auf die Einordnung als großes Unternehmen oder als kleines oder mittleres Unternehmen, dessen Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, sollte für die Tochterunternehmen von Drittlandsunternehmen gelten, da diese Tochterunternehmen und Zweigniederlassungen für die Veröffentlichung des Nachhaltigkeitsberichts des Drittlandsunternehmens verantwortlich sein sollten.*

Die von dem Tochterunternehmen oder der Zweigniederlassung eines Drittlandsunternehmens veröffentlichten Nachhaltigkeitsberichte sollten im Einklang mit Standards erstellt werden, die bis zum 30. Juni 2024 von der Kommission im Wege delegierter Rechtsakte verabschiedet werden. Das Tochterunternehmen oder die Zweigniederlassung eines Drittlandsunternehmens sollte zudem in der Lage sein, gemäß den Standards, die für in der Union niedergelassene Unternehmen gelten, oder gemäß Standards, die gemäß einem Durchführungsrechtsakt als gleichwertig gelten, Bericht zu erstatten. Werden von dem Drittlandsunternehmen nicht alle gemäß dieser Änderungsrichtlinie erforderlichen Informationen zur Verfügung gestellt, obwohl sich das Tochterunternehmen oder die Zweigniederlassung dieses Drittlandsunternehmens nach besten Kräften bemüht hat, die erforderlichen Informationen einzuholen, so sollte dieses Tochterunternehmen oder diese Zweigniederlassung alle in seinem/ihrem Besitz befindlichen Informationen zur Verfügung stellen und eine Erklärung abgeben, aus der hervorgeht, dass das Drittlandsunternehmen die restlichen erforderlichen Informationen nicht zur Verfügung gestellt hat. Um die Qualität und Zuverlässigkeit der Berichterstattung zu gewährleisten, sollten die Nachhaltigkeitsberichte von Drittlandsunternehmen zusammen mit einem Bestätigungsurteil veröffentlicht werden, das einem von einer Person oder Gesellschaft abgegebenen wurde, die nach dem nationalen Recht des Drittlandsunternehmens oder eines Mitgliedstaats zur Abgabe eines Bestätigungsurteils über die Nachhaltigkeitsberichterstattung befugt ist. Wird ein solches Bestätigungsurteil nicht abgegeben, sollte das Tochterunternehmen oder die Zweigniederlassung des Drittlandsunternehmens eine Erklärung abgeben, aus der hervorgeht, dass das Drittlandsunternehmen das erforderliche Bestätigungsurteil nicht abgegeben hat.

Der Nachhaltigkeitsbericht sollte der Öffentlichkeit über die Zentral-, Handels- oder Gesellschaftsregister der Mitgliedstaaten oder alternativ auf der Website des Tochterunternehmens oder der Zweigniederlassung des Drittlandsunternehmens kostenlos zugänglich gemacht werden. Die Mitgliedstaaten sollten in der Lage sein, die Kommission jährlich über die Tochterunternehmen oder Zweigniederlassungen der Drittlandsunternehmen zu informieren, die die Veröffentlichungspflicht erfüllt haben, sowie über die Fälle, in denen zwar ein Bericht veröffentlicht wurde, das Tochterunternehmen oder die Zweigniederlassung des Drittlandsunternehmens jedoch erklärt hat, dass es/sie die erforderlichen Informationen von dem Drittlandsunternehmen nicht einholen konnte. Die Kommission sollte auf ihrer Website eine Liste der Drittlandsunternehmen öffentlich zugänglich machen, die einen Nachhaltigkeitsbericht veröffentlicht haben.

- (21) Angesichts der zunehmenden Bedeutung von Nachhaltigkeitsrisiken und unter Berücksichtigung der Tatsache, dass kleine und mittlere Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, einen erheblichen Anteil aller Unternehmen ausmachen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, sollten zur Gewährleistung des Anlegerschutzes auch kleine und mittlere Unternehmen – mit Ausnahme von Kleinstunternehmen –, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, verpflichtet werden, Informationen zu Nachhaltigkeitsaspekten offenzulegen. Mit der Einführung dieser Anforderung wird mit dazu beigetragen, dass Finanzmarktteilnehmer auch kleinere Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, in ihre Anlageportfolios aufnehmen können, da diese sodann die von Finanzmarktteilnehmern benötigten Nachhaltigkeitsinformationen bereitstellen. So wird dazu beigetragen, den Zugang kleinerer Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, zu Finanzkapital zu erhalten und zu verbessern und zu vermeiden, dass solche Unternehmen von den Finanzmarktteilnehmern vernachlässigt werden. Die Einführung der Anforderung für kleine und mittlere Unternehmen – mit Ausnahme von Kleinstunternehmen –, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, Informationen zu Nachhaltigkeitsaspekten offenzulegen, ist überdies erforderlich, um sicherzustellen, dass Finanzmarktteilnehmer über die Informationen verfügen, die sie von den Unternehmen, in die investiert wird, benötigen, um ihre eigenen nachhaltigkeitsbezogenen Offenlegungspflichten gemäß der Verordnung (EU) 2019/2088 erfüllen zu können. Kleinen und mittleren Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, sollte **die Möglichkeit gegeben werden, sich bei ihrer Berichterstattung nach Standards zu richten, die in einem angemessenen Verhältnis zu ihren Kapazitäten und Ressourcen stehen und dem Umfang und der Komplexität ihrer Tätigkeiten entsprechen**. Kleine und mittlere Unternehmen, deren Wertpapiere nicht **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, sollten ebenfalls die Möglichkeit haben, sich dafür zu entscheiden, solche verhältnismäßigen Standards freiwillig anzuwenden. Die Standards für die

Nachhaltigkeitsberichterstattung von kleinen und mittleren Unternehmen werden den in den Anwendungsbereich der durch diese Änderungsrichtlinie eingeführten Anforderungen fallenden Unternehmen als Referenz für den Umfang der Nachhaltigkeitsinformationen dienen, die sie von kleinen und mittleren Unternehmen, die Zulieferer oder Abnehmer entlang ihrer Wertschöpfungsketten dieser Unternehmen sind, vertretbarerweise verlangen können.

Kleinen und mittleren Unternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, sollte – aufgrund ihrer geringeren Größe und ihrer begrenzten Ressourcen sowie unter Berücksichtigung der schwierigen wirtschaftlichen Umstände infolge der COVID-19-Pandemie – zudem ausreichend Zeit eingeräumt werden, um sich auf die Anwendung der Bestimmungen, die die Nachhaltigkeitsberichterstattung vorschreiben, vorzubereiten. Daher sollten die Bestimmungen über die Nachhaltigkeitsberichterstattung von Unternehmen in Bezug auf kleine und mittlere Unternehmen – mit Ausnahme von Kleinstunternehmen –, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, für Geschäftsjahre gelten, die am oder nach dem 1. Januar 2026 beginnen. Nach diesem Datum sollten kleine und mittlere Unternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, während eines Übergangszeitraums von zwei Jahren die Möglichkeit haben, von den in dieser Änderungsrichtlinie festgelegten Anforderungen an die Nachhaltigkeitsberichterstattung abzuweichen, sofern sie in ihrem Lagebericht kurz darlegen, weshalb die Nachhaltigkeitsinformationen nicht bereitgestellt wurden.

- (22) *Den Mitgliedstaaten sollte es freistehen, die Auswirkungen ihrer nationalen Umsetzungsmaßnahmen auf kleine und mittlere Unternehmen zu prüfen, um sicherzustellen, dass sie nicht unverhältnismäßig beeinträchtigt werden, wobei Kleinstunternehmen besondere Aufmerksamkeit zu widmen und unnötiger Verwaltungsaufwand zu vermeiden ist. Die Mitgliedstaaten sollten die Einführung von Maßnahmen zur Unterstützung von kleinen und mittleren Unternehmen bei der Anwendung der Standards für die Nachhaltigkeitsberichterstattung in Erwägung ziehen.*

- (23) Die Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates⁵² gilt für Unternehmen, deren Wertpapiere ***zum Handel auf einem geregelten Markt in der Union zugelassen*** sind. Um sicherzustellen, dass Unternehmen, deren Wertpapiere ***zum Handel auf einem geregelten Markt in der Union zugelassen*** sind, einschließlich Emittenten aus einem Drittland, denselben Anforderungen an die Nachhaltigkeitsberichterstattung unterliegen, sollte die Richtlinie 2004/109/EG die erforderlichen Querverweise auf etwaige Anforderungen an die Nachhaltigkeitsberichterstattung im Jahresfinanzbericht enthalten.

⁵² Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates vom 15. Dezember 2004 zur Harmonisierung der Transparenzanforderungen in Bezug auf Informationen über Emittenten, deren Wertpapiere zum Handel auf einem geregelten Markt zugelassen sind, und zur Änderung der Richtlinie 2001/34/EG (ABl. L 390 vom 31.12.2004, S. 38).

- (24) Mit Artikel 23 Absatz 4 Unterabsatz 1 Buchstabe i und Artikel 23 Absatz 4 Unterabsatz 4 der Richtlinie 2004/109/EG wird der Kommission jeweils die Befugnis übertragen, Maßnahmen zur Einführung eines Mechanismus für die Feststellung der Gleichwertigkeit von gemäß jener Richtlinie erforderlichen Informationen bzw. zur Aufstellung allgemeiner Äquivalenzkriterien für Rechnungslegungsstandards zu erlassen. Nach Artikel 23 Absatz 4 Unterabsatz 3 der Richtlinie 2004/109/EG ist die Kommission zudem befugt, die notwendigen Beschlüsse über die Gleichwertigkeit der Rechnungslegungsstandards, die von Emittenten mit Sitz in Drittländern angewandt werden, zu fassen. Damit der Erweiterung der Richtlinie 2004/109/EG um Nachhaltigkeitsanforderungen Rechnung getragen ist, sollte der Kommission die Befugnis übertragen werden, einen Mechanismus für die Feststellung der Gleichwertigkeit der von Emittenten mit Sitz in Drittländern angewandten Standards für die Nachhaltigkeitsberichterstattung einzurichten, **ähnlich der bestehenden Verordnung (EG) Nr. 1569/2007 der Kommission⁵³, in der die Kriterien für die Feststellung der Gleichwertigkeit der von Emittenten mit Sitz in Drittländern angewandten Rechnungslegungsstandards festgelegt sind**. Aus demselben Grund sollte die Kommission zudem die Befugnis erhalten, die notwendigen Beschlüsse über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung, die von Emittenten mit Sitz in Drittländern angewandt werden, zu fassen. Die mit dieser Änderungsrichtlinie eingeführten Änderungen werden einheitliche Gleichwertigkeitsregelungen für die Anforderungen an die Nachhaltigkeitsberichterstattung und für die Anforderungen an die Finanzberichterstattung im Zusammenhang mit dem Jahresfinanzbericht sicherstellen.

⁵³ **Verordnung (EG) Nr. 1569/2007 der Kommission vom 21. Dezember 2007 über die Einrichtung eines Mechanismus zur Festlegung der Gleichwertigkeit der von Drittstaatemittenten angewandten Rechnungslegungsgrundsätze gemäß den Richtlinien 2003/71/EG und 2004/109/EG des Europäischen Parlaments und des Rates (ABl. L 340 vom 22.12.2007, S. 66).**

- (25) Nach Artikel 19a Absatz 3 und Artikel 29a Absatz 3 der Richtlinie 2013/34/EU sind sämtliche Tochterunternehmen von der Pflicht zur Berichterstattung über nichtfinanzielle Informationen befreit, sofern diese Unternehmen und ihre Tochterunternehmen in den konsolidierten Lagebericht ihres Mutterunternehmens einbezogen werden und dieser Bericht **nichtfinanzielle Informationen umfasst, die gemäß der genannten Richtlinie bereitzustellen sind**. Es muss jedoch sichergestellt werden, dass Nachhaltigkeitsinformationen für die Nutzer leicht zugänglich sind, und es muss für Transparenz hinsichtlich der Frage gesorgt werden, welches das auf Gruppenebene Bericht erstattende Mutterunternehmen des befreiten Tochterunternehmens ist. Diese Tochterunternehmen müssen daher verpflichtet werden, **in ihren Lagebericht den Namen und den Sitz des Mutterunternehmens, das über Nachhaltigkeitsinformationen auf Gruppenebene Bericht erstattet, die Weblinks zum konsolidierten Lagebericht ihres Mutterunternehmens und einen Hinweis darauf, dass sie von der Nachhaltigkeitsberichterstattung befreit sind, aufnehmen. Die Mitgliedstaaten sollten vorschreiben können, dass das Mutterunternehmen den konsolidierten Lagebericht in den von ihnen akzeptierten Sprachen veröffentlicht und die erforderlichen Übersetzungen in diese Sprachen vorlegt**. Derartige Befreiungen sollten auch dann gelten, wenn es sich bei dem auf Gruppenebene Bericht erstattenden Mutterunternehmen um ein Drittlandsunternehmen handelt, dessen Nachhaltigkeitsberichterstattung **gemäß gleichwertigen** Standards für die Nachhaltigkeitsberichterstattung **erfolgt**.

Die Richtlinie 2004/109/EG in der mit der vorliegenden Änderungsrichtlinie geänderten Fassung sollte geeignete Mechanismen zur Feststellung der Gleichwertigkeit von Standards für die Nachhaltigkeitsberichterstattung vorsehen, und Unternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, sowie Unternehmen, deren Wertpapiere nicht zum Handel auf einem geregelten Markt in der Union zugelassen sind, sollten einer Berichtspflicht nach denselben Standards für die Nachhaltigkeitsberichterstattung unterliegen. In diesem Zusammenhang sollten die gemäß Artikel 23 Absatz 4 Unterabsatz 1 Ziffer i und Artikel 23 Absatz 4 Unterabsatz 4 der Richtlinie 2004/109/EG von der Kommission erlassenen Durchführungsrechtsakte zur Einrichtung eines Mechanismus zur Feststellung der Gleichwertigkeit von Standards für die Feststellung verwendet werden, um zu bestimmen, ob Tochterunternehmen von Mutterunternehmen aus Drittländern im Rahmen der Regelung der Richtlinie 2013/34/EU zu befreien sind. Daher sollte das Tochterunternehmen befreit werden, wenn die konsolidierte Nachhaltigkeitsberichterstattung gemäß den nach dem durch die vorliegende Änderungsrichtlinie eingeführten Artikel 29b der Richtlinie 2013/34/EU von der Kommission erlassenen Standards für die Nachhaltigkeitsberichterstattung oder in einer Weise durchgeführt wurde, die diesen Standards für die Nachhaltigkeitsberichterstattung gleichwertig ist, was in einem gemäß Artikel 23 Absatz 4 Unterabsatz 3 der Richtlinie 2004/109/EG erlassenen Durchführungsrechtsakt über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung festgestellt wurde. Diese Befreiung sollte aus Gründen des Anlegerschutzes nicht für große Unternehmen gelten, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, um mehr Transparenz in Bezug auf diese Unternehmen sicherzustellen.

- (26) Nach Artikel 23 der Richtlinie 2013/34/EU sind Mutterunternehmen von der Verpflichtung zur Erstellung eines konsolidierten Abschlusses und eines konsolidierten Lageberichts ausgenommen, sofern sie Tochterunternehmen eines anderen Mutterunternehmens sind, das dieser Verpflichtung nachkommt. Es sollte jedoch präzisiert werden, dass die Ausnahmeregelung für konsolidierte Abschlüsse und konsolidierte Lageberichte unabhängig von der Ausnahmeregelung für die konsolidierte Nachhaltigkeitsberichterstattung Anwendung findet. Es ist daher möglich, dass ein Unternehmen von den Anforderungen zur konsolidierten Finanzberichterstattung, nicht aber von den Anforderungen zur konsolidierten Nachhaltigkeitsberichterstattung befreit ist, wenn sein oberstes Mutterunternehmen konsolidierte Abschlüsse und konsolidierte Lageberichte im Einklang mit dem Unionsrecht oder – im Fall von Unternehmen mit Sitz in einem Drittland – gemäß gleichwertigen Anforderungen erstellt, jedoch keine konsolidierte Nachhaltigkeitsberichterstattung im Einklang mit dem Unionsrecht oder – im Fall von Unternehmen mit Sitz in einem Drittland – gemäß gleichwertigen Anforderungen vornimmt. ***Mutterunternehmen, die auf Gruppenebene Bericht erstatten, müssen ein angemessenes Verständnis der Risiken für ihre Tochterunternehmen und der Auswirkungen ihrer Tochterunternehmen vermitteln, gegebenenfalls einschließlich Informationen über ihre Due-Diligence-Prozesse. Es kann Fälle geben, in denen die Unterschiede bei der Situation der Gruppe und der Situation ihrer einzelnen Tochterunternehmen oder bei der Situation einzelner Tochterunternehmen in verschiedenen Bereichen besonders groß sind und die Nutzer der Information in Ermangelung zusätzlicher Informationen über das betreffende Tochterunternehmen zu einer stark abweichenden Schlussfolgerung hinsichtlich der Risiken für ihre oder Auswirkungen ihres Tochterunternehmens veranlassen würden.***

- (27) Kreditinstitute und Versicherungsunternehmen spielen beim Übergang zu einem gänzlich nachhaltigen und inklusiven Wirtschafts- und Finanzsystem im Einklang mit dem Grünen Deal eine entscheidende Rolle. Sie können durch ihre Kreditvergabe-, Anlage- und Versicherungstätigkeiten erhebliche positive und negative Auswirkungen haben. Kreditinstitute und Versicherungsunternehmen, die nicht zur Einhaltung der Richtlinie 2013/34/EU verpflichtet sind, einschließlich Genossenschaften und Gegenseitigkeitsgesellschaften, sollten daher, sofern sie bestimmte Größenkriterien erfüllen, Anforderungen an die Nachhaltigkeitsberichterstattung unterliegen. Die Nutzer von Nachhaltigkeitsinformationen würden somit in die Lage versetzt, sowohl die gesellschaftlichen und ökologischen Auswirkungen solcher Kreditinstitute und Versicherungsunternehmen als auch die sich aus Nachhaltigkeitsaspekten ergebenden Risiken, denen solche Kreditinstitute und Versicherungsunternehmen ausgesetzt sein könnten, zu bewerten.

Die Richtlinie 2013/34/EU sieht drei mögliche Kriterien vor, um festzustellen, ob ein Unternehmen als „großes Unternehmen“ gilt, nämlich die Bilanzsumme, die Nettoumsatzerlöse und die durchschnittliche Zahl der während des Geschäftsjahres Beschäftigten. Das Kriterium der Nettoumsatzerlöse muss für Kreditinstitute und Versicherungsunternehmen angepasst werden, indem anstelle der allgemeinen Definition der Richtlinie 2013/34/EU auf die Definition der Nettoumsatzerlöse in den Richtlinien 86/635/EWG⁵⁴ und 91/674/EWG⁵⁵ des Rates Bezug genommen wird. Zur Gewährleistung der Kohärenz mit den Berichterstattungsanforderungen der Richtlinie 86/635/EWG können die Mitgliedstaaten in diesem Zusammenhang beschließen, die Anforderungen an die Nachhaltigkeitsberichterstattung nicht auf die in Artikel 2 Absatz 5 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates⁵⁶ genannten Kreditinstitute anzuwenden.

⁵⁴ Richtlinie 86/635/EWG des Rates vom 8. Dezember 1986 über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten (ABl. L 372 vom 31.12.1986, S. 1).

⁵⁵ Richtlinie 91/674/EWG des Rates vom 19. Dezember 1991 über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen (ABl. L 374 vom 31.12.1991, S. 7).

⁵⁶ 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).

- (28) Die Liste der Nachhaltigkeitsaspekte, über die Unternehmen Bericht erstatten müssen, sollte so weit wie möglich im Einklang mit der Bestimmung des Begriffs „Nachhaltigkeitsfaktoren“ im Sinne der Verordnung (EU) 2019/2088 stehen, **um eine Nichtübereinstimmung der von Datennutzern verlangten Informationen und den Informationen, über die Unternehmen Bericht zu erstatten haben, zu verhindern.** Diese Liste sollte zudem den Bedürfnissen und Erwartungen der Nutzer sowie der Unternehmen entsprechen, die zur Kategorisierung der drei wichtigsten Nachhaltigkeitsaspekte häufig die Begriffe „Umwelt“, „Soziales“ und „Unternehmensführung“ verwenden. Der Aspekt der Unternehmensführung wird von der Verordnung (EU) 2019/2088 festgelegten Definition des Begriffs „Nachhaltigkeitsfaktoren“ jedoch nicht ausdrücklich erfasst. Die Definition des Begriffs "Nachhaltigkeitsaspekte" in der Richtlinie 2013/34/EU in der durch die vorliegende Änderungsrichtlinie geänderten Fassung sollte daher **Umwelt-, Sozial- und Menschenrechts- sowie Governance-Faktoren abdecken und** die Bestimmung des Begriffs „Nachhaltigkeitsfaktoren“ im Sinne der Verordnung (EU) 2019/2088 **miteinschließen. Die Berichterstattungsanforderungen der Richtlinie 2013/34/EU sollten die nationalen Berichterstattungspflichten unberührt lassen.**

- (29) Nach Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU muss die Berichterstattung nicht nur Angaben umfassen, die für das Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses und der Lage des Unternehmens erforderlich sind, sondern auch Angaben, die für das Verständnis der Auswirkungen der Tätigkeiten des Unternehmens im Hinblick auf Umwelt-, Sozial-, und Arbeitnehmerbelange, die Achtung der Menschenrechte und die Bekämpfung von Korruption und Bestechung erforderlich sind. Nach diesen Artikeln sind Unternehmen daher verpflichtet, sowohl über die Auswirkungen ■ der Tätigkeiten des Unternehmens auf Mensch und Umwelt **als auch über die Auswirkungen der Nachhaltigkeitsaspekte auf das Unternehmen** Bericht zu erstatten. Dies wird als Konzept der doppelten Wesentlichkeit bezeichnet, bei dem die Risiken für das Unternehmen sowie dessen Auswirkungen jeweils einen Wesentlichkeitsaspekt darstellen. Die Eignungsprüfung der Berichterstattung von Unternehmen zeigt, dass diese beiden Aspekte häufig nicht korrekt verstanden oder angewandt werden. Daher muss klargestellt werden, dass Unternehmen jeden Wesentlichkeitsaspekt eigenständig betrachten und sowohl Informationen, die nach beiden Aspekten wesentlich sind, als auch Informationen offenlegen sollten, die nur nach einem Aspekt wesentlich sind.

- (30) Nach Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU müssen Unternehmen Informationen zu fünf Berichterstattungsbereichen offenlegen: Geschäftsmodell; Konzepte, einschließlich der angewandten Due-Diligence-Prozesse; Ergebnisse dieser Konzepte; Risiken und deren Handhabung sowie wichtigste Leistungsindikatoren, die für die betreffende Geschäftstätigkeit von Bedeutung sind. Artikel 19a Absatz 1 der Richtlinie 2013/34/EU enthält keine ausdrücklichen Verweise auf andere Berichterstattungsbereiche, die Nutzer von Informationen für relevant halten und von denen einige mit Offenlegungen in internationalen Rahmenwerken, einschließlich der Empfehlungen der Taskforce „Klimabezogene Finanzinformationen“, im Einklang stehen. Die Offenlegungspflichten sollten hinreichend spezifiziert werden, um sicherzustellen, dass Unternehmen Bericht über Informationen über ihre Widerstandsfähigkeit im Zusammenhang mit Nachhaltigkeitsrisiken erstatten. Zusätzlich zu den in Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU genannten Berichterstattungsbereichen sollten Unternehmen zur Offenlegung von Informationen zu folgenden Bereichen und Fragen verpflichtet werden: Geschäftsstrategie und Widerstandsfähigkeit des Geschäftsmodells und der Strategie im Zusammenhang mit Nachhaltigkeitsrisiken **■**. ***Sie sollten auch verpflichtet werden, etwaige Pläne offenzulegen, mit denen die Vereinbarkeit ihres Geschäftsmodells und ihrer Geschäftsstrategie mit dem Übergang zu einer nachhaltigen Wirtschaft und mit den Zielen der Begrenzung der Erderwärmung auf 1,5 °C ohne oder mit nur begrenzter Überschreitung im Einklang mit dem Übereinkommen von Paris und der Verwirklichung der Klimaneutralität bis 2050 gemäß der Verordnung (EU) 2021/1119 sichergestellt werden soll.***

Es ist besonders wichtig, dass klimabezogene Pläne auf den neuesten wissenschaftlichen Erkenntnissen beruhen, einschließlich der Berichte des Zwischenstaatlichen Ausschusses für Klimaänderungen (IPCC) und der Berichte des europäischen wissenschaftlichen Beirats für Klimaänderungen. Mit gemäß Artikel 8 der Verordnung (EU) 2020/852 offengelegten Informationen über die Höhe der Investitionsausgaben (CapEx) oder der Betriebsausgaben (OpEx) im Zusammenhang mit den taxonomiekonformen Tätigkeiten könnten gegebenenfalls Finanz- und Investitionspläne im Zusammenhang mit diesen Plänen unterstützt werden. Unternehmen sollten daher ebenfalls dazu verpflichtet werden, offenzulegen, ob und wie ihr Geschäftsmodell und ihre Geschäftsstrategie den Interessen der Interessenträger Rechnung tragen; etwaige Chancen des Unternehmens im Zusammenhang mit Nachhaltigkeitsaspekten; Umsetzung jener Aspekte der Geschäftsstrategie, die Auswirkungen auf Nachhaltigkeitsaspekte haben oder von Nachhaltigkeitsaspekten betroffen sind; etwaige Nachhaltigkeitsziele des Unternehmens und diesbezüglich erzielte Fortschritte; die Rolle des Verwaltungsrats und der Geschäftsleitung im Hinblick auf Nachhaltigkeitsaspekte; die wesentlichen – tatsächlichen und potenziellen – nachteiligen Auswirkungen im Zusammenhang mit den Tätigkeiten des Unternehmens; und wie das Unternehmen die Informationen, die Gegenstand der Berichterstattung sind, ermittelt. Sobald die Offenlegung von Elementen wie den Zielen und den diesbezüglich erzielten Fortschritten verpflichtend eingeführt wird, wird eine gesonderte Verpflichtung zur Offenlegung der Ergebnisse von Konzepten hinfällig.

- (31) Zur Gewährleistung der Kohärenz mit internationalen Instrumenten wie den „Leitprinzipien der Vereinten Nationen für Unternehmen und Menschenrechte: Umsetzung des Rahmens der Vereinten Nationen „Schutz, Achtung und Abhilfe““ (im Folgenden "Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte"), **den OECD-Leitsätzen für multinationale Unternehmen** und den OECD-Leitsätzen für die Erfüllung der Sorgfaltspflicht für verantwortungsvolles unternehmerisches Handeln sollten die Offenlegungspflichten im Hinblick auf Due-Diligence-Prozesse genauer spezifiziert werden, als dies in Artikel 19a Absatz 1 Buchstabe b und Artikel 29a Absatz 1 Buchstabe b der Richtlinie 2013/34/EU aktuell der Fall ist. Due-Diligence-Prozesse werden von Unternehmen mit dem Ziel durchgeführt, die wesentlichen – tatsächlichen und potenziellen – nachteiligen Auswirkungen im Zusammenhang mit ihren Tätigkeiten zu ermitteln, **zu überwachen**, zu verhüten, zu mildern, wiedergutzumachen **oder zu beseitigen**; dabei wird auch ermittelt, wie die Unternehmen diesen nachteiligen Auswirkungen begegnen. Die Auswirkungen im Zusammenhang mit den Tätigkeiten eines Unternehmens schließen die unmittelbar vom Unternehmen verursachten Auswirkungen, die Auswirkungen, zu denen das Unternehmen beiträgt, sowie jene Auswirkungen ein, die anderweitig mit der Wertschöpfungskette des Unternehmens zusammenhängen. Der Due-Diligence-Prozess deckt die gesamte Wertschöpfungskette des Unternehmens ab, einschließlich seiner eigenen Tätigkeiten, seiner Produkte und Dienstleistungen, seiner Geschäftsbeziehungen und seiner Lieferketten. Im Einklang mit den Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte sind tatsächliche oder potenzielle nachteilige Auswirkungen als wesentliche Auswirkungen anzusehen, wenn sie im Hinblick auf die nachstehenden Faktoren zu den größten Auswirkungen im Zusammenhang mit den Tätigkeiten des betreffenden Unternehmens zählen: Schwere der Auswirkungen auf Mensch oder Umwelt; Anzahl der Personen, die betroffen sind oder betroffen sein könnten, bzw. Ausmaß der Umweltschäden; und Aufwand, der erforderlich ist, um die Schäden zu beheben und – mit Blick auf die Umwelt bzw. die betroffenen Menschen – den ursprünglichen Zustand wiederherzustellen.

- (32) Nach der Richtlinie 2013/34/EU ist die Offenlegung von Angaben über immaterielle **Ressourcen**, bei denen es sich nicht um in der Bilanz angesetzte immaterielle Anlagewerte handelt, nicht erforderlich. Es ist weithin anerkannt, dass über Informationen zu immateriellen Anlagewerten und anderen immateriellen Faktoren, einschließlich intern geschaffener immaterieller Ressourcen, in zu geringem Maße Bericht erstattet wird, wodurch eine ordnungsgemäße Bewertung des Geschäftsverlaufs, des Geschäftsergebnisses und der Lage eines Unternehmens sowie die Überwachung von Investitionen erschwert wird. Um Anlegern ein besseres Verständnis der bei zahlreichen Unternehmen und in vielen Wirtschaftszweigen zunehmend beobachteten Diskrepanz zwischen Buchwert und Marktbewertung zu verschaffen, sollte **von allen großen Unternehmen und allen Unternehmen** – mit Ausnahme von Kleinstunternehmen –, **deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind**, eine angemessene Berichterstattung über immaterielle Ressourcen verlangt werden. **Nichtsdestotrotz sind bestimmte Informationen über immaterielle Ressourcen untrennbar mit Nachhaltigkeitsaspekten verbunden und sollten daher Teil der Nachhaltigkeitsberichterstattung sein. Beispielsweise sind Informationen über die Fähigkeiten der Beschäftigten, ihre Kompetenzen, ihre Erfahrung, ihre Loyalität gegenüber dem Unternehmen und ihre Motivation zur Verbesserung von Prozessen, Waren und Dienstleistungen Nachhaltigkeitsinformationen zu sozialen Aspekten, die auch als Informationen über immaterielle Ressourcen betrachtet werden könnten. Ebenso sind Informationen über die Qualität der Beziehungen zwischen dem Unternehmen und seinen Interessenträgern, einschließlich Kunden, Lieferanten und Gemeinschaften, die von den Tätigkeiten des Unternehmens betroffen sind, Nachhaltigkeitsinformationen, die für Sozial- oder Governance-Aspekte relevant sind und ebenfalls als Informationen über immaterielle Ressourcen betrachtet werden könnten. Diese Beispiele verdeutlichen, dass es in manchen Fällen nicht möglich ist, Informationen über immaterielle Ressourcen von Informationen über Nachhaltigkeitsaspekte zu unterscheiden.**

- (33) In Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU wird nicht spezifiziert, ob die Informationen, über die Bericht zu erstatten ist, zukunftsbezogen sein oder frühere Entwicklungen betreffen sollen. Derzeit ist ein Mangel an zukunftsbezogenen Offenlegungen zu verzeichnen, die von Nutzern von Nachhaltigkeitsinformationen besonders geschätzt werden. In Artikel 19a und Artikel 29a der Richtlinie 2013/34/EU sollte daher spezifiziert werden, dass die bereitgestellten Nachhaltigkeitsinformationen sowohl zukunfts- als auch vergangenheitsbezogene Informationen und sowohl qualitative als auch quantitative Informationen umfassen müssen. **Die Informationen sollten sich gegebenenfalls auf schlüssige wissenschaftliche Erkenntnisse stützen. Die Informationen sollten zudem harmonisiert und vergleichbar sein und gegebenenfalls auf einheitlichen Indikatoren beruhen, wobei eine unternehmensspezifische Berichterstattung möglich sein sollte, die die Geschäftslage des Unternehmens nicht gefährdet.** Die bereitgestellten Nachhaltigkeitsinformationen sollten zudem kurz-, mittel- und langfristige Zeiträume abdecken und Informationen zur gesamten Wertschöpfungskette des Unternehmens, einschließlich – sofern zweckmäßig – seiner eigenen Tätigkeiten, seiner Produkte und Dienstleistungen, seiner Geschäftsbeziehungen und seiner Lieferketten, enthalten. Informationen zur gesamten Wertschöpfungskette des Unternehmens würden sowohl Informationen zu dessen Wertschöpfungskette in der Union als auch Informationen in Bezug auf Drittländer umfassen, sofern die Wertschöpfungskette des Unternehmens über die Grenzen der Union hinausgeht. **Für die ersten drei Jahre der Anwendung der von den Mitgliedstaaten gemäß dieser Änderungsrichtlinie angenommenen Maßnahmen und für den Fall, dass nicht alle erforderlichen Informationen über seine Wertschöpfungskette verfügbar sind, sollte das Unternehmen erläutern, welche Anstrengungen unternommen wurden, um die Informationen über seine Wertschöpfungskette zu erhalten, begründen, warum diese Informationen nicht eingeholt werden konnten, und seine Pläne darlegen, um künftig die entsprechenden Informationen einzuholen.**

- (34) ***Diese Änderungsrichtlinie zielt nicht darauf ab, Unternehmen zur Offenlegung von geistigem Kapital, geistigem Eigentum, Know-how oder Innovationsergebnissen zu verpflichten, die als Geschäftsgeheimnisse im Sinne der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates⁵⁷ einzustufen sind. Die in dieser Änderungsrichtlinie vorgesehenen Berichterstattungsanforderungen sollten daher unbeschadet der Richtlinie (EU) 2016/943 gelten.***
- (35) Nach Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU müssen Unternehmen in ihre nichtfinanzielle Berichterstattung auch Hinweise auf im Jahresabschluss ausgewiesene Beträge und zusätzliche Erläuterungen dazu aufnehmen. Nach diesen Artikeln sind Unternehmen jedoch nicht dazu verpflichtet, im Lagebericht auf andere Informationen hinzuweisen oder solche Informationen um zusätzliche Erläuterungen zu ergänzen. Folglich mangelt es derzeit an Kohärenz zwischen den nichtfinanziellen Informationen, über die Bericht erstattet wurde, und den übrigen im Lagebericht offengelegten Informationen. Es ist erforderlich, diesbezüglich klare Anforderungen festzulegen.

⁵⁷ Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.6.2016, S. 1).

- (36) Nach Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU müssen Unternehmen, die in Bezug auf einen oder mehrere der in diesen Artikeln aufgeführten Belange kein Konzept verfolgen, eine klare und begründete Erklärung dafür vorlegen. Dass Offenlegungen zu den etwaigen bestehenden Konzepten von Unternehmen anders behandelt werden als Offenlegungen in den anderen in diesen Artikeln aufgeführten Berichterstattungsbereichen, hat bei den Bericht erstattenden Unternehmen für Verwirrung gesorgt und keineswegs zur Verbesserung der Qualität der Informationen, über die Bericht erstattet wurde, beigetragen. Es ist daher nicht erforderlich, diese unterschiedliche Behandlung von Konzepten in der genannten Richtlinie beizubehalten. In den Standards für die Nachhaltigkeitsberichterstattung sollte festgelegt werden, welche Informationen für jeden der in den Artikeln 19a und 29a der Richtlinie 2013/34/EU in der durch die vorliegenden Änderungsrichtlinie geänderten Fassung genannten Berichterstattungsbereiche offengelegt werden müssen.

- (37) Unternehmen, die in den Anwendungsbereich von Artikel 19a Absatz 1 und Artikel 29a Absatz 1 der Richtlinie 2013/34/EU fallen, können sich auf nationale, unionsbasierte oder internationale Rahmenwerke für die Berichterstattung stützen und haben, wenn sie hiervon Gebrauch machen, anzugeben, auf welche Rahmenwerke sie sich gestützt haben. Nach der Richtlinie 2013/34/EU sind Unternehmen jedoch nicht dazu verpflichtet, einen gemeinsamen Rahmen oder Standard für die Berichterstattung zu verwenden, und Unternehmen werden nicht daran gehindert, überhaupt keine Rahmenwerke oder Standards für die Berichterstattung zu verwenden. Gemäß Artikel 2 der Richtlinie 2014/95/EU veröffentlichte die Kommission am 5. Juli 2017 eine Mitteilung mit dem Titel „Leitlinien für die Berichterstattung über nichtfinanzielle Informationen (Methode zur Berichterstattung über nichtfinanzielle Informationen)“ (im Folgenden „Leitlinien für die Berichterstattung über nichtfinanzielle Informationen“), die unverbindliche Leitlinien für in den Anwendungsbereich jener Richtlinie fallende Unternehmen enthält. Am 17. Juni 2019 verabschiedete die Kommission ihre Leitlinien für die klimabezogene Berichterstattung mit zusätzlichen Leitlinien, die insbesondere die klimabezogene Berichterstattung zum Gegenstand hatten. In diesen Leitlinien für die klimabezogene Berichterstattung fanden die Empfehlungen der Taskforce „Klimabezogene Finanzinformationen“ ausdrückliche Berücksichtigung. Die verfügbaren Informationen deuten darauf hin, dass die Leitlinien für die Berichterstattung über nichtfinanzielle Informationen keine wesentlichen Auswirkungen auf die Qualität der Berichterstattung über nichtfinanzielle Informationen von in den Anwendungsbereich von Artikel 19a und Artikel 29a der Richtlinie 2013/34/EU fallenden Unternehmen hatten. Angesichts des unverbindlichen Charakters der Leitlinien steht es den Unternehmen frei zu entscheiden, ob sie diese anwenden oder nicht. Die Leitlinien allein können daher weder die Vergleichbarkeit der von verschiedenen Unternehmen offengelegten Informationen noch die Offenlegung sämtlicher von den Nutzern dieser Informationen für relevant erachteten Informationen gewährleisten. Deshalb sind verbindliche gemeinsame Standards für die Nachhaltigkeitsberichterstattung erforderlich, um sicherzustellen, dass die Informationen vergleichbar sind und alle relevanten Informationen offengelegt werden. Aufbauend auf dem Grundsatz der doppelten Wesentlichkeit sollten die Standards alle Informationen abdecken, die für

Nutzer dieser Informationen wesentlich sind. Gemeinsame Standards für die Nachhaltigkeitsberichterstattung sind überdies erforderlich, um die Bestätigung und Digitalisierung der Nachhaltigkeitsberichterstattung zu ermöglichen und deren Beaufsichtigung und Durchsetzung zu erleichtern. Die Entwicklung verbindlicher gemeinsamer Standards für die Nachhaltigkeitsberichterstattung ist notwendig, um zu erreichen, dass Nachhaltigkeitsinformationen einen vergleichbaren Status haben wie Finanzinformationen.

Mit der Verabschiedung von Standards für die Nachhaltigkeitsberichterstattung im Wege delegierter Rechtsakte würde eine unionsweit harmonisierte Nachhaltigkeitsberichterstattung gewährleistet werden. Somit würde ein Unternehmen die Anforderungen der Richtlinie 2013/34/EU an die Nachhaltigkeitsberichterstattung erfüllen, wenn es gemäß den Standards für die Nachhaltigkeitsberichterstattung Bericht erstattet. Bei der Festlegung solcher Standards ist es von wesentlicher Bedeutung, die wichtigsten weltweit angewandten Standards für die Nachhaltigkeitsberichterstattung im größtmöglichen Umfang gebührend zu berücksichtigen, ohne dabei die Ziele dieser Änderungsrichtlinie und der auf ihrer Grundlage erlassenen delegierten Rechtsakte zu mindern.

- (38) Kein bestehender Standard und kein bestehendes Rahmenwerk entspricht den Bedürfnissen der Union im Hinblick auf eine Nachhaltigkeitsberichterstattung. Die nach der Richtlinie 2013/34/EU erforderlichen Informationen müssen Informationen, die für beide Wesentlichkeitsaspekte relevant sind, umfassen, sämtliche Nachhaltigkeitsaspekte abdecken und gegebenenfalls mit anderen nach dem Unionsrecht bestehenden Verpflichtungen zur Offenlegung von Nachhaltigkeitsinformationen, einschließlich der in den Verordnungen (EU) 2019/2088 und (EU) 2020/852 vorgesehenen Verpflichtungen, in Einklang gebracht werden. Darüber hinaus sollten solche verbindlichen Standards für die Nachhaltigkeitsberichterstattung von Unternehmen in der Union den Zielsetzungen des Grünen Deals sowie dem Ziel der Union, bis 2050 Klimaneutralität zu erreichen, **und den Zwischenzielen gemäß der Verordnung (EU) 2021/1119** gerecht werden. Der Kommission muss daher die Befugnis übertragen werden, Standards der Union für die Nachhaltigkeitsberichterstattung anzunehmen, damit diese rasch verabschiedet werden können und sichergestellt ist, dass der Inhalt dieser Standards für die Nachhaltigkeitsberichterstattung den Bedürfnissen der Union entspricht.

- (39) Die Europäische Beratungsgruppe für Rechnungslegung (European Financial Reporting Advisory Group – EFRAG) ist eine nach belgischem Recht gegründete Vereinigung ohne Gewinnerzielungsabsicht, die dem öffentlichen Interesse dient, indem sie die Kommission bei der Übernahme internationaler Rechnungslegungsstandards berät. Die EFRAG genießt den Ruf eines europäischen Kompetenzzentrums für Unternehmensberichterstattung und ist gut aufgestellt, um die Koordinierung zwischen Standards der Union für die Nachhaltigkeitsberichterstattung und internationalen Initiativen zur Entwicklung weltweit einheitlicher Standards zu fördern. Im März 2021 veröffentlichte eine von der EFRAG eingesetzte Arbeitsgruppe verschiedener Interessenträger Empfehlungen für die mögliche Entwicklung von Standards für die Nachhaltigkeitsberichterstattung für die Union. Diese Empfehlungen enthalten Vorschläge zur Entwicklung kohärenter und umfassender Standards für die Nachhaltigkeitsberichterstattung, die gemäß dem Konzept der doppelten Wesentlichkeit sämtliche Nachhaltigkeitsaspekte abdecken. Die Empfehlungen enthalten zudem einen detaillierten Fahrplan für die Entwicklung solcher Standards sowie Vorschläge für eine auf gegenseitigen Nutzen ausgelegte Zusammenarbeit zwischen globalen Standardsetzungsinitiativen und Standardsetzungsinitiativen der Union. Im März 2021 veröffentlichte der Präsident des EFRAG-Aufsichtsrats für den Fall, dass die EFRAG zur Ausarbeitung technischer Empfehlungen für Standards für die Nachhaltigkeitsberichterstattung aufgefordert werden sollte, Empfehlungen für mögliche Änderungen an der Governance der EFRAG. Die Empfehlungen des Präsidenten des EFRAG-Aufsichtsrats betreffen unter anderem die Errichtung einer neuen Säule der Nachhaltigkeitsberichterstattung innerhalb der EFRAG, wobei an der bestehenden Säule der Rechnungslegung keine wesentlichen Änderungen vorgenommen werden sollen. **Im März 2022 ernannte die Generalversammlung der EFRAG die Mitglieder des neu geschaffenen Gremiums für Nachhaltigkeitsberichterstattung der EFRAG.** Bei der Annahme von Standards für die Nachhaltigkeitsberichterstattung sollte die Kommission technische Empfehlungen berücksichtigen, die von der EFRAG ausarbeitet werden.

Zur Gewährleistung hochwertiger Standards, die zum europäischen Gemeinwohl beitragen und den Bedürfnissen der Unternehmen und der Nutzer der bereitgestellten Informationen entsprechen, **sollte die EFRAG über ausreichende öffentliche Mittel verfügen, um ihre Unabhängigkeit zu gewährleisten. Ihre** technischen Empfehlungen sollten in einem einwandfreien Verfahren mit angemessener öffentlicher Aufsicht und Transparenz und auf der Grundlage des Fachwissens **einer ausgewogenen Vertretung** einschlägiger Interessenträger, **einschließlich Unternehmen, Investoren, Organisationen der Zivilgesellschaft und Gewerkschaften**, weiterentwickelt werden und mit Kosten-Nutzen-Analysen einhergehen. **Die Teilnahme an der Arbeit der EFRAG auf technischer Ebene sollte von Fachwissen im Bereich der Nachhaltigkeitsberichterstattung und nicht von finanziellen Beiträgen abhängig gemacht werden, unbeschadet der Beteiligung öffentlicher Stellen und nationaler Standardsetzungseinrichtungen an dieser Arbeit. Es sollte ein transparentes Verfahren zur Vermeidung von Interessenkonflikten gewährleistet werden.** Um sicherzustellen, dass die Standards der Union für die Nachhaltigkeitsberichterstattung den Standpunkten der Mitgliedstaaten Rechnung tragen, sollte die Kommission vor der Annahme dieser Standards die in der Verordnung (EU) 2020/852 genannte Sachverständigengruppe der Mitgliedstaaten für nachhaltiges Finanzwesen (im Folgenden "Sachverständigengruppe der Mitgliedstaaten für nachhaltiges Finanzwesen") **und den in der Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates⁵⁸ genannten Regelungsausschuss für Rechnungslegung** (im Folgenden "Regelungsausschuss für Rechnungslegung") zu den technischen Empfehlungen der EFRAG konsultieren.

⁵⁸

Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates vom 19. Juli 2002 betreffend die Anwendung internationaler Rechnungslegungsstandards (ABl. L 243 vom 11.9.2002, S. 1).

Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA), **die Europäische Bankenaufsichtsbehörde (EBA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA)** sind gemäß der Verordnung (EU) 2019/2088 an der Ausarbeitung technischer Regulierungsstandards beteiligt, und zwischen diesen technischen Regulierungsstandards und den Standards für die Nachhaltigkeitsberichterstattung muss Kohärenz bestehen. Gemäß der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates⁵⁹ trägt die ESMA auch zur Förderung der aufsichtlichen Konvergenz bei der Durchsetzung der Unternehmensberichterstattung von Emittenten bei, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind und die zur Mitteilung im Einklang mit diesen Standards für die Nachhaltigkeitsberichterstattung verpflichtet sein werden. Daher sollten die ESMA, **die EBA und die EIOPA** verpflichtet werden, eine Stellungnahme zur fachlichen Stellungnahme der EFRAG abzugeben. Diese **Stellungnahmen** sollten innerhalb von zwei Monaten nach Eingang des entsprechenden Antrags der Kommission vorgelegt werden. Darüber hinaus sollte die Kommission **■** die Europäische Umweltagentur, die Agentur der Europäischen Union für Grundrechte, die EZB, den Ausschuss der Europäischen Aufsichtsstellen für Abschlussprüfer (**im Folgenden „Ausschuss der Aufsichtsstellen“**) und die Plattform für ein nachhaltiges Finanzwesen konsultieren, um sicherzustellen, dass die Standards für die Nachhaltigkeitsberichterstattung mit den einschlägigen Strategien und Rechtsvorschriften der Union im Einklang stehen. Beschließt eine dieser Einrichtungen, eine Stellungnahme zu übermitteln, so sollte sie diese binnen zwei Monaten nach ihrer Konsultation durch die Kommission vorlegen.

⁵⁹ 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).

- (40) *Im Sinne der Förderung der demokratischen Überwachung, Kontrolle und Transparenz sollte die Kommission mindestens einmal jährlich das Europäische Parlament sowie die Sachverständigengruppe der Mitgliedstaaten für nachhaltiges Finanzwesen und den Regelungsausschuss für Rechnungslegung gemeinsam zum Arbeitsprogramm der EFrag im Hinblick auf die Entwicklung von Standards für die Nachhaltigkeitsberichterstattung konsultieren.*

- (41) Die Standards für die Nachhaltigkeitsberichterstattung sollten mit anderem Unionsrecht im Einklang stehen. Diese Standards sollten insbesondere an die in der Verordnung (EU) 2019/2088 festgelegten Offenlegungspflichten angepasst werden und die zugrunde liegenden Indikatoren und Methoden, die in den verschiedenen gemäß der Verordnung (EU) 2020/852 erlassenen delegierten Rechtsakten festgelegt sind, genauso berücksichtigen wie die gemäß der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates⁶⁰ für Referenzwert-Administratoren geltenden Offenlegungspflichten, die Mindeststandards für EU-Referenzwerte für den klimabedingten Wandel und für Paris-abgestimmte EU-Referenzwerte sowie alle Arbeiten der EBA zur Umsetzung der Säule-III-Offenlegungspflichten nach der Verordnung (EU) Nr. 575/2013. Die Standards sollten den Umweltvorschriften der Union, einschließlich der Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates⁶¹ und Richtlinie 2003/87/EG des Europäischen Parlaments und des Rates⁶², sowie auch der Empfehlung 2013/179/EU der Kommission⁶³ und deren Anhängen, einschließlich ihrer aktualisierten Fassungen, Rechnung tragen. Anderes Unionsrecht, einschließlich der Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates⁶⁴, sowie andere im Unionsrecht für Unternehmen geltenden Anforderungen im Hinblick auf die Pflichten von Vorständen und Due Diligence sollten ebenfalls berücksichtigt werden.

⁶⁰ 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).

⁶¹ Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates vom 25. November 2009 über die freiwillige Teilnahme von Organisationen an einem Gemeinschaftssystem für Umweltmanagement und Umweltbetriebsprüfung (EMAS) und zur Aufhebung der Verordnung (EG) Nr. 761/2001, sowie der Beschlüsse der Kommission 2001/681/EG und 2006/193/EG (ABl. L 342 vom 22.12.2009, S. 1).

⁶² Richtlinie 2003/87/EG des Europäischen Parlaments und des Rates vom 13. Oktober 2003 über ein System für den Handel mit Treibhausgasemissionszertifikaten in der Gemeinschaft und zur Änderung der Richtlinie 96/61/EG des Rates (ABl. L 275 vom 25.10.2003, S. 32).

⁶³ Empfehlung 2013/179/EU der Kommission vom 9. April 2013 für die Anwendung gemeinsamer Methoden zur Messung und Offenlegung der Umweltleistung von Produkten und Organisationen (ABl. L 124 vom 4.5.2013, S. 1).

⁶⁴ Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24. November 2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung) (ABl. L 334 vom 17.12.2010, S. 17).

- (42) Die Standards für die Nachhaltigkeitsberichterstattung sollten den Leitlinien für die Berichterstattung über nichtfinanzielle Informationen sowie den Leitlinien für die klimabezogenen Berichterstattung Rechnung tragen. Sie sollten auch anderen in der Richtlinie 2013/34/EU vorgesehenen Berichterstattungsanforderungen Rechnung tragen, die nicht unmittelbar Nachhaltigkeitsaspekte betreffen, damit den Nutzern der bereitgestellten Informationen – durch engere Verknüpfungen zwischen Nachhaltigkeitsinformationen und anderen gemäß der Richtlinie 2013/34/EU bereitzustellenden Informationen – ein besseres Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses, der Lage des Unternehmens sowie der Auswirkungen seiner Tätigkeit vermittelt wird.

- (43) Die Standards für die Nachhaltigkeitsberichterstattung sollten verhältnismäßig sein und den Unternehmen, die sie anwenden müssen, keinen unnötigen Verwaltungsaufwand auferlegen. Damit Unternehmen, die bereits Nachhaltigkeitsinformationen bereitstellen, so geringe Störungen wie möglich entstehen, sollten die Standards für die Nachhaltigkeitsberichterstattung gegebenenfalls bereits bestehende Standards und Rahmenwerke für nachhaltigkeitsbezogene Berichterstattung und Rechnungslegung berücksichtigen. Zu solchen bestehenden Standards und Rahmenwerken gehören die Global Reporting Initiative, das Sustainability Accounting Standards Board, der International Integrated Reporting Council, das International Accounting Standards Board, die Taskforce „Klimabezogene Finanzinformationen“, das Carbon Disclosure Standards Board und CDP, früher bekannt als Carbon Disclosure Project. Die Standards der Union sollten sämtlichen Standards für die Nachhaltigkeitsberichterstattung Rechnung tragen, die unter der Schirmherrschaft der International Financial Reporting Standards Foundation entwickelt wurden. Zur Vermeidung einer unnötigen regulatorischen Fragmentierung, die negative Folgen für weltweit tätige Unternehmen haben könnte, sollten die Standards der Union für die Nachhaltigkeitsberichterstattung auf globaler Ebene zur Konvergenz der Standards für die Nachhaltigkeitsberichterstattung beitragen, **indem die Arbeit des International Sustainability Standards Board (ISSB) unterstützt wird. Anhand Standards der Union für die Nachhaltigkeitsberichterstattung sollte das Risiko inkohärenter Berichterstattungsanforderungen für weltweit tätige Unternehmen verringert werden, indem der Inhalt der vom ISSB zu entwickelnden globalen Basisstandards einbezogen wird, soweit der Inhalt dieser Basisstandards mit dem Rechtsrahmen der Union und den Zielen des Grünen Deals im Einklang steht.**

- (44) Um einen angemessenen Umgang mit Umwelttrisiken zu gewährleisten, für angemessene Klimaschutzmöglichkeiten zu sorgen und die damit verbundenen Transaktionskosten zu senken, verpflichtete sich die Europäische Kommission im Grünen Deal, Unternehmen und andere Interessenträger bei der Entwicklung standardisierter Verfahren für die Naturkapitalbilanzierung in der EU und auf internationaler Ebene zu unterstützen. Im Rahmen des mit Mitteln aus dem durch die Verordnung (EU) 2021/783 des Europäischen Parlaments und des Rates⁶⁵ eingerichteten Programm für die Umwelt- und Klimapolitik (LIFE) geförderten Projekts „Transparent“ wird eine erste Methodik für die Naturkapitalbilanzierung entwickelt, mit der Vergleichbarkeit und Transparenz der bestehenden Methoden verbessert und Hemmnisse für die Unternehmen gegenüber einer Einführung und Nutzung von Systemen zur zukunftssicheren Gestaltung ihrer Geschäftstätigkeiten abgebaut werden sollen. Das Natural Capital Protocol ist im Zusammenhang mit der Naturkapitalbilanzierung ebenfalls eine wichtige Referenz. Zwar dienen die Methoden für die Naturkapitalbilanzierung in erster Linie der Untermauerung interner Unternehmensentscheidungen, doch sollten sie auch bei der Festlegung von Standards für die Nachhaltigkeitsberichterstattung gebührend berücksichtigt werden. Einige Methoden der Naturkapitalbilanzierung zielen darauf ab, die Auswirkungen von Unternehmenstätigkeiten auf die Umwelt anhand eines monetären Werts auszudrücken; dies könnte den Nutzern von Nachhaltigkeitsinformationen dabei helfen, solche Auswirkungen besser zu verstehen. Standards für die Nachhaltigkeitsberichterstattung sollten daher monetäre Indikatoren für Nachhaltigkeitsauswirkungen einschließen können, sofern dies für notwendig erachtet wird.

⁶⁵ Verordnung (EU) 2021/783 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Einrichtung des Programms für die Umwelt- und Klimapolitik (LIFE) und zur Aufhebung der Verordnung (EU) Nr. 1293/2013 (ABl. L 172 vom 17.5.2021, S. 53).

- (45) Standards für die Nachhaltigkeitsberichterstattung sollten auch international anerkannten Grundsätzen und Rahmenbestimmungen für verantwortungsvolles unternehmerisches Handeln, soziale Verantwortung von Unternehmen und nachhaltige Entwicklung Rechnung tragen, wie etwa den Zielen für nachhaltige Entwicklung, den Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte, den OECD-Leitsätzen für multinationale Unternehmen, den OECD-Leitsätzen zur Erfüllung der Sorgfaltspflicht zur Förderung verantwortungsvollen unternehmerischen Handelns und damit verbundenen sektoralen Leitlinien, dem Globalen Pakt, der Trilateralen Grundsatzerklärung der Internationalen Arbeitsorganisation zu multinationalen Unternehmen und zur Sozialpolitik, der ISO-Norm 26000 „Leitfaden zur gesellschaftlichen Verantwortung“ und den Grundsätzen der Vereinten Nationen für verantwortungsvolle Investitionen.

- (46) Es sollte sichergestellt werden, dass die Informationen, über die Unternehmen gemäß den Standards für die Nachhaltigkeitsberichterstattung Bericht erstatten, den Bedürfnissen der Nutzer entsprechen **und den Bericht erstattenden Unternehmen sowie den als Teil der Wertschöpfungskette dieser Unternehmen indirekt Betroffenen keine unverhältnismäßig hohe Last in Bezug auf Aufwand und Kosten auferlegen**. In den Standards für die Nachhaltigkeitsberichterstattung sollte daher festgelegt werden, welche Informationen die Unternehmen zu den wichtigen Umweltfaktoren offenlegen müssen, einschließlich Angaben zu ihren Auswirkungen auf Klima, Luft, Boden, Wasser und biologische Vielfalt und damit verbundenen Abhängigkeiten. Die Verordnung (EU) 2020/852 enthält eine Klassifizierung der Umweltziele der Union. Aus Gründen der Kohärenz empfiehlt es sich, bei der Ermittlung der Umweltfaktoren, auf die Standards für die Nachhaltigkeitsberichterstattung Bezug nehmen sollten, eine ähnliche Klassifizierung zu verwenden. In den Standards für die Nachhaltigkeitsberichterstattung sollten alle geografischen und sonstigen kontextbezogenen Informationen berücksichtigt und präzisiert werden, die Unternehmen offenlegen sollten, um ein besseres Verständnis der wichtigsten nachhaltigkeitsrelevanten Auswirkungen ihrer Tätigkeiten und der größten Risiken, denen sie im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt sind, zu vermitteln. **Bei der Präzisierung der Informationen über die Umweltfaktoren, die Unternehmen offenlegen müssen, sollte für Kohärenz mit den Begriffsbestimmungen in Artikel 2 der Verordnung (EU) 2020/852 sowie den Berichterstattungsanforderungen gemäß Artikel 8 der genannten Verordnung und den gemäß der genannten Verordnung erlassenen delegierten Rechtsakten gesorgt werden.**

- (47) Klimabezogene Informationen sind bei den Nutzern insbesondere im Hinblick auf physische Risiken und Übergangsrisiken **und** die Widerstandsfähigkeit der Unternehmen in verschiedenen Klimaszenarien **sowie ihre entsprechenden Pläne zur Anpassung sowie auf das Ziel der Union, bis 2050 Klimaneutralität zu erreichen, sowie ihre entsprechenden Pläne zur Anpassung** gefragt. Ferner interessieren diese Nutzer sich für Angaben zu Menge und Umfang der dem Unternehmen zugeordneten Emissionen und des erreichten Abbaus von Treibhausgasen, einschließlich des Umfangs, in dem das Unternehmen Kompensationen nutzt, und der Quelle, aus der diese stammen. Um eine klimaneutrale Wirtschaft zu erreichen, müssen Standards für die Anrechnung und Kompensation von Treibhausgasemissionen aufeinander abgestimmt werden. Doppelzählungen und Überbewertungen bergen Risiken für das Erreichen klimabezogener Ziele, weshalb die Nutzer zuverlässige Informationen über Kompensationen benötigen, bei denen Bedenken hinsichtlich möglicher Doppelzählungen und Überbewertungen Rechnung getragen wird. **Bei diesen Nutzern sind auch die Bemühungen der Unternehmen um deutlich reduzierte absolute Treibhausgasemissionen im Rahmen ihrer Strategien für den Klimaschutz und die Anpassung an den Klimawandel, einschließlich Scope-1- und Scope-2-Emissionen und gegebenenfalls Scope-3-Emissionen gefragt. In Bezug auf Scope-3-Emissionen besteht eine Priorität in Bezug auf die Nutzer darin, dass diese Informationen darüber erhalten, welche Kategorien von Scope 3 im Falle des Unternehmens von Bedeutung sind, sowie über die Emissionen in jeder dieser Kategorien von Scope 3.** Daher sollte in den Standards für die Nachhaltigkeitsberichterstattung festgelegt werden, über welche Informationen die Unternehmen in Bezug auf solche Aspekte Bericht erstatten sollten.

- (48) Die Ziele einer klimaneutralen Kreislaufwirtschaft **ohne Verschmutzung aus diffusen Quellen** können nur erreicht werden, wenn es gelingt, sämtliche Wirtschaftszweige uneingeschränkt zu mobilisieren. Die Verringerung des Energieverbrauchs und die Steigerung der Energieeffizienz sind in diesem Zusammenhang von entscheidender Bedeutung, da Energie über Lieferketten hinweg genutzt wird. Daher sollten in den Standards für die Nachhaltigkeitsberichterstattung Energieaspekte, insbesondere im Zusammenhang mit **umwelt- und klimarelevanten** Aspekten, gebührend berücksichtigt werden.
- (49) In den Standards für die Nachhaltigkeitsberichterstattung sollte festgelegt werden, welche Informationen Unternehmen zu sozialen Faktoren, einschließlich **Arbeitsbedingungen, Beteiligung der Sozialpartner, Tarifverhandlungen, Gleichstellung, Nichtdiskriminierung, Vielfalt und Inklusion sowie** Menschenrechten, offenlegen sollten. Diese Informationen sollten die Auswirkungen **des Unternehmens** auf Menschen, einschließlich **der Arbeitnehmer, und die** Auswirkungen auf die menschliche Gesundheit abdecken. Die Informationen, die Unternehmen über Menschenrechte offenlegen, sollten gegebenenfalls auch Angaben über Zwangsarbeit **und Kinderarbeit** in ihren Wertschöpfungsketten umfassen. **Anforderungen an die Nachhaltigkeitsberichterstattung in Bezug auf Zwangsarbeit sollten die Behörden nicht von ihrer Verantwortung befreien, mit handelspolitischen und diplomatischen Mitteln gegen die Einfuhr von Waren vorzugehen, die infolge von Menschenrechtsverletzungen, einschließlich Zwangsarbeit, hergestellt wurden. Unternehmen sollte es ferner möglich sein, über mögliche Risiken und Tendenzen in Bezug auf Beschäftigung und Einkommen Bericht zu erstatten.** In Standards für die Nachhaltigkeitsberichterstattung, die sich mit sozialen Faktoren befassen, sollte präzisiert werden, welche Informationen Unternehmen im Hinblick auf für sie relevante Grundsätze der europäischen Säule sozialer Rechte offenlegen sollten, einschließlich Angaben zur Chancengleichheit für alle und zu den Arbeitsbedingungen.

In dem von der Kommission am 4. März 2021 angenommenen Aktionsplan zur europäischen Säule sozialer Rechte werden strengere Anforderungen bezüglich der Berichterstattung der Unternehmen über soziale Fragen gefordert. In den Standards für die Nachhaltigkeitsberichterstattung sollte auch festgelegt werden, welche Informationen Unternehmen in Bezug auf die Menschenrechte, Grundfreiheiten, demokratischen Grundsätze und Normen offenlegen sollten, die in der Internationalen Charta der Menschenrechte und anderen grundlegenden Menschenrechtsübereinkommen der Vereinten Nationen, ***einschließlich des Übereinkommens der Vereinten Nationen über die Rechte von Menschen mit Behinderungen, der Erklärung der Vereinten Nationen über die Rechte der indigenen Völker, des Übereinkommens der Vereinten Nationen über die Rechte des Kindes, der Erklärung der Internationalen Arbeitsorganisation über grundlegende Prinzipien und Rechte bei der Arbeit, den grundlegenden Übereinkommen der Internationalen Arbeitsorganisation, der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, der Europäischen Sozialcharta und der Charta der Grundrechte der Europäischen Union festgelegt sind. Die Berichterstattung über Sozialfaktoren sowie über Umwelt- und Governance-Faktoren sollte in einem angemessenen Verhältnis zum Anwendungsbereich und zu den Zielen dieser Änderungsrichtlinie stehen. In Standards für die Nachhaltigkeitsberichterstattung, die die Gleichstellung der Geschlechter und gleichen Lohn bei gleichwertiger Arbeit betreffen, sollte unter anderem festgelegt werden, über welche Informationen bezüglich des geschlechtsspezifischen Lohngefälles Bericht erstattet werden sollte, wobei anderem einschlägigen Unionsrecht Rechnung getragen werden sollte. In Standards für die Nachhaltigkeitsberichterstattung, die die Beschäftigung und Inklusion von Menschen mit Behinderungen betreffen, sollte unter anderem festgelegt werden, über welche Informationen bezüglich der vom Unternehmen ergriffenen Barrierefreiheitsmaßnahmen Bericht erstattet werden sollte.***

In Standards für die Nachhaltigkeitsberichterstattung, die die Bereiche Ausbildung und Kompetenzentwicklung betreffen, sollte unter anderem festgelegt werden, über welche Informationen bezüglich des Anteils und der Aufschlüsselung der an der Ausbildung teilnehmenden Arbeitnehmer Bericht erstattet werden sollte. In Standards für die Nachhaltigkeitsberichterstattung, die Tarifverhandlungen betreffen, sollte unter anderem festgelegt werden, welche Informationen über die Existenz von Betriebsräten sowie über das Bestehen von Tarifverträgen und den Anteil der Arbeitnehmer, für die solche Vereinbarungen gelten, offengelegt werden sollten. In Standards für die Nachhaltigkeitsberichterstattung, die die Arbeitnehmerbeteiligung betreffen, sollte unter anderem festgelegt werden, welche Informationen über die Beteiligung von Arbeitnehmern an Verwaltungs- und Aufsichtsorganen offengelegt werden sollten. In Standards für die Nachhaltigkeitsberichterstattung, die das Thema Vielfalt betreffen, sollte unter anderem festgelegt werden, über welche Informationen über die Geschlechtervielfalt auf der obersten Führungsebene und die Zahl der Mitglieder des unterrepräsentierten Geschlechts in ihren Leitungsorganen Bericht erstattet werden sollte.

- (50) Die Nutzer benötigen Informationen über Governance-Faktoren. **Die für die Nutzer relevantesten Governance-Faktoren werden in verbindlichen Rahmen für die Berichterstattung, etwa jenen der Global Reporting Initiative und der Taskforce „Klimabezogene Finanzinformationen“, sowie in verbindlichen globalen Rahmen wie den Global Governance Principles des International Corporate Governance Network und den G20/OECD-Grundsätzen der Corporate Governance aufgeführt. In Standards für die Nachhaltigkeitsberichterstattung sollte festgelegt werden, welche Informationen Unternehmen zu Governance-Faktoren offenlegen sollten. Diese Informationen sollten sich auf die Rolle der Verwaltungs-, Leitungs- und Aufsichtsorgane eines Unternehmens in Bezug auf Nachhaltigkeitsaspekte, das zur Erfüllung dieser Rolle notwendige Fachwissen und die entsprechend notwendigen Fähigkeiten oder den Zugang dieser Organe zu solchen Fachkenntnissen und Fähigkeiten sowie darauf erstrecken, ob das Unternehmen eine mit den Nachhaltigkeitsaspekten verknüpfte Strategie in Bezug auf Anreize für Mitglieder, die in diesen Organen tätig sind, verfolgt, sowie auf Informationen über die internen Kontroll- und Risikomanagementsysteme eines Unternehmens** ■ in Bezug auf den Nachhaltigkeitsberichterstattungsprozess.

Die Nutzer benötigen ferner Informationen über Unternehmenskultur und Unternehmensethik, **die anerkannte Elemente der verbindlichen Corporate-Governance-Rahmen wie der Global Governance Principles des International Corporate Governance Network sind**, einschließlich **Informationen über die** Bekämpfung von Korruption und Bestechung, sowie über Tätigkeiten und Verpflichtungen des Unternehmens im Hinblick auf die Ausübung seines politischen Einflusses, einschließlich **seiner** Lobbytätigkeiten. Informationen über die Leitung des Unternehmens und die Qualität der Beziehungen zu **Kunden, Lieferanten und Gemeinschaften, die von den Tätigkeiten des Unternehmens betroffen sind, vermitteln den Nutzern ein besseres Verständnis der Risiken eines Unternehmens und der Auswirkungen im Zusammenhang mit Nachhaltigkeitsaspekten.**

Informationen über die Beziehungen zu Lieferanten umfassen Zahlungspraktiken in Bezug auf Zahlungstermine oder Zahlungsfristen, den Zinssatz für verspätete Zahlungen oder die Entschädigung für in der Richtlinie 2011/7/EU des Europäischen Parlaments und des Rates⁶⁶ genannte Beitreibungskosten. ■ Jedes Jahr müssen Tausende von Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), administrative und finanzielle Belastungen tragen, weil sie verspätet oder gar nicht bezahlt werden. Letztendlich führt Zahlungsverzug zu Insolvenz und Konkurs mit destruktiven Auswirkungen auf ganze Wertschöpfungsketten. Wenn Unternehmen mehr Informationen über Zahlungspraktiken zur Verfügung gestellt werden, dürften sie besser in der Lage sein, schnelle und zuverlässige Zahler zu ermitteln, unlautere Zahlungspraktiken aufzudecken, sich über Unternehmen, mit denen sie Handel treiben, zu informieren und fairere Zahlungsbedingungen auszuhandeln.

⁶⁶ Richtlinie 2011/7/EU des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Bekämpfung von Zahlungsverzug im Geschäftsverkehr (ABl. L 48 vom 23.2.2011, S. 1).

- (51) Die Standards für die Nachhaltigkeitsberichterstattung sollten darauf ausgerichtet sein, einen stärker integrierten Gesamtüberblick über die Informationen, die die Unternehmen in ihrem Lagebericht veröffentlichen, zu ermöglichen und so den Nutzern dieser Informationen ein besseres Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses, der Lage des Unternehmens sowie der Auswirkungen seiner Tätigkeit zu vermitteln. In den Standards für die Nachhaltigkeitsberichterstattung sollte erforderlichenfalls zwischen Informationen, die Unternehmen bei der Berichterstattung auf Einzelebene und solchen, die sie bei der Berichterstattung auf Gruppenebene offenlegen sollten, unterschieden werden. Die Standards für die Nachhaltigkeitsberichterstattung sollten auch Leitlinien zu dem Verfahren enthalten, anhand dessen Unternehmen die in den Lagebericht aufzunehmenden Nachhaltigkeitsinformationen ermitteln, ***da ein Unternehmen nur zur Offenlegung der Informationen verpflichtet werden sollte, die für das Verständnis seiner Auswirkungen auf Nachhaltigkeitsaspekte von Belang sind oder die für das Verständnis der Auswirkungen von Nachhaltigkeitsaspekten auf Geschäftsverlauf, Geschäftsergebnis und Lage des Unternehmens von Belang sind.***

- (52) *Die Mitgliedstaaten sollten sicherstellen, dass die Nachhaltigkeitsberichterstattung im Einklang mit dem Recht der Arbeitnehmer auf Unterrichtung und Anhörung erfolgt. Die Unternehmensleitung sollte daher die Arbeitnehmervertreter auf geeigneter Ebene informieren und mit ihnen die einschlägigen Informationen und die Mittel zur Einholung und Überprüfung von Nachhaltigkeitsinformationen erörtern. Dies setzt für die Zwecke dieser Änderungsrichtlinie die Aufnahme eines Dialogs und eines Meinungsaustauschs zwischen den Arbeitnehmervertretern und der zentralen Leitung oder jeder anderen besser geeigneten Leitungsebene voraus, und zwar zu einem Zeitpunkt, in einer Weise und mit einem Inhalt, der es den Arbeitnehmervertretern ermöglicht, Stellung zu nehmen. Ihre Stellungnahme sollte, wo angezeigt, den zuständigen Verwaltungs-, Leitungs- oder Aufsichtsorganen mitgeteilt werden.*

- (53) Unternehmen derselben Branche sind häufig ähnlichen nachhaltigkeitsbezogenen Risiken ausgesetzt und haben häufig ähnliche Auswirkungen auf Gesellschaft und Umwelt. Vergleiche zwischen Unternehmen derselben Branche sind für Anleger und andere Nutzer von Nachhaltigkeitsinformationen besonders wertvoll. Daher sollte in den Standards für die Nachhaltigkeitsberichterstattung festgelegt werden, welche Informationen die Unternehmen sämtlicher Branchen und welche Informationen die Unternehmen je nach Tätigkeitsbereich offenlegen sollten. **Sektorspezifische Standards** für die Nachhaltigkeitsberichterstattung **sind besonders wichtig für Wirtschaftszweige, die mit hohen Nachhaltigkeitsrisiken für oder mit Auswirkungen auf Umwelt, Menschenrechte und Governance verbunden sind, einschließlich der in Anhang I Abschnitte A bis H und Abschnitt L der Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates⁶⁷ aufgeführten Wirtschaftszweige und der einschlägigen Tätigkeiten in diesen Wirtschaftszweigen. Bei der Annahme sektorspezifischer Standards** für die Nachhaltigkeitsberichterstattung **sollte die Kommission sicherstellen, dass die in diesen Standards** für die Nachhaltigkeitsberichterstattung **vorgeschriebenen Informationen in einem angemessenen Verhältnis zum Ausmaß der Risiken und Auswirkungen im Zusammenhang mit Nachhaltigkeitsaspekten stehen, die für jeden Wirtschaftszweig spezifisch sind, wobei berücksichtigt werden sollte, dass die Risiken und Auswirkungen einiger Wirtschaftszweige im Vergleich höher sind. Die Kommission sollte auch berücksichtigen, dass nicht alle Tätigkeiten in diesen Wirtschaftszweigen notwendigerweise mit hohen Nachhaltigkeitsrisiken oder -auswirkungen verbunden sind. Für Unternehmen, die in Wirtschaftszweigen tätig sind, die in besonderem Maße auf natürliche Ressourcen angewiesen sind, würden sektorspezifische Standards** für die Nachhaltigkeitsberichterstattung **die Offenlegung der naturbezogenen Auswirkungen auf die biologische Vielfalt und die Ökosysteme sowie der entsprechenden Risiken erfordern.**

⁶⁷ Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik (ABl. L 393 vom 30.12.2006, S. 1).

In den Standards für die Nachhaltigkeitsberichterstattung sollte auch berücksichtigt werden, dass es für Unternehmen nicht immer problemlos möglich ist, Informationen bei Akteuren entlang ihrer gesamten Wertschöpfungskette, insbesondere Lieferanten, bei denen es sich um kleine und mittlere Unternehmen handelt, und Lieferanten aus Schwellenländern und aufstrebenden Märkten, einzuholen. ***In den Standards für die Nachhaltigkeitsberichterstattung sollten Offenlegungen in Bezug auf Wertschöpfungsketten festgelegt werden, die dem Umfang und der Komplexität der Tätigkeiten der Unternehmen sowie den Kapazitäten und Merkmalen von Unternehmen in Wertschöpfungsketten, insbesondere den Kapazitäten und Merkmalen von Unternehmen, die nicht den Anforderungen an die Nachhaltigkeitsberichterstattung nach dieser Änderungsrichtlinie unterliegen, angemessen sind und entsprechen. In den Standards für die Nachhaltigkeitsberichterstattung sollten keine Offenlegungen festgelegt werden, die Unternehmen verpflichten würden, Informationen von kleinen und mittleren Unternehmen in ihrer Wertschöpfungskette einzuholen, die über die Informationen hinausgehen, die gemäß den Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen offenzulegen sind. Dies sollte unbeschadet der Anforderungen der Union an Unternehmen, einen Due-Diligence-Prozess durchzuführen, gelten.***

- (54) Um den Informationsbedarf der Nutzer rechtzeitig zu decken und angesichts des besonderen dringlichen Informationsbedarfs von Finanzmarktteilnehmern, die den Anforderungen der gemäß Artikel 4 Absätze 6 und 7 der Verordnung (EU) 2019/2088 erlassenen delegierten Rechtsakte unterliegen, sollte die Kommission bis zum **30. Juni 2023** mittels delegierter Rechtsakte ein erstes Paket von Standards für die Nachhaltigkeitsberichterstattung festlegen. In diesem Paket von Standards für die Nachhaltigkeitsberichterstattung sollte festgelegt werden, welche Informationen Unternehmen in Bezug auf alle Berichterstattungsbereiche und Nachhaltigkeitsaspekte offenlegen sollten; gleichzeitig sollte von den Finanzmarktteilnehmern verlangt werden, den Offenlegungspflichten der Verordnung (EU) 2019/2088 nachzukommen. Die Kommission sollte spätestens bis zum **30. Juni 2024** mittels delegierter Rechtsakte ein zweites Paket von Standards für die Nachhaltigkeitsberichterstattung annehmen, in denen festgelegt wird, welche ergänzenden Informationen Unternehmen in Bezug auf Nachhaltigkeitsaspekte und Berichterstattungsbereiche erforderlichenfalls offenlegen sollten und welche spezifischen Informationen sie für den Sektor, in dem sie tätig sind, offenlegen sollten. Die Kommission sollte die Standards für die Nachhaltigkeitsberichterstattung, ***einschließlich der Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen***, alle drei Jahre überprüfen, um relevanten Entwicklungen, einschließlich der Entwicklung internationaler Standards, Rechnung zu tragen.

- (55) Die Richtlinie 2013/34/EU schreibt nicht vor, dass der Lagebericht in digitalem Format vorgelegt werden muss, was es schwieriger macht, die Informationen, über die Bericht erstattet wurde, zu finden und zu nutzen. Die Nutzer von Nachhaltigkeitsinformationen erwarten zunehmend, dass diese Informationen in digitalem Format auffindbar, **vergleichbar** und maschinenlesbar sind. **Die Mitgliedstaaten sollten vorschreiben können, dass Unternehmen, die den Anforderungen der Richtlinie 2013/34/EU an die Nachhaltigkeitsberichterstattung unterliegen, ihre Lageberichte der Öffentlichkeit kostenlos auf ihren Websites zugänglich machen.** Die Digitalisierung eröffnet Möglichkeiten für eine effizientere Nutzung von Informationen und birgt sowohl für Nutzer als auch für Unternehmen das Potenzial erheblicher Kosteneinsparungen. **Die Digitalisierung ermöglicht auch die Zentralisierung von Daten auf Ebene der Union und der Mitgliedstaaten in einem offenen, barrierefreien Format, das das Lesen erleichtert und den Vergleich von Daten ermöglicht.** Unternehmen sollten daher dazu verpflichtet werden, den Lagebericht im **elektronischen Berichtsformat** gemäß Artikel 3 der Delegierten Verordnung (EU) 2019/815 der Kommission⁶⁸ zu erstellen und Nachhaltigkeitsberichterstattung, einschließlich der nach Artikel 8 der Verordnung (EU) 2020/852 erforderlichen Angaben, im Einklang mit dem **elektronischen Berichtsformat** gemäß der genannten Delegierten Verordnung (EU) 2019/815 auszuzeichnen, **sobald dies entsprechend festgelegt wurde.** Um Informationen, über die Bericht erstattet wurde, gemäß den Standards der Union für die Nachhaltigkeitsberichterstattung kennzeichnen zu können, wird eine entsprechende digitale Taxonomie benötigt. Diese Anforderungen sollten in die von der Kommission in ihrer Mitteilung vom 19. Februar 2020 mit dem Titel „Eine europäische Datenstrategie“ und in ihrer Mitteilung vom 24. September 2020 mit dem Titel „Strategie für ein digitales Finanzwesen in der EU“ angekündigten Arbeiten zur Digitalisierung einfließen. Diese Anforderungen würden zudem die Schaffung des in der Mitteilung der Kommission vom 24. September 2020 mit dem Titel „Eine Kapitalmarktunion für die Menschen und Unternehmen – neuer

⁶⁸ Delegierte Verordnung (EU) 2019/815 der Kommission vom 17. Dezember 2018 zur Ergänzung der Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates im Hinblick auf technische Regulierungsstandards für die Spezifikation eines einheitlichen elektronischen Berichtsformats (ABl. L 143 vom 29.5.2019, S. 1).

Aktionsplan“ vorgesehenen einheitlichen europäischen Zugangspunkts (European Single Access Point – ESAP) für öffentliche Unternehmensinformationen ergänzen, in der der Bedarf an der Bereitstellung vergleichbarer Informationen in einem digitalen Format ebenfalls thematisiert wird.

- (56) Um die Einbeziehung der Nachhaltigkeitsinformationen, über die Bericht erstattet wurde, in den ESAP zu ermöglichen, sollten die Mitgliedstaaten sicherstellen, dass Unternehmen, ***deren Wertpapiere nicht zum Handel auf einem geregelten Markt in der Union zugelassen sind, ihren Lagebericht, einschließlich der Nachhaltigkeitsberichterstattung, in dem in Artikel 3 der Delegierten Verordnung (EU) 2019/815 vorgeschriebenen elektronischen Berichtsformat veröffentlichen.***

- (57) Gemäß Artikel 19a Absatz 4 der Richtlinie 2013/34/EU können Mitgliedstaaten Unternehmen von der gemäß Artikel 19a Absatz 1 der genannten Richtlinie festgelegten Pflicht zur Abgabe der nichtfinanziellen Erklärung befreien. Die Mitgliedstaaten können dies tun, wenn das betreffende Unternehmen einen gesonderten Bericht erstellt, der zusammen mit dem Lagebericht gemäß Artikel 30 der genannten Richtlinie veröffentlicht wird, oder wenn dieser Bericht innerhalb eines angemessenen Zeitraums von höchstens sechs Monaten nach dem Bilanzstichtag auf der Website des Unternehmens öffentlich zugänglich gemacht wird und im Lagebericht auf ihn Bezug genommen wird. Dieselbe Möglichkeit besteht gemäß der Richtlinie 2013/34/EU bei der konsolidierten nichtfinanziellen Erklärung. 20 Mitgliedstaaten haben von dieser Möglichkeit Gebrauch gemacht. Die Möglichkeit, einen gesonderten Bericht zu veröffentlichen, verringert jedoch die Verfügbarkeit von Informationen, die Finanz- und Nachhaltigkeitsaspekte miteinander verbinden. Sie behindert auch die Auffindbarkeit und Zugänglichkeit von Informationen für Nutzer; dies gilt insbesondere für Anleger, die an Finanz- und Nachhaltigkeitsinformationen gleichermaßen interessiert sind. Wenn Finanz- und Nachhaltigkeitsinformationen zudem zu unterschiedlichen Zeitpunkten veröffentlicht werden können, wird dieses Problem weiter verschärft. Außerdem kann die Veröffentlichung in einem gesonderten Bericht intern und extern den Eindruck erwecken, dass Nachhaltigkeitsinformationen zu einer Kategorie von weniger relevanten Informationen gehören, was sich negativ auf die wahrgenommene Zuverlässigkeit der Informationen auswirken kann. Unternehmen sollten über Nachhaltigkeitsinformationen daher **in einem dafür vorgesehenen Abschnitts klar erkennbar** Bericht erstatten, und die Mitgliedstaaten sollten Unternehmen nicht länger von der Verpflichtung befreien können, Informationen über Nachhaltigkeitsaspekte in den Lagebericht aufzunehmen. Eine solche Verpflichtung würde auch dazu beitragen, klarzustellen, welche Rolle den nationalen zuständigen Behörden bei der Aufsicht der Nachhaltigkeitsberichterstattung als Teil des gemäß der Richtlinie 2004/109/EG erstellten Lageberichts zukommt. Darüber hinaus sollten Unternehmen, die Bericht über Nachhaltigkeitsinformationen erstatten müssen, in keinem Fall von der Pflicht zur Veröffentlichung des Lageberichts befreit werden, da sichergestellt werden muss, dass Nachhaltigkeitsinformationen öffentlich zugänglich sind.

- (58) Gemäß Artikel 20 der Richtlinie 2013/34/EU müssen Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, in ihren Lagebericht eine Erklärung zur Unternehmensführung aufnehmen, die unter anderem eine Beschreibung des im Zusammenhang mit den Verwaltungs-, Leitungs- und Aufsichtsorganen des Unternehmens verfolgten Diversitätskonzepts enthalten muss. Artikel 20 der Richtlinie 2013/34/EU räumt den Unternehmen die Möglichkeit ein, selbst zu entscheiden, über welche Diversitätsaspekte sie Bericht erstatten. Die Unternehmen werden nicht ausdrücklich dazu verpflichtet, Informationen über bestimmte Diversitätsaspekte aufzunehmen. Um Fortschritte in Richtung einer ausgewogeneren Beteiligung von Frauen und Männern am wirtschaftlichen Entscheidungsprozess zu erzielen, muss sichergestellt werden, dass Unternehmen, deren Wertpapiere **zum Handel auf einem geregelten Markt in der Union zugelassen** sind, stets über ihr Konzept zur Förderung der Geschlechtervielfalt und dessen Umsetzung Bericht zu erstatten. Um jedoch unnötigen Verwaltungsaufwand zu vermeiden, sollten diese Unternehmen die Möglichkeit haben, über einige der gemäß Artikel 20 der Richtlinie 2013/34/EU erforderlichen Informationen zusammen mit anderen Nachhaltigkeitsinformationen Bericht zu erstatten. **Wenn sie sich hierfür entscheiden, sollte die Erklärung zur Unternehmensführung einen Verweis auf die Nachhaltigkeitsberichterstattung des Unternehmens enthalten, und die gemäß Artikel 20 der Richtlinie 2013/34/EU erforderlichen Informationen sollten weiterhin den Anforderungen an die Bestätigung der Erklärung zur Unternehmensführung unterliegen.**

- (59) Gemäß Artikel 33 der Richtlinie 2013/34/EU müssen die Mitgliedstaaten dafür sorgen, dass die Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane eines Unternehmens die gemeinsame Aufgabe haben sicherzustellen, dass der Jahresabschluss, der konsolidierte Abschluss, der Lagebericht, der konsolidierte Lagebericht, die Erklärung zur Unternehmensführung und die konsolidierte Erklärung zur Unternehmensführung entsprechend den Anforderungen der genannten Richtlinie erstellt und offengelegt werden. Diese gemeinsame Verantwortung sollte auf die in der Delegierten Verordnung (EU) 2019/815 festgelegten Digitalisierungsanforderungen, auf die Anforderung, die Standards der Union für die Nachhaltigkeitsberichterstattung einzuhalten, und die Anforderung, die Nachhaltigkeitsberichterstattung auszuzeichnen, ausgeweitet werden.

- (60) Es wird zwischen Aufträgen zur Erlangung einer begrenzten Prüfungssicherheit und einer hinreichenden Prüfungssicherheit unterschieden. Bei einem Auftrag zur Erlangung begrenzter Prüfungssicherheit erfolgt die Feststellung in Form einer Negativaussage, d. h. durch die Angabe, dass keine Sachverhalte bekannt geworden sind, die zu der Annahme veranlassen, dass wesentliche falsche Darstellungen enthalten sind. In diesem Fall werden weniger Prüfungen vorgenommen als im Rahmen eines Auftrags zur Erlangung hinreichender Prüfungssicherheit. Die Erlangung begrenzter Prüfungssicherheit verursacht deshalb weniger Arbeitsaufwand als die Erlangung hinreichender Prüfungssicherheit. Ein Auftrag zur Erlangung hinreichender Prüfungssicherheit erfordert umfangreiche Verfahren, einschließlich der Betrachtung der internen Kontrollen des Bericht erstattenden Unternehmens und vertiefter Prüfungen, und ist daher mit deutlich höherem Arbeitsaufwand verbunden als ein Auftrag zur Erlangung begrenzter Prüfungssicherheit. Bei hinreichender Prüfungssicherheit wird in der Regel eine positive Feststellung getroffen, und sie resultiert in einem Urteil über die Messung des Prüfgegenstands an im Voraus festgelegten Kriterien. Gemäß der Richtlinie 2013/34/EU müssen die Mitgliedstaaten sicherstellen, dass der Abschlussprüfer oder die Prüfungsgesellschaft prüft, ob die nichtfinanzielle Erklärung oder der gesonderte Bericht vorgelegt wurde. Die Richtlinie schreibt nicht vor, dass ein unabhängiger Erbringer von Bestätigungsleistungen die Informationen überprüft, gestattet es den Mitgliedstaaten jedoch, eine solche Überprüfung zu verlangen, wenn sie dies für sinnvoll halten.

Wenn im Gegensatz zur Verpflichtung des Abschlussprüfers, die Abschlussprüfung auf der Grundlage einer hinreichenden Prüfungssicherheit durchzuführen, bei der Nachhaltigkeitsberichterstattung keine Bestätigung verlangt werden würde, so würde dies der Glaubwürdigkeit der offengelegten Nachhaltigkeitsinformationen schaden und würden die Bedürfnisse der Nutzer, für die diese Informationen bestimmt sind, nicht erfüllt. Bei der Finanzberichterstattung und bei der Nachhaltigkeitsberichterstattung soll letztlich ein ähnliches Maß an Prüfungssicherheit erreicht werden, doch besteht in Ermangelung eines gemeinsam vereinbarten Standards für die Bestätigung der Nachhaltigkeitsberichterstattung die Gefahr einer unterschiedlichen Auslegung und unterschiedlicher Erwartungen hinsichtlich dessen, was ein Auftrag zur Erlangung hinreichender Prüfungssicherheit bei verschiedenen Kategorien von Nachhaltigkeitsinformationen, insbesondere bei zukunftsgerichteten und qualitativen Offenlegungen, beinhaltet. Daher sollte im Hinblick auf Nachhaltigkeitsinformationen ein Ansatz zur progressiven Erhöhung der verlangten Prüfungssicherheit in Betracht gezogen werden, beginnend mit der Verpflichtung des Abschlussprüfers oder der Prüfungsgesellschaft, auf der Grundlage eines Auftrags zur Erlangung begrenzter Prüfungssicherheit ein Urteil darüber abzugeben, ob die Nachhaltigkeitsberichterstattung den Anforderungen der Union entspricht. Dabei sollte nicht nur die Einhaltung der Standards der Union für die Nachhaltigkeitsberichterstattung bewertet werden, sondern auch das vom Unternehmen genutzte Verfahren zur Ermittlung der Informationen, über die gemäß den Standards für die Nachhaltigkeitsberichterstattung Bericht erstattet wurde, und die Erfüllung der Pflicht zur Auszeichnung der Nachhaltigkeitsberichterstattung. Der Prüfer sollte ferner bewerten, ob das Unternehmen in seiner Berichterstattung den Berichterstattungsanforderungen gemäß Artikel 8 der Verordnung (EU) 2020/852 genügt.

Wenn die Kommission **bis spätestens 1. Oktober 2028 nach einer Bewertung dessen, ob hinreichende Prüfungssicherheit für Prüfer und Unternehmen möglich wäre**, mittels delegierter Rechtsakte Standards für die Erlangung hinreichender Prüfungssicherheit bei der Bestätigung der Nachhaltigkeitsberichterstattung annimmt, sollte zur Gewährleistung eines gemeinsamen Verständnisses und gemeinsamer Erwartungen hinsichtlich dessen, was unter hinreichender Prüfungssicherheit zu verstehen ist, der Abschlussprüfer oder die Prüfungsgesellschaft verpflichtet sein, auf der Grundlage eines Auftrags zur Erlangung hinreichender Prüfungssicherheit ein Urteil über die Übereinstimmung der Nachhaltigkeitsberichterstattung mit den Anforderungen der Union abzugeben.

Der allmähliche Übergang von der begrenzten Prüfungssicherheit zur hinreichenden Prüfungssicherheit würde auch die Voraussetzung **dafür** schaffen, dass allmählich ein Markt für die Bestätigung von Nachhaltigkeitsinformationen entsteht und die Unternehmen eine bestimmte Berichterstattungspraxis entwickeln. Dieser allmähliche Ansatz würde schrittweise zu einem Anstieg der Kosten für die Bericht erstattenden Unternehmen führen, da die Bestätigung der Nachhaltigkeitsberichterstattung auf der Grundlage einer hinreichenden Prüfungssicherheit mit höheren Kosten verbunden ist als die Bestätigung der Nachhaltigkeitsberichterstattung auf der Grundlage einer begrenzten Prüfungssicherheit. **Unternehmen, die Anforderungen an die Nachhaltigkeitsberichterstattung unterliegen, sollten sich dafür entscheiden können, ein Bestätigungsurteil zu ihrer Nachhaltigkeitsberichterstattung auf der Grundlage eines Auftrags zur Erlangung hinreichender Prüfungssicherheit einzuholen, wenn sie dies wünschen, wobei in diesem Fall davon ausgegangen werden sollte, dass sie der Verpflichtung nachgekommen sind, ein Urteil auf der Grundlage eines Auftrags zur Erlangung begrenzter Prüfungssicherheit einzuholen. Das Urteil auf der Grundlage eines Auftrags zur Erlangung hinreichender Prüfungssicherheit bei zukunftsbezogenen Informationen bietet lediglich Gewähr dafür, dass diese Informationen im Einklang mit den geltenden Standards erstellt wurden.**

- (61) Abschlussprüfer oder Prüfungsgesellschaften überprüfen bereits Jahresabschluss und Lagebericht. Die Bestätigung der Nachhaltigkeitsberichterstattung durch die Abschlussprüfer oder Prüfungsgesellschaften würde dazu beitragen, die Verknüpfung zwischen Finanz- und Nachhaltigkeitsinformationen und deren Kohärenz zu gewährleisten, was für die Nutzer von Nachhaltigkeitsinformationen von besonderer Bedeutung ist. Allerdings besteht die Gefahr einer weiteren Konzentration am Markt für Abschlussprüfungen, wodurch die Unabhängigkeit der Prüfer gefährdet würde und sich die **Abschlussprüfungshonorare oder die Honorare in Bezug auf die Bestätigung der Nachhaltigkeitsberichterstattung erhöhen könnten. Angesichts der Schlüsselrolle, die Abschlussprüfer bei der Bestätigung der Nachhaltigkeitsberichterstattung und der Gewährleistung zuverlässiger Nachhaltigkeitsinformationen spielen, hat die Kommission angekündigt, dass sie tätig werden wird, damit sich die Qualität der Abschlussprüfung weiter verbessert und ein offenerer, stärker diversifizierter Prüfungsmarkt entsteht, was die Voraussetzung für eine erfolgreiche Anwendung dieser Änderungsrichtlinie darstellt. Darüber hinaus ist es im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung wünschenswert, dass die Unternehmen auf eine größere Auswahl an unabhängigen Erbringern von Bestätigungsleistungen zurückgreifen können. Die Mitgliedstaaten sollten daher die Möglichkeit haben, unabhängige Erbringer von Bestätigungsleistungen gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates⁶⁹ für die Abgabe eines Bestätigungsurteils über die Nachhaltigkeitsberichterstattung zur gemeinsamen Veröffentlichung mit dem Lagebericht zu akkreditieren. **Darüber hinaus sollten die Mitgliedstaaten die Möglichkeit haben, einem anderen Abschlussprüfer als dem- oder denjenigen, die die Abschlussprüfung durchführen, zu gestatten, ein Bestätigungsurteil über die Nachhaltigkeitsberichterstattung abzugeben. Gestatten sie zudem unabhängigen Erbringern von Bestätigungsleistungen, die Bestätigung der Nachhaltigkeitsberichterstattung durchzuführen, so sollten die Mitgliedstaaten auch einem anderen Abschlussprüfer als dem- oder denjenigen, die die****

⁶⁹ Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

Abschlussprüfung durchführen, gestatten, ein Bestätigungsurteil über die Nachhaltigkeitsberichterstattung abzugeben.

Die Mitgliedstaaten sollten Anforderungen festlegen, mit denen die Qualität der von unabhängigen Erbringern von Bestätigungsleistungen durchgeführten Bestätigungen der Nachhaltigkeitsberichterstattung sowie kohärente Ergebnisse bei der Bestätigung der Nachhaltigkeitsberichterstattung sichergestellt werden.

Daher sollten alle unabhängigen Erbringer von Bestätigungsleistungen Anforderungen unterliegen, die in Bezug auf die Bestätigung der Nachhaltigkeitsberichterstattung den in der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates⁷⁰ festgelegten Anforderungen ***gleichwertig sind, jedoch an die Merkmale unabhängiger Erbringer von Bestätigungsleistungen, die keine Abschlussprüfungen durchführen, angepasst sind. Insbesondere sollten die Mitgliedstaaten gleichwertige Anforderungen an Ausbildung und Eignungsprüfung, kontinuierliche Fortbildung, Qualitätssicherungssysteme, Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis, Bestellung und Abberufung, die Organisation der Arbeit der unabhängigen Erbringer von Bestätigungsleistungen, Untersuchungen und Sanktionen sowie die Meldung von Unregelmäßigkeiten festlegen.*** Dies würde zudem gleiche Wettbewerbsbedingungen für alle Personen und Gesellschaften gewährleisten, die von den Mitgliedstaaten dazu befugt werden, ein Bestätigungsurteil über die Nachhaltigkeitsberichterstattung abzugeben, einschließlich Abschlussprüfern. Beschließt ein Unternehmen, das Urteil über seine Nachhaltigkeitsberichterstattung bei einem akkreditierten unabhängigen Erbringer von Bestätigungsleistungen einzuholen, der nicht sein Abschlussprüfer ist, so sollte es nicht zusätzlich ein Bestätigungsurteil des Abschlussprüfers zu seiner Nachhaltigkeitsberichterstattung einholen müssen.

⁷⁰

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).

Unabhängige Erbringer von Bestätigungsleistungen, die bereits von einem Mitgliedstaat für die Bestätigung der Nachhaltigkeitsberichterstattung akkreditiert wurden, sollten ebensolche auch weiterhin durchführen dürfen. Ebenso sollten die Mitgliedstaaten sicherstellen, dass unabhängige Erbringer von Bestätigungsleistungen, die zum Zeitpunkt des Inkrafttretens der neuen Anforderungen an Ausbildung und Eignungsprüfung ihr Akkreditierungsverfahren durchlaufen, diesen neuen Akkreditierungsanforderungen nicht unterliegen, sofern sie das Verfahren innerhalb von zwei Jahren nach dem Geltungsbeginn dieser neuen Anforderungen abschließen. Die Mitgliedstaaten sollten jedoch sicherstellen, dass alle unabhängigen Erbringer von Bestätigungsleistungen, die innerhalb von zwei Jahren nach dem Geltungsbeginn der neuen Akkreditierungsanforderungen für die Bestätigung der Nachhaltigkeitsberichterstattung durch einen Mitgliedstaat akkreditiert wurden, durch kontinuierliche berufliche Fortbildung die erforderlichen Kenntnisse auf dem Gebiet der Nachhaltigkeitsberichterstattung und deren Bestätigung erwerben.

- (62) *Um den freien Dienstleistungsverkehr zu fördern, sollten die Mitgliedstaaten unabhängigen Erbringern von Bestätigungsleistungen, die in einem anderen Mitgliedstaat niedergelassen sind, gestatten, die Bestätigung der Nachhaltigkeitsberichterstattung in ihrem Hoheitsgebiet durchzuführen. Dies würde auch die Öffnung des Marktes für Bestätigungsleistungen begünstigen, auch wenn nicht alle Mitgliedstaaten die Akkreditierung unabhängiger Erbringer von Bestätigungsleistungen in ihrem Hoheitsgebiet zulassen. Wenn unabhängige Erbringer von Bestätigungsleistungen die Bestätigung der Nachhaltigkeitsberichterstattung im Hoheitsgebiet eines Aufnahmemitgliedstaats durchführen, sollte dieser Aufnahmemitgliedstaat beschließen können, unabhängige Erbringer von Bestätigungsleistungen zu beaufsichtigen, wobei die Möglichkeit besteht, den umgesetzten Rahmen für die Beaufsichtigung von Abschlussprüfern, die Bestätigungen der Nachhaltigkeitsberichterstattung durchführen, zu nutzen.*
- (63) *Die Mitgliedstaaten sollten sicherstellen, dass in Fällen, in denen ein Unternehmen nach dem Unionsrecht verpflichtet ist, Teile seiner Nachhaltigkeitsberichterstattung durch eine akkreditierte unabhängige dritte Partei prüfen zu lassen, der Bericht der akkreditierten unabhängigen dritten Partei entweder als Anlage zum Lagebericht oder auf andere öffentlich zugängliche Weise bereitgestellt werden sollte. Eine solche Bereitstellung sollte dem Ergebnis des Bestätigungsurteils, das von der Überprüfung durch dritte Parteien unabhängig bleiben sollte, nicht vorgreifen. Es sollte nicht zu Doppelarbeit zwischen dem Abschlussprüfer oder dem unabhängigen Erbringer von Bestätigungsleistungen, der das Bestätigungsurteil abgibt, und der akkreditierten unabhängigen dritten Partei führen.*

- (64) Die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates enthält Vorschriften für die Abschlussprüfung von Jahresabschlüssen und konsolidierten Abschlüssen. Bei den Regeln für die Prüfung von Abschlüssen und die Bestätigung der Nachhaltigkeitsberichterstattung durch den Abschlussprüfer muss Kohärenz gewährleistet sein. Wenn das Bestätigungsurteil über die Nachhaltigkeitsberichterstattung **von einem** Abschlussprüfer oder **einer** Prüfungsgesellschaft ■ abgegeben wird, sollte die Richtlinie 2006/43/EG gelten.
- (65) Im Rahmen der Vorschriften über die Zulassung und Anerkennung von Abschlussprüfern und Prüfungsgesellschaften sollten **Abschlussprüfer sich auch für die Bestätigung der Nachhaltigkeitsberichterstattung qualifizieren können. Die Mitgliedstaaten** sollten sicherstellen, dass Abschlussprüfer, **die sich für die Bestätigung der Nachhaltigkeitsberichterstattung qualifizieren möchten**, über die erforderlichen theoretischen Kenntnisse in Bereichen, die für die **Bestätigung** der Nachhaltigkeitsberichterstattung relevant sind, verfügen und dass sie in der Lage sind, diese Kenntnisse in der Praxis anzuwenden.

Daher sollten Abschlussprüfer eine mindestens achtmonatige praktische Ausbildung zur Bestätigung der jährlichen und konsolidierten Nachhaltigkeitsberichterstattung oder in anderen nachhaltigkeitsbezogenen Dienstleistungen absolvieren, wobei frühere Berufserfahrung berücksichtigt werden sollte. Abschlussprüfer, die bereits von einem Mitgliedstaat zugelassen oder anerkannt wurden, sollten weiterhin *Bestätigungen der* Nachhaltigkeitsberichterstattung durchführen dürfen. *Ebenso sollten die Mitgliedstaaten sicherstellen, dass natürliche Personen, die zum Zeitpunkt des Inkrafttretens solcher neuer Anforderungen an die Bestätigung der Nachhaltigkeitsberichterstattung das Zulassungsverfahren durchlaufen, diesen Anforderungen nicht unterliegen, sofern sie das Verfahren innerhalb der folgenden zwei Jahre abschließen.* Die Mitgliedstaaten sollten jedoch sicherstellen, dass *Abschlussprüfer, die innerhalb von zwei Jahren nach dem Geltungsbeginn dieser Anforderungen zugelassen werden und Bestätigung der Nachhaltigkeitsberichterstattung durchführen wollen,* durch kontinuierliche berufliche Fortbildung die erforderlichen Kenntnisse im Bereich der Nachhaltigkeitsberichterstattung und deren *Bestätigung* erwerben.

Natürliche Personen, die sich entschließen, lediglich eine Zulassung als Abschlussprüfer für die Abschlussprüfung zu erwerben, sollten sich zu einem späteren Zeitpunkt entschließen können, sich auch für die Bestätigung der Nachhaltigkeitsberichterstattung zu qualifizieren. Hierzu sollten diese Personen die Anforderungen erfüllen, die von den Mitgliedstaaten festgelegt wurden, um sicherzustellen, dass sie auch über die erforderlichen theoretischen Kenntnisse in Bereichen, die für die Bestätigung der Nachhaltigkeitsberichterstattung relevant sind, verfügen und dass sie in der Lage sind, diese Kenntnisse in der Praxis anzuwenden.

- (66) Es sollte sichergestellt werden, dass Abschlussprüfer in Bezug auf die Abschlussprüfung und die Bestätigung der Nachhaltigkeitsberichterstattung kohärenten Anforderungen unterliegen. Daher sollte **mindestens eine benannte Person** aktiv an der Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung beteiligt **sein („verantwortlicher Nachhaltigkeitspartner“)**. Abschlussprüfer sollten verpflichtet sein, bei der Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung ausreichend Zeit für das Mandat aufzubringen und die zur angemessenen Wahrnehmung ihrer Aufgaben erforderlichen Ressourcen **und das entsprechend notwendige Fachwissen** vorzusehen. In der Mandantendatei sollten die Gebühren angegeben werden, die für die Bestätigung der Nachhaltigkeitsberichterstattung in Rechnung gestellt werden, und **es sollte eine Bestätigungsakte angelegt werden**, die Informationen über die Bestätigung der Nachhaltigkeitsberichterstattung enthält. **Führt derselbe Abschlussprüfer die Abschlussprüfung des Jahresabschlusses und die Bestätigung der Nachhaltigkeitsberichterstattung durch, so sollte die Bestätigungsakte in die Prüfungsakte aufgenommen werden können.** **Anforderungen an Abschlussprüfer in Bezug auf die Bestätigung der Nachhaltigkeitsberichterstattung sollten jedoch nur für die Abschlussprüfer gelten, die die Bestätigung der Nachhaltigkeitsberichterstattung durchführen.**

- (67) ***Abschlussprüfer oder Prüfungsgesellschaften, die die Bestätigung der Nachhaltigkeitsberichterstattung durchführen, sollten über ein hohes Maß an technischem und spezifischem Fachwissen auf dem Gebiet der Nachhaltigkeit verfügen.***
- (68) Gemäß der Richtlinie 2006/43/EG sorgen die Mitgliedstaaten für eine angemessene Regelung, die vermeidet, dass Honorare für Abschlussprüfungen von der Erbringung zusätzlicher Leistungen für das geprüfte Unternehmen beeinflusst oder bestimmt oder an Bedingungen geknüpft werden. Gemäß der genannten Richtlinie sorgen die Mitgliedstaaten ebenfalls dafür, dass Abschlussprüfer, die Abschlussprüfungen durchführen, Anforderungen im Hinblick auf Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis erfüllen. Aus Gründen der Kohärenz sollten diesen Vorschriften auch auf Abschlussprüfer, die Bestätigungen der Nachhaltigkeitsberichterstattung durchführen, ausgeweitet werden.

- (69) Um bei der Nachhaltigkeitsberichterstattung unionsweit einheitliche Bestätigungsverfahren und eine hochwertige Bestätigung der Nachhaltigkeitsberichterstattung zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, mittels delegierter Rechtsakte Standards für die Bestätigung der Nachhaltigkeitsberichterstattung anzunehmen. Den Mitgliedstaaten **sollte die Möglichkeit eingeräumt werden**, nationale Bestätigungsstandards, -verfahren oder -anforderungen **anzuwenden**, solange die Kommission keine Bestätigungsstandards, die für denselben Bereich gelten, mittels delegierter Rechtsakte angenommen hat. In diesen Standards sollten die Verfahren festgelegt werden, anhand deren der Abschlussprüfer seine Schlussfolgerungen zur Bestätigung der Nachhaltigkeitsberichterstattung zu ziehen hat. **Daher sollte die Kommission vor dem 1. Oktober 2026 mittels delegierter Rechtsakte Bestätigungsstandards für die begrenzte Prüfungssicherheit erlassen. Um die Harmonisierung der Bestätigung der Nachhaltigkeitsberichterstattung in den Mitgliedstaaten zu erleichtern, sollte der Ausschuss der Aufsichtsstellen ermutigt werden, unverbindliche Leitlinien anzunehmen, um die Verfahren festzulegen, die bei der Abgabe eines Bestätigungsurteils über die Nachhaltigkeitsberichterstattung anzuwenden sind, bis die Kommission Bestätigungsstandards für denselben Bereich annimmt.**
- (70) Die Richtlinie 2006/43/EG enthält Vorschriften für die Abschlussprüfung von Unternehmensgruppen. **Ähnliche** Vorschriften sollten **■** für die Bestätigung **der** konsolidierten Nachhaltigkeitsberichterstattung **festgelegt werden**.

- (71) Gemäß der Richtlinie 2006/43/EG legen der Abschlussprüfer oder die Prüfungsgesellschaften die Ergebnisse der Abschlussprüfung in einem Bestätigungsvermerk dar. **Ähnliche Vorschriften sollten für die Bestätigung der Nachhaltigkeitsberichterstattung festgelegt werden. Die Ergebnisse der Bestätigung der Nachhaltigkeitsberichterstattung sollten in einem Prüfungsvermerk dargelegt werden. Führt derselbe Abschlussprüfer die Abschlussprüfung des Jahresabschlusses und die Bestätigung der Nachhaltigkeitsberichterstattung durch, so sollten die Informationen über die Bestätigung der Nachhaltigkeitsberichterstattung in den Bestätigungsvermerk aufgenommen werden können.**
- (72) Gemäß der Richtlinie 2006/43/EG richten die Mitgliedstaaten ein Qualitätssicherungssystem für Abschlussprüfer und Prüfungsgesellschaften ein. Um sicherzustellen, dass auch bei der Bestätigung der Nachhaltigkeitsberichterstattung eine Qualitätssicherung erfolgt und dass die Qualitätssicherungsprüfer über eine angemessene fachliche Ausbildung und einschlägige Erfahrung auf dem Gebiet der Nachhaltigkeitsberichterstattung und der Bestätigung der Nachhaltigkeitsberichterstattung verfügen, sollte diese Anforderung zur Einrichtung eines Systems der Qualitätssicherungsprüfung auch für die Bestätigung der Nachhaltigkeitsberichterstattung gelten. **Als Übergangsmaßnahme sollten die Personen, die Qualitätssicherungsprüfungen im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung durchführen, bis zum 31. Dezember 2025 von der Anforderung befreit werden, über einschlägige Erfahrung auf dem Gebiet der Nachhaltigkeitsberichterstattung und der Bestätigung der Nachhaltigkeitsberichterstattung oder anderer nachhaltigkeitsbezogener Dienstleistungen zu verfügen.**

- (73) Gemäß der Richtlinie 2006/43/EG müssen die Mitgliedstaaten über ein System für Untersuchungen und Sanktionen für Abschlussprüfer und Prüfungsgesellschaften, die Abschlussprüfungen durchführen, verfügen. Gemäß der genannten Richtlinie müssen die Mitgliedstaaten ein wirksames System für die öffentliche Aufsicht einrichten und sicherstellen, dass die Regelungen für öffentliche Aufsichtssysteme auf Unionsebene eine wirksame Zusammenarbeit bei den Aufsichtstätigkeiten der Mitgliedstaaten ermöglichen. Diese Anforderungen sollten auch für Abschlussprüfer und Prüfungsgesellschaften gelten, die die Nachhaltigkeitsberichterstattung bestätigen, um die Kohärenz von Untersuchungen, Sanktionen und Aufsichtsrahmen für die Arbeit des Prüfers im Bereich der Abschlussprüfung und der Bestätigung der Nachhaltigkeitsberichterstattung sicherzustellen.
- (74) Die Richtlinie 2006/43/EG enthält Vorschriften über die Bestellung und Entlassung von Abschlussprüfern und Prüfungsgesellschaften, die Abschlussprüfungen durchführen. Diese Vorschriften sollten auch für die Bestätigung der Nachhaltigkeitsberichterstattung gelten, um die Kohärenz der Vorschriften, denen Prüfer im Bereich der Abschlussprüfung und der Bestätigung der Nachhaltigkeitsberichterstattung unterliegen, sicherzustellen.

- (75) *Gemäß Artikel 6 der Richtlinie 2007/36/EG des Europäischen Parlaments und des Rates⁷¹ haben die Mitgliedstaaten sicherzustellen, dass Aktionäre von Unternehmen, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind, die einzeln oder gemeinsam handeln, das Recht haben, Punkte auf die Tagesordnung der Hauptversammlung der Aktionäre zu setzen, sofern jedem dieser Punkte eine Begründung oder ein Beschlussentwurf beigelegt ist, der in der Hauptversammlung anzunehmen ist, und dass sie das Recht haben, Beschlussentwürfe für Punkte einzureichen, die in die Tagesordnung einer Hauptversammlung aufgenommen wurden oder aufgenommen werden sollen. Sind diese Rechte an die Bedingung geknüpft, dass der bzw. die betreffenden Aktionäre eine Mindestbeteiligung am Unternehmen halten, so darf diese Mindestbeteiligung 5 % des Gesellschaftskapitals nicht überschreiten. Was die Bestätigung der Nachhaltigkeitsberichterstattung betrifft, sollten die Aktionäre die in Artikel 6 der Richtlinie 2007/36/EG festgelegten Rechte ausüben können, um Beschlussentwürfe, die in der Hauptversammlung anzunehmen sind, vorzulegen, nach denen zum einen ein zugelassener Dritter, der nicht derselben Prüfungsgesellschaft oder demselben -netzwerk angehört wie der Abschlussprüfer oder die Prüfungsgesellschaft, der bzw. die die Abschlussprüfung durchführt, einen Bericht über bestimmte Teile der Nachhaltigkeitsberichterstattung erstellen muss und zum anderen dieser Bericht der Hauptversammlung zur Verfügung gestellt werden muss. Bei Unternehmen, die den durch diese Änderungsrichtlinie eingeführten Anforderungen an die Nachhaltigkeitsberichterstattung unterliegen und nicht in den Anwendungsbereich von Artikel 6 der Richtlinie 2007/36/EG fallen, sollten Aktionäre, die einzeln oder gemeinsam mehr als 5 % der Stimmrechte oder 5 % des Kapitals des Unternehmens vertreten bzw. halten, auch das Recht erhalten, ein Beschlussentwurf, die in der Hauptversammlung anzunehmen ist, auf die Tagesordnung zu setzen, nach der zum einen ein akkreditierter Dritter, der nicht derselben Prüfungsgesellschaft oder demselben Netzwerk angehört wie der Abschlussprüfer oder die Prüfungsgesellschaft, die bzw. der die Abschlussprüfung durchführt, einen Bericht über bestimmte Teile der*

⁷¹ Richtlinie 2007/36/EG des Europäischen Parlaments und des Rates vom 11. Juli 2007 über die Ausübung bestimmter Rechte von Aktionären in börsennotierten Gesellschaften (ABl. L 184 vom 14.7.2007, S. 17).

Nachhaltigkeitsberichterstattung erstellen muss und zum anderen dieser Bericht der Hauptversammlung zur Verfügung gestellt werden muss.

- (76) Die Richtlinie 2006/43/EG verlangt, dass die Mitgliedstaaten sicherstellen, dass jedes Unternehmen von öffentlichem Interesse einen Prüfungsausschuss hat, und legt dessen Aufgaben im Zusammenhang mit der Abschlussprüfung fest. Diesem Prüfungsausschuss sollten bestimmte Aufgaben im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung übertragen werden. Diese Aufgaben sollten auch die Verpflichtung umfassen, das Verwaltungs- oder Aufsichtsorgan des Unternehmens von öffentlichem Interesse über die Ergebnisse der Bestätigung der Nachhaltigkeitsberichterstattung zu unterrichten und zu erläutern, wie der Prüfungsausschuss zur Integrität der Nachhaltigkeitsberichterstattung beigetragen hat und welche Rolle der Prüfungsausschuss dabei spielte. **Die Mitgliedstaaten sollten gestatten können, dass die dem Prüfungsausschuss übertragenen Aufgaben im Zusammenhang mit der Nachhaltigkeitsberichterstattung und im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung von dem Verwaltungs- oder Aufsichtsorgan in seiner Gesamtheit oder von einem vom Verwaltungs- oder Aufsichtsorgan eigens eingerichteten Gremium wahrgenommen werden.**
- (77) Die Richtlinie 2006/43/EG enthält Anforderungen an die Registrierung von Abschlussprüfern und Prüfungsgesellschaften aus Drittländern und die Aufsicht über diese. Um einen kohärenten Rahmen für die Tätigkeiten der Prüfer bei der Abschlussprüfung und bei der Bestätigung der Nachhaltigkeitsberichterstattung sicherzustellen, müssen diese Anforderungen auch für die Bestätigung der Nachhaltigkeitsberichterstattung gelten.

- (78) Die Verordnung (EU) Nr. 537/2014 des Europäischen Parlaments und des Rates⁷² gilt für Abschlussprüfer und Prüfungsgesellschaften, die Abschlussprüfungen bei Unternehmen von öffentlichem Interesse durchführen. Um die Unabhängigkeit des Abschlussprüfers **bei der Durchführung einer Abschlussprüfung zu gewährleisten, wird in der genannten Verordnung eine Begrenzung der Honorare, die er für andere Leistungen erhalten kann, festgelegt. Es ist wichtig klarzustellen, dass die Bestätigung der Nachhaltigkeitsberichterstattung bei der Berechnung dieser Begrenzung nicht berücksichtigt werden sollte. Darüber hinaus** verbietet die Verordnung (EU) Nr. 537/2014 während bestimmter Zeiträume die Erbringung bestimmter Nichtprüfungsleistungen, **wenn der Abschlussprüfer die Abschlussprüfung durchführt. Leistungen im Zusammenhang mit der Erstellung der Nachhaltigkeitsberichterstattung, einschließlich jeglicher Beratungsleistungen, sollten während des in der Verordnung (EU) Nr. 537/2014 festgelegten Zeitraums ebenfalls als verbotene Leistungen betrachtet werden. Das Verbot der Erbringung solcher Leistungen sollte in allen Fällen gelten, in denen der Abschlussprüfer die Abschlussprüfung durchführt. Um die Unabhängigkeit des Abschlussprüfers zu gewährleisten, sollten auch bestimmte Nichtprüfungsleistungen verboten werden, wenn der Abschlussprüfer die Bestätigung der Nachhaltigkeitsberichterstattung durchführt. Gemäß der Verordnung (EU) Nr. 537/2014 sind Abschlussprüfer verpflichtet, Unregelmäßigkeiten dem geprüften Unternehmen und unter bestimmten Umständen den von den Mitgliedstaaten benannten Behörden, die für die Untersuchung solcher Unregelmäßigkeiten verantwortlich sind, zu melden. Solche Pflichten sollten gegebenenfalls auch auf Abschlussprüfer und Prüfungsgesellschaften im Hinblick auf ihre Tätigkeiten zur Bestätigung der Nachhaltigkeitsberichterstattung bei Unternehmen von öffentlichem Interesse ausgeweitet werden.**

⁷² Verordnung (EU) Nr. 537/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über spezifische Anforderungen an die Abschlussprüfung bei Unternehmen von öffentlichem Interesse und zur Aufhebung des Beschlusses 2005/909/EG der Kommission (ABl. L 158 vom 27.5.2014, S. 77).

I

- (79) In der Richtlinie 2004/109/EG wird die Aufgabe der Durchsetzung der Anforderungen an die Unternehmensberichterstattung durch Unternehmen, deren Wertpapiere ***zum Handel auf einem geregelten Markt in der Union zugelassen*** sind, den nationalen Aufsichtsbehörden übertragen. Artikel 4 der genannten Richtlinie legt den Inhalt der Jahresfinanzberichte fest, enthält jedoch keinen expliziten Verweis auf die Artikel 19a und 29a der Richtlinie 2013/34/EU, in denen die Erstellung einer nichtfinanziellen Erklärung und einer konsolidierten nichtfinanziellen Erklärung vorgeschrieben ist. Dies bedeutet in der Folge, dass die zuständigen nationalen Behörden einiger Mitgliedstaaten rechtlich nicht befugt sind, diese nichtfinanziellen Erklärungen zu überwachen, insbesondere wenn diese nichtfinanziellen Erklärungen in einem gesonderten Bericht außerhalb des Jahresabschlusses veröffentlicht werden, was die Mitgliedstaaten derzeit zulassen können. Daher ist es notwendig, in Artikel 4 Absatz 5 der Richtlinie 2004/109/EG einen Verweis auf die Nachhaltigkeitsberichterstattung aufzunehmen. Außerdem müssen die verantwortlichen Personen beim Emittenten dazu verpflichtet werden, im Jahresfinanzbericht zu bestätigen, dass der Lagebericht nach ihrem besten Wissen entsprechend den Standards für die Nachhaltigkeitsberichterstattung erstellt wird. Darüber hinaus sollte die ESMA angesichts des neuartigen Charakters dieser Anforderungen an die Nachhaltigkeitsberichterstattung Leitlinien für die zuständigen nationalen Behörden herausgeben, um eine konvergierende Aufsicht der Nachhaltigkeitsberichterstattung durch Emittenten, die der Richtlinie 2004/109/EG unterliegen, zu fördern. ***Diese Leitlinien sollten nur für die Beaufsichtigung von Unternehmen gelten, deren Wertpapiere zum Handel auf einem geregelten Markt in der Union zugelassen sind.***

- (80) Um die Anforderungen dieser Änderungsrichtlinie festzulegen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte hinsichtlich der Festlegung von Standards für die Nachhaltigkeitsberichterstattung, der Festlegung gleichwertiger Standards für Drittlandsunternehmen und der Festlegung von Standards für die Bestätigung der Nachhaltigkeitsberichterstattung zu erlassen. 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 Rechtsetzung⁷³ 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.

⁷³

ABl. L 123 vom 12.5.2016, S. 1.

I

- (81) *Die Kommission sollte dem Europäischen Parlament und dem Rat einen Bericht über die Umsetzung dieser Änderungsrichtlinie vorlegen, der unter anderem Folgendes umfasst: eine Bewertung der Erreichung der Ziele dieser Änderungsrichtlinie, einschließlich der Konvergenz der Berichterstattungsverfahren zwischen Mitgliedstaaten; eine Bewertung der Zahl der kleinen und mittleren Unternehmen, die freiwillig Standards für die Nachhaltigkeitsberichterstattung anwenden; eine Bewertung, ob und wie der Anwendungsbereich der Berichterstattungsanforderungen ausgeweitet werden sollte, insbesondere in Bezug auf kleine und mittlere Unternehmen und Drittlandsunternehmen, die ohne ein Tochterunternehmen oder eine Zweigniederlassung im Gebiet der Union unmittelbar im Binnenmarkt der Union tätig sind; eine Bewertung der Umsetzung der mit dieser Änderungsrichtlinie eingeführten Berichterstattungsanforderungen für Tochterunternehmen und Zweigniederlassungen von Drittlandsunternehmen, einschließlich einer Bewertung der Zahl der Drittlandsunternehmen, die über ein Tochterunternehmen oder eine Zweigniederlassung verfügen, das bzw. die Berichterstattungsanforderungen gemäß der Richtlinie 2013/34/EU unterliegt bzw. unterliegen; eine Bewertung des Durchsetzungsmechanismus und der einschlägigen in der Richtlinie 2013/34/EU festgelegten Schwellenwerte; eine Bewertung, ob und wie der Zugang von Menschen mit Behinderungen zu der Nachhaltigkeitsberichterstattung sichergestellt werden kann, die von Unternehmen veröffentlicht wird, die in den Anwendungsbereich dieser Änderungsrichtlinie fallen.*

Der Bericht über die Umsetzung dieser Änderungsrichtlinie sollte bis zum 30. April 2029 und danach alle drei Jahre veröffentlicht und gegebenenfalls durch Legislativvorschläge ergänzt werden. Bis zum 31. Dezember 2028 sollte die Kommission den Konzentrationsgrad des Marktes für die Bestätigung der Nachhaltigkeitsprüfung überprüfen und darüber Bericht erstatten. Bei der Überprüfung sollten die für unabhängige Erbringer von Bestätigungsleistungen geltenden nationalen Regelungen berücksichtigt werden, und es sollte bewertet werden, ob und inwieweit diese nationalen Regelungen zur Öffnung des Marktes für Bestätigungsleistungen beitragen. Bis zum 31. Dezember 2028 sollte die Kommission mögliche rechtliche Maßnahmen prüfen, um eine ausreichende Diversifizierung des Marktes für die Bestätigung der Nachhaltigkeitsprüfung und eine angemessene Qualität der Nachhaltigkeitsberichterstattung zu gewährleisten. Der Bericht über den Konzentrationsgrad des Marktes für die Bestätigung der Nachhaltigkeitsprüfung sollte dem Europäischen Parlament und dem Rat bis zum 31. Dezember 2028 übermittelt und gegebenenfalls durch Legislativvorschläge ergänzt werden.

- (82) Da die Ziele dieser Änderungsrichtlinie von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder 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 Änderungsrichtlinie nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(83) Die Verordnung (EU) Nr. 537/2014 und die Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU sollten daher entsprechend geändert werden.

(84) *Die EZB wurde angehört und hat ihre Stellungnahme am 7. September 2021 abgegeben –*

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1
Änderung der Richtlinie 2013/34/EU

Die Richtlinie 2013/34/EU wird wie folgt geändert:

- (1) 1. Dem Artikel 1 **werden die folgenden Absätze** angefügt:
- „(3) Die in den Artikeln 19a, ■ 29a, **29d**, 30 und 33, Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa, Artikel 34 Absätze 2 und 3 sowie Artikel 51 der vorliegenden Richtlinie vorgeschriebenen Koordinierungsmaßnahmen gelten unabhängig von der jeweiligen Rechtsform auch für die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für folgende Unternehmen, **sofern es sich um große Unternehmen oder um kleine und mittlere Unternehmen** – mit Ausnahme von Kleinstunternehmen –, **handelt, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der vorliegenden Richtlinie sind:**
- a) Versicherungsunternehmen im Sinne von Artikel 2 Absatz 1 der Richtlinie 91/674/EWG des Rates*;
- b) Kreditinstitute im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates**.

Die Mitgliedstaaten können beschließen, die in Unterabsatz 1 genannten Koordinierungsmaßnahmen nicht auf die in Artikel 2 Absatz 5 Nummern 2 bis 23 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates*** genannten Unternehmen anzuwenden.

- (4) *Die in den Artikeln 19a, 29a und 29d vorgeschriebenen Koordinierungsmaßnahmen gelten nicht für Finanzprodukte nach Artikel 2 Nummer 12 Buchstaben b und f der Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates****.*
- (5) *Die in den Artikeln 40a bis 40d vorgeschriebenen Koordinierungsmaßnahmen gelten auch für die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Tochterunternehmen und Zweigniederlassungen von Unternehmen, die nicht dem Recht eines Mitgliedstaats unterliegen, deren Rechtsform aber den in Anhang I genannten Rechtsformen vergleichbar ist.*

* *Richtlinie 91/674/EWG des Rates vom 19. Dezember 1991 über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen (ABl. L 374 vom 31.12.1991, S. 7).*

** *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).*

*** *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).*

**** *Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27. November 2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor (ABl. L 317 vom 9.12.2019, S. 1).“*

(2) 2. **Artikel 2 wird wie folgt geändert:**

a) **Nummer 5 erhält folgende Fassung:**

„5. ,Nettoumsatzerlöse‘ die Beträge, die sich aus dem Verkauf von Produkten und der Erbringung von Dienstleistungen nach Abzug von Erlösschmälerungen und der Mehrwertsteuer sowie sonstigen direkt mit dem Umsatz verbundenen Steuern ergeben; für Versicherungsunternehmen nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe a der vorliegenden Richtlinie wird der Begriff ,Nettoumsatzerlöse‘ jedoch gemäß Artikeln 35 und Artikel 66 Nummer 2 der Richtlinie 91/674/EWG des Rates* definiert; für Kreditinstitute nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe b der vorliegenden Richtlinie wird der Begriff ,Nettoumsatzerlöse‘ gemäß Artikel 43 Absatz 2 Buchstabe c der Richtlinie 86/635/EWG des Rates definiert; und für Unternehmen, die in den Anwendungsbereich von Artikel 40a Absatz 1 dieser Richtlinie fallen, bezeichnet der Begriff ,Nettoumsatzerlöse‘ die Einnahmen gemäß der Definition durch die bzw. im Sinne der Rechnungslegungsgrundsätze, auf deren Grundlage die Abschlüsse des Unternehmens erstellt werden;**

*** Richtlinie 91/674/EWG des Rates vom 19. Dezember 1991 über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen (ABl. L 374 vom 31.12.1991, S. 7).**

**** Richtlinie 86/635/EWG des Rates vom 8. Dezember 1986 über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten (ABl. L 372 vom 31.12.1986, S. 1).“**

b) Folgende Nummern werden angefügt:

- „17. ‚Nachhaltigkeitsaspekte‘ **Umwelt-, Sozial- und Menschenrechtsfaktoren sowie Governance-Faktoren, einschließlich Nachhaltigkeitsfaktoren** im Sinne von Artikel 2 Nummer 24 der Verordnung (EU) 2019/2088 **■** ;
18. ‚Nachhaltigkeitsberichterstattung‘ die Berichterstattung über Informationen über Nachhaltigkeitsaspekte gemäß den Artikeln 19a, **29a und 29d**;
19. **‚wichtigste immaterielle Ressourcen‘** Ressourcen **ohne physische Substanz, von denen das Geschäftsmodell** des Unternehmens **grundlegend abhängt und die eine Wertschöpfungsquelle für das Unternehmen darstellen**;
20. ‚unabhängiger Erbringer von Bestätigungsleistungen‘ eine Konformitätsbewertungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates* für die in Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa der vorliegenden Richtlinie genannte Konformitätsbewertung akkreditiert ist.

* Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).“

- (3) 3. ***In Artikel 19 Absatz 1 wird folgender Unterabsatz angefügt:***
„Große Unternehmen sowie kleine und mittlere Unternehmen – mit Ausnahme von Kleinstunternehmen –, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a handelt, erstatten Bericht über Informationen über die wichtigsten immateriellen Ressourcen und erläutern, inwiefern das Geschäftsmodell des Unternehmens grundlegend von diesen Ressourcen abhängt und inwiefern diese Ressourcen eine Wertschöpfungsquelle für das Unternehmen darstellen.“
- (4) 4. Artikel 19a erhält folgende Fassung:
„Artikel 19a
Nachhaltigkeitsberichterstattung
- (1) Große Unternehmen sowie ■ kleine und mittlere Unternehmen – mit Ausnahme von Kleinstunternehmen –, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a handelt, nehmen in den Lagebericht Angaben auf, die für das Verständnis der Auswirkungen der Tätigkeiten des Unternehmens auf Nachhaltigkeitsaspekte sowie das Verständnis der Auswirkungen von Nachhaltigkeitsaspekten auf Geschäftsverlauf, Geschäftsergebnis und Lage des Unternehmens erforderlich sind.
- Die in Unterabsatz 1 genannten Angaben müssen im Lagebericht mittels eines dafür vorgesehenen Abschnitts klar erkennbar sein.***

■ 2. Die in Absatz 1 genannten Informationen umfassen ■ Folgendes:

- a) eine kurze Beschreibung von Geschäftsmodell und Strategie des Unternehmens, einschließlich Angaben
 - i) zur Widerstandsfähigkeit von Geschäftsmodell und Strategie des Unternehmens gegenüber Risiken im Zusammenhang mit Nachhaltigkeitsaspekten;
 - ii) zu den Chancen des Unternehmens im Zusammenhang mit Nachhaltigkeitsaspekten;
 - iii) zu der Art und Weise, **einschließlich Durchführungsmaßnahmen und zugehörigen Finanz- und Investitionsplänen**, wie das Unternehmen beabsichtigt sicherzustellen, dass sein Geschäftsmodell und seine Strategie mit dem Übergang zu einer nachhaltigen Wirtschaft und der Begrenzung der Erderwärmung auf 1,5 °C im Einklang mit dem **am 12. Dezember 2015 angenommenen** Übereinkommen von Paris im Rahmen des Rahmenübereinkommens der Vereinten Nationen über Klimaänderungen (im Folgenden „Übereinkommen von Paris“) **und dem in der Verordnung (EU) 2021/1119 des Europäischen Parlaments und des Rates* verankerten Ziel der Verwirklichung der Klimaneutralität bis 2050** vereinbar sind, **und gegebenenfalls die Exposition des Unternehmens gegenüber Aktivitäten mit Bezug zu Kohle, Öl und Gas**;
 - iv) zu der Art und Weise, wie das Unternehmen den Belangen seiner Interessenträger und den Auswirkungen seiner Tätigkeiten auf Nachhaltigkeitsaspekte in seinem Geschäftsmodell und seiner Strategie Rechnung trägt;
 - v) zu der Art und Weise, wie die Strategie des Unternehmens im Hinblick auf Nachhaltigkeitsaspekte umgesetzt wird;

- b) eine Beschreibung der **zeitgebundenen** Nachhaltigkeitsziele, die sich das Unternehmen gesetzt hat, **gegebenenfalls einschließlich der absoluten Ziele für die Verringerung der Treibhausgasemissionen mindestens für 2030 und 2050, eine Beschreibung** der Fortschritte, die **das Unternehmen** im Hinblick auf die Erreichung dieser Ziele erzielt hat, **und eine Erklärung, ob die auf Umweltfaktoren bezogenen Ziele des Unternehmens auf schlüssigen wissenschaftlichen Beweisen beruhen;**
- c) eine Beschreibung der Rolle der Verwaltungs-, Leitungs- und Aufsichtsorgane im Zusammenhang mit Nachhaltigkeitsaspekten **sowie ihres Fachwissens und ihrer Fähigkeiten zur Wahrnehmung dieser Rolle oder ihres Zugangs zu solchem Fachwissen und solchen Fähigkeiten;**
- d) eine Beschreibung der Unternehmenspolitik hinsichtlich Nachhaltigkeit;
- e) **Angaben über das Vorhandensein von mit Nachhaltigkeitsaspekten verknüpften Anreizsystemen, die Mitgliedern der Verwaltungs-, Leitungs- und Aufsichtsorgane angeboten werden;**
- f) eine Beschreibung
 - i) des **vom Unternehmen** mit Blick auf Nachhaltigkeitsaspekte **und gegebenenfalls im Einklang mit den Anforderungen der Union für Unternehmen zur Durchführung eines Due-Diligence-Prozesses** durchgeführten Due-Diligence-Prozesses;

- ii) der wichtigsten tatsächlichen oder potenziellen negativen Auswirkungen, die mit der ***eigenen Geschäftstätigkeit des Unternehmens und mit seiner*** Wertschöpfungskette **■**, einschließlich **■** seiner Produkte und Dienstleistungen, seiner Geschäftsbeziehungen und seiner Lieferkette, verknüpft sind, ***der Maßnahmen zur Ermittlung und Überwachung dieser Auswirkungen, und anderer negativer Auswirkungen, die das Unternehmen gemäß anderen Anforderungen der Union für Unternehmen zur Durchführung eines Due-Diligence-Prozesses ermitteln muss;***
- iii) jeglicher Maßnahmen ***des Unternehmens*** zur Verhinderung, Minderung, ***Behebung oder Beendigung*** tatsächlicher oder potenzieller negativer Auswirkungen und des Erfolgs dieser Maßnahmen;
- g) eine Beschreibung der wichtigsten Risiken, denen das Unternehmen im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt ist, einschließlich einer Beschreibung der wichtigsten Abhängigkeiten in diesem Bereich, und der Handhabung dieser Risiken durch das Unternehmen;
- h) Indikatoren, die für die unter den Buchstaben a bis g genannten Offenlegungen relevant sind. **■**

Die Unternehmen erstattet über den Prozess zur Ermittlung der gemäß Absatz 1 in den Lagebericht aufgenommenen Informationen Bericht **■**. **Die in Unterabsatz 1 des vorliegenden Absatzes aufgeführten Informationen umfassen gegebenenfalls Informationen über** kurz-, mittel- und langfristige Zeiträume.

■

- (3) **Gegebenenfalls** umfassen die in den Absätzen 1 und 2 genannten Informationen Angaben **zur eigenen Geschäftstätigkeit** des Unternehmens **und zu seiner Wertschöpfungskette**, einschließlich Angaben zu **■** seinen Produkten und Dienstleistungen, seinen Geschäftsbeziehungen und seiner Lieferkette.

*Für die ersten drei Jahre der Anwendung der von den Mitgliedstaaten gemäß Artikel 5 Absatz 2 der Richtlinie (EU) .../...⁺ des Europäischen Parlaments und des Rates** angenommenen Maßnahmen und für den Fall, dass nicht alle erforderlichen Informationen über seine Wertschöpfungskette verfügbar sind, erläutert das Unternehmen, welche Anstrengungen unternommen wurden, um die erforderlichen Informationen über seine Wertschöpfungskette zu erhalten, begründet das Unternehmen, warum nicht alle erforderlichen Informationen eingeholt werden konnten, und erläutert das Unternehmen seine Pläne, um künftig die erforderlichen Informationen einzuholen.*

Gegebenenfalls umfassen die in den Absätzen 1 und 2 genannten Angaben auch Verweise auf andere gemäß Artikel 19 in den Lagebericht aufgenommene Angaben und zusätzliche Erläuterungen dazu sowie auf die im Jahresabschluss ausgewiesenen Beträge.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in PE 35/22 (2021/0104(COD)) und in die Fußnote die Nummer, das Datum und die Amtsblattfundstelle jener Richtlinie einfügen.

Die Mitgliedstaaten können gestatten, dass Informationen über künftige Entwicklungen oder Belange, über die Verhandlungen geführt werden, in Ausnahmefällen weggelassen werden, wenn eine solche Angabe nach der ordnungsgemäß begründeten Einschätzung der Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane, die im Rahmen der ihnen durch einzelstaatliche Rechtsvorschriften übertragenen Zuständigkeiten handeln und gemeinsam für diese Einschätzung zuständig sind, der Geschäftslage des Unternehmens ernsthaft schaden würde, sofern eine solche Nichtaufnahme ein den tatsächlichen Verhältnissen entsprechendes und ausgewogenes Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses und der Lage des Unternehmens, sowie der Auswirkungen seiner Tätigkeit nicht verhindert.

- (4) Die Unternehmen erstatten Bericht über die in den Absätzen 1 bis 3 des vorliegenden Artikels genannten Informationen gemäß den im Einklang mit Artikel **29b** angenommenen Standards für die Nachhaltigkeitsberichterstattung.
- (5) ***Die Unternehmensleitung unterrichtet die Arbeitnehmervertreter auf geeigneter Ebene und erörtert mit ihnen die einschlägigen Informationen und die Mittel zur Einholung und Überprüfung von Nachhaltigkeitsinformationen. Die Stellungnahme der Arbeitnehmervertreter wird gegebenenfalls den zuständigen Verwaltungs-, Leitungs- oder Aufsichtsorganen mitgeteilt.***

- (6) Abweichend von den Absätzen 2 bis 4 **und unbeschadet der Absätze 9 und 10** können kleine und mittlere Unternehmen nach **Absatz 1, kleine und nicht komplexe Institute im Sinne von Artikel 4 Absatz 1 Nummer 145 der Verordnung (EU) Nr. 575/2013, firmeneigene Versicherungsunternehmen im Sinne von Artikel 13 Nummer 2 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates*** und firmeneigene Rückversicherungsunternehmen im Sinne von Artikel 13 Nummer 5 der genannten Richtlinie ihre Nachhaltigkeitsberichterstattung auf folgende Informationen beschränken:**
- a) **eine kurze Beschreibung von Geschäftsmodell und Strategie des Unternehmens;**
 - b) **eine Beschreibung der Unternehmenspolitik hinsichtlich Nachhaltigkeit;**
 - c) **die wichtigsten tatsächlichen oder potenziellen negativen Auswirkungen des Unternehmens in Bezug auf Nachhaltigkeitsaspekte sowie jegliche Maßnahmen zur Ermittlung, Überwachung, Verhinderung, Minderung oder Behebung solcher tatsächlichen oder potenziellen negativen Auswirkungen;**
 - d) **die wichtigsten Risiken, denen das Unternehmen im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt ist, und die Handhabung dieser Risiken durch das Unternehmen;**
 - e) **Schlüsselindikatoren, die für die unter den Buchstaben a bis d genannten Offenlegungen erforderlich sind.**

Kleine und mittlere Unternehmen, kleine und nicht komplexe Institute sowie firmeneigene Versicherungs- und Rückversicherungsunternehmen, die von der Ausnahmeregelung gemäß Unterabsatz 1 Gebrauch machen, erstatten gemäß den Standards für die Nachhaltigkeitsberichterstattung durch kleine und mittlere Unternehmen nach Artikel 29c Bericht.

- (7) *Für Geschäftsjahre, die vor dem 1. Januar 2028 beginnen, können kleine und mittlere Unternehmen, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a handelt, abweichend von Absatz 1 des vorliegenden Artikels beschließen, die in Absatz 1 genannten Informationen nicht in ihren Lagebericht aufzunehmen. In solchen Fällen gibt das Unternehmen jedoch in seinem Lagebericht kurz an, warum die Nachhaltigkeitsberichterstattung nicht vorgelegt wurde.*
- (8) Bei Unternehmen, die die Anforderungen der Absätze 1 bis 4 des vorliegenden Artikels erfüllen, **und Unternehmen, die von der Ausnahmeregelung nach Absatz 6** des vorliegenden Artikels **Gebrauch machen**, wird davon ausgegangen, dass sie die Anforderung von Artikel 19 Absatz 1 Unterabsatz 3 erfüllen.

- (9) Sofern die in Unterabsatz 2 des vorliegenden Absatzes festgelegten Bedingungen erfüllt sind, wird ein Unternehmen, das ein Tochterunternehmen ist, von den in den Absätzen 1 bis 4 des vorliegenden Artikels festgelegten Pflichten befreit (*im Folgenden „befreites Tochterunternehmen“*), wenn dieses Unternehmen und seine Tochterunternehmen in den konsolidierten Lagebericht eines Mutterunternehmens einbezogen werden und dieser konsolidierte Lagebericht gemäß Artikel 29 und Artikel 29a erstellt wird. Ein Unternehmen, das Tochterunternehmen eines in einem Drittland niedergelassenen Mutterunternehmens ist, wird ebenfalls von den in den Absätzen 1 bis 4 des vorliegenden Artikels festgelegten Pflichten befreit, wenn dieses Unternehmen und seine Tochterunternehmen in **die konsolidierte Nachhaltigkeitsberichterstattung** dieses in einem Drittland niedergelassenen Mutterunternehmens einbezogen werden und **diese konsolidierte Nachhaltigkeitsberichterstattung gemäß den nach Artikel 29b erlassenen Standards für die Nachhaltigkeitsberichterstattung oder** in einer Weise durchgeführt wird, die diesen **Standards für die Nachhaltigkeitsberichterstattung gleichwertig ist, was in einem** gemäß Artikel 23 Absatz 4 **Unterabsatz 3** der Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates**** erlassenen **Durchführungsrechtsakt über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung festgestellt wurde.**

Die Befreiung nach Unterabsatz 1 ist an folgende Bedingungen geknüpft:

- a) Der Lagebericht des befreiten Tochterunternehmens enthält alle folgenden Informationen:***
 - i) Namen und Sitz des Mutterunternehmens, das über Informationen auf Gruppenebene gemäß dem vorliegenden Artikel oder in einer Weise Bericht erstattet, die den nach Artikel 29b der vorliegenden Richtlinie erlassenen Standards für die Nachhaltigkeitsberichterstattung gleichwertig ist, was in einem gemäß Artikel 23 Absatz 4 Unterabsatz 3 der Richtlinie 2004/109/EG erlassenen Durchführungsrechtsakt über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung festgestellt wurde;***
 - ii) die Weblinks zum konsolidierten Lagebericht des Mutterunternehmens oder gegebenenfalls zu der konsolidierten Nachhaltigkeitsberichterstattung des Mutterunternehmens nach Unterabsatz 1 des vorliegenden Absatzes und zu dem Bestätigungsurteil nach Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa der vorliegenden Richtlinie oder zum Bestätigungsurteil nach Buchstabe b dieses Unterabsatzes;***
 - iii) die Information, dass das Unternehmen von den in den Absätzen 1 bis 4 dieses Artikels genannten Pflichten befreit ist;***

- b) *ist das Mutterunternehmen in einem Drittland niedergelassen, so werden seine konsolidierte Nachhaltigkeitsberichterstattung und das Bestätigungsurteil zu der konsolidierten Nachhaltigkeitsberichterstattung, das von einer oder mehreren Personen oder Gesellschaften abgegeben wurde, die nach dem für dieses Mutterunternehmen geltenden Recht zur Abgabe eines Urteils über die Bestätigung der Nachhaltigkeitsberichterstattung befugt sind, gemäß Artikel 30 der vorliegenden Richtlinie und im Einklang mit dem Recht des Mitgliedstaats, dem das befreite Tochterunternehmen unterliegt, veröffentlicht;*
- c) *ist das Mutterunternehmen in einem Drittland niedergelassen, so werden die in Artikel 8 der Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates***** festgelegten Offenlegungen über die Tätigkeiten des in der Union niedergelassenen befreiten Tochterunternehmens und seiner Tochterunternehmen in den Lagebericht des befreiten Tochterunternehmens oder in der konsolidierten Nachhaltigkeitsberichterstattung des in einem Drittland niedergelassenen Mutterunternehmens aufgenommen.*

Der Mitgliedstaat, dessen einzelstaatlichem Recht das befreite Tochterunternehmen unterliegt, kann verlangen, dass der konsolidierte Lagebericht des Mutterunternehmens oder gegebenenfalls der konsolidierte Nachhaltigkeitsbericht des Mutterunternehmens in einer von diesem Mitgliedstaat akzeptierten Sprache offengelegt wird und dass alle erforderlichen Übersetzungen in diese Sprache bereitgestellt werden. Jede Übersetzung, die nicht beglaubigt wurde, muss eine entsprechende Erklärung enthalten.

Unternehmen, die gemäß Artikel 37 von der Erstellung eines Lageberichts befreit sind, brauchen die in Unterabsatz 2 Buchstabe a Ziffern i bis iii dieses Absatzes genannten Informationen nicht vorzulegen, sofern diese Unternehmen den konsolidierten Lagebericht gemäß Artikel 37 offenlegen.

Für die Zwecke von Unterabsatz 1 dieses Absatzes und in Fällen, in denen Artikel 10 der Verordnung (EU) Nr. 575/2013 Anwendung findet, werden Kreditinstitute nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe b dieser Richtlinie, die einer Zentralorganisation ständig zugeordnet sind, welche sie unter den in Artikel 10 der Verordnung (EU) Nr. 575/2013 festgelegten Bedingungen beaufsichtigt, wie Tochterunternehmen dieser Zentralorganisation behandelt.

Für die Zwecke von Unterabsatz 1 werden Versicherungsunternehmen nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe a der vorliegenden Richtlinie, die auf der Grundlage einer in Artikel 212 Absatz 1 Buchstabe c Ziffer ii der Richtlinie 2009/138/EG genannten finanziellen Beziehung einer Gruppe angehören und gemäß Artikel 213 Absatz 2 Buchstaben a bis c der genannten Richtlinie der Gruppenaufsicht unterliegen, wie Tochterunternehmen des Mutterunternehmens der Gruppe behandelt.

■

- (10) *Die Befreiung nach Absatz 9 gilt auch für Unternehmen von öffentlichem Interesse, die den Anforderungen dieses Artikels unterliegen, mit Ausnahme großer Unternehmen, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a dieser Richtlinie handelt.*

* *Verordnung (EU) 2021/1119 des Europäischen Parlaments und des Rates vom 30. Juni 2021 zur Schaffung des Rahmens für die Verwirklichung der Klimaneutralität und zur Änderung der Verordnungen (EG) Nr. 401/2009 und (EU) 2018/1999 („Europäisches Klimagesetz“) (ABl. L 243 vom 9.7.2021, S. 1).*

** *Richtlinie (EU) .../... des Europäischen Parlaments und des Rates vom ... zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG , 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen (ABl. ...).*

*** *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).***** *Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates vom 15. Dezember 2004 zur Harmonisierung der Transparenzanforderungen in Bezug auf Informationen über Emittenten, deren Wertpapiere zum Handel auf einem geregelten Markt zugelassen sind, und zur Änderung der Richtlinie 2001/34/EG (ABl. L 390 vom 31.12.2004, S. 38).*

***** *Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088 (ABl. L 198 vom 22.6.2020, S. 13).“*

(5)

- (6) 5. Artikel 20 Absatz 1 wird wie folgt geändert:
- (a) a) Buchstabe g erhält folgende Fassung:
- „g) eine Beschreibung des Diversitätskonzepts, das im Zusammenhang mit den Verwaltungs-, Leitungs- und Aufsichtsorganen des Unternehmens in Bezug auf das Geschlecht sowie andere Aspekte wie beispielsweise Alter, Behinderungen oder Bildungs- und Berufshintergrund verfolgt wird, der Ziele dieses Diversitätskonzepts sowie der Art und Weise der Umsetzung dieses Konzepts und der Ergebnisse im Berichtszeitraum. Wird ein derartiges Konzept nicht angewendet, wird in der Erklärung erläutert, warum dies der Fall ist.“
- (b) b) Folgender Unterabsatz wird eingefügt:
- „Bei Unternehmen, die Artikel 19a unterliegen, wird davon ausgegangen, dass sie die Pflichten gemäß Unterabsatz 1 **Buchstabe** g erfüllen, wenn sie die nach diesem Buchstaben erforderlichen Angaben in ihre Nachhaltigkeitsberichterstattung aufnehmen **und in der Erklärung zur Unternehmensführung ein Verweis darauf aufgenommen wird.**“

- (7) 6. Artikel 23 wird wie folgt geändert:
- (a) a) Absatz 4 Buchstabe b erhält folgende Fassung:
„b) der konsolidierte Abschluss nach Buchstabe a und der konsolidierte Lagebericht des größeren Kreises von Unternehmen sind von dem Mutterunternehmen dieses Kreises von Unternehmen nach dem Recht des Mitgliedstaats, dem das Mutterunternehmen unterliegt, im Einklang mit dieser Richtlinie, ausgenommen den in Artikel 29a festgelegten Anforderungen, oder mit gemäß der Verordnung (EG) Nr. 1606/2002 übernommenen internationalen Rechnungslegungsstandards aufgestellt;“
- (b) b) Absatz 8 Buchstabe b Ziffer i erhält folgende Fassung:
„i) im Einklang mit dieser Richtlinie, ausgenommen den Anforderungen des Artikels 29a,“
- (c) c) Absatz 8 Buchstabe b Ziffer iii erhält folgende Fassung:
„iii) derart, dass sie einem nach dieser Richtlinie erstellten konsolidierten Abschluss und konsolidierten Lagebericht gleichwertig sind, ausgenommen den Anforderungen des Artikels 29a, oder“.

(8) 7. Artikel 29a erhält folgende Fassung:

„Artikel 29a

Konsolidierte Nachhaltigkeitsberichterstattung

- (1) Mutterunternehmen einer großen Gruppe **nach Artikel 3 Absatz 7** nehmen in den konsolidierten Lagebericht Angaben auf, die für das Verständnis der Auswirkungen der Gruppe auf Nachhaltigkeitsaspekte sowie das Verständnis der Auswirkungen von Nachhaltigkeitsaspekten auf Geschäftsverlauf, Geschäftsergebnis und Lage der Gruppe erforderlich sind.

Die in Unterabsatz 1 genannten Angaben müssen im konsolidierten Lagebericht mittels eines dafür vorgesehenen Abschnitts erkennbar ausgewiesen sein.

- (2) Die in Absatz 1 genannten Informationen umfassen ■ Folgendes:

- a) eine kurze Beschreibung von Geschäftsmodell und Strategie der Gruppe, einschließlich Angaben
- i) zur Widerstandsfähigkeit von Geschäftsmodell und Strategie der Gruppe gegenüber Risiken im Zusammenhang mit Nachhaltigkeitsaspekten;
- ii) zu den Chancen der Gruppe im Zusammenhang mit Nachhaltigkeitsaspekten;
- iii) zu der Art und Weise, ***einschließlich Durchführungsmaßnahmen und zugehörigen Finanz- und Investitionsplänen***, wie die Gruppe beabsichtigt sicherzustellen, dass ihr Geschäftsmodell und ihre Strategie mit dem Übergang zu einer nachhaltigen Wirtschaft und der Begrenzung der Erderwärmung auf 1,5 °C im Einklang mit dem Übereinkommen von Paris ***und dem in der Verordnung (EU) 2021/1119 verankerten Ziel der Verwirklichung der Klimaneutralität bis 2050*** vereinbar sind, ***und gegebenenfalls die Exposition des Unternehmens gegenüber Aktivitäten mit Bezug zu Kohle, Öl und Gas***;

- iv) zu der Art und Weise, wie die Gruppe in ihrem Geschäftsmodell und ihrer Strategie den Belangen ihrer Interessenträger und den nachhaltigkeitsrelevanten Auswirkungen ihrer Tätigkeiten Rechnung trägt;
- v) zu der Art und Weise, wie die Strategie der Gruppe mit Blick auf Nachhaltigkeitsaspekte umgesetzt wird;
- b) eine Beschreibung der **zeitgebundenen** Nachhaltigkeitsziele, die sich die Gruppe gesetzt hat, ***gegebenenfalls einschließlich der absoluten Ziele für die Verringerung der Treibhausgasemissionen mindestens für 2030 und 2050, eine Beschreibung der Fortschritte, die die Gruppe im Hinblick auf die Erreichung dieser Ziele erzielt hat, und eine Erklärung, ob die auf Umweltfaktoren bezogenen Ziele der Gruppe auf schlüssigen wissenschaftlichen Beweisen beruhen;***
- c) eine Beschreibung der Rolle der Verwaltungs-, Leitungs- und Aufsichtsorgane im Zusammenhang mit Nachhaltigkeitsaspekten ***sowie ihres Fachwissens und ihrer Fähigkeiten zur Wahrnehmung dieser Rolle oder ihres Zugangs zu solchem Fachwissen und solchen Fähigkeiten;***
- d) eine Beschreibung der Unternehmenspolitik der Gruppe hinsichtlich Nachhaltigkeit;

- e) **Angaben über das Vorhandensein von mit Nachhaltigkeitsaspekten verknüpften Anreizsystemen, die Mitgliedern der Verwaltungs-, Leitungs- und Aufsichtsorgane angeboten werden;**
- f) eine Beschreibung
 - i) des **von der Gruppe** mit Blick auf Nachhaltigkeitsaspekte **und gegebenenfalls im Einklang mit den Anforderungen der Union für Unternehmen zur Durchführung eines Due-Diligence-Prozesses** angewandten Due-Diligence-Prozesses;
 - ii) der wichtigsten tatsächlichen oder potenziellen negativen Auswirkungen, die mit der **eigenen Geschäftstätigkeit der Gruppe und mit ihrer** Wertschöpfungskette ■ , einschließlich ■ ihrer Produkte und Dienstleistungen, ihrer Geschäftsbeziehungen und ihrer Lieferkette, verknüpft sind, **der Maßnahmen zur Ermittlung und Überwachung dieser Auswirkungen, und anderer negativer Auswirkungen, die das Unternehmen gemäß anderen Anforderungen der Union zur Durchführung eines Due-Diligence-Prozesses ermitteln muss;**
 - iii) jeglicher Maßnahmen **der Gruppe** zur Verhinderung, Minderung, **Behebung oder Beendigung** tatsächlicher oder potenzieller negativer Auswirkungen und des Ergebnisses dieser Maßnahmen;

- g) eine Beschreibung der wichtigsten Risiken, denen die Gruppe im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt ist, einschließlich der wichtigsten Abhängigkeiten in diesem Bereich, und der Art und Weise, wie die Gruppe solche Risiken steuert;
- h) Indikatoren, die für die unter den Buchstaben a bis g genannten Offenlegungen relevant sind.

■

Die Mutterunternehmen **teilen** das Verfahren zur Ermittlung der im Einklang mit **Absatz 1 dieses Artikels** in den konsolidierten Lagebericht eingeflossenen Informationen **mit. Die in Unterabsatz 1 dieses Absatzes aufgeführten Informationen umfassen gegebenenfalls Informationen über kurz-, mittel- und langfristige Zeiträume.**

■

- (3) **Gegebenenfalls umfassen** die in den Absätzen 1 und 2 genannten Informationen ■ Angaben **zur eigenen Geschäftstätigkeit** der Gruppe **und zu ihrer Wertschöpfungskette**, einschließlich Angaben zu ■ ihren Produkten und Dienstleistungen, ihren Geschäftsbeziehungen und ihrer Lieferkette.

Für die ersten drei Jahre der Anwendung der von den Mitgliedstaaten gemäß Artikel 5 Absatz 2 der Richtlinie (EU) .../...⁺ angenommenen Maßnahmen und für den Fall, dass nicht alle erforderlichen Informationen über seine Wertschöpfungskette verfügbar sind, erläutert das Mutterunternehmen, welche Anstrengungen unternommen wurden, um die erforderlichen Informationen über seine Wertschöpfungskette zu erhalten, begründet das Mutterunternehmen, warum nicht alle erforderlichen Informationen eingeholt werden konnten, und erläutert das Mutterunternehmen seine Pläne, um künftig alle erforderlichen Informationen einzuholen.

⁺ ABl.: Bitte die Nummer der Richtlinie in Dokument PE 35/22 (2021/0104(COD)) in den Text einfügen.

Gegebenenfalls umfassen die in den Absätzen 1 und 2 genannten Informationen auch Verweise auf andere gemäß Artikel 29 in den konsolidierten Lagebericht aufgenommene Informationen und zusätzliche Erläuterungen dazu sowie auf die im konsolidierten Abschluss ausgewiesenen Beträge.

Die Mitgliedstaaten können gestatten, dass Informationen über künftige Entwicklungen oder Belange, über die Verhandlungen geführt werden, in Ausnahmefällen weggelassen werden, wenn nach der ordnungsgemäß begründeten Einschätzung der Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane, die im Rahmen der ihnen durch einzelstaatliche Rechtsvorschriften übertragenen Zuständigkeiten handeln und die gemeinsam für diese Einschätzung zuständig sind, eine solche Offenlegung von Informationen der Geschäftslage der Gruppe ernsthaft schaden würde, sofern eine solche Nichtaufnahme ein den tatsächlichen Verhältnissen entsprechendes und ausgewogenes Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses und der Lage der Gruppe sowie der Auswirkungen ihrer Tätigkeit nicht verhindert.

- (4) *Stellt das Bericht erstattende Unternehmen erhebliche Unterschiede zwischen den Risiken für die Gruppe oder Auswirkungen der Gruppe und den Risiken für ein oder mehrere Tochterunternehmen oder Auswirkungen eines oder mehrerer Tochterunternehmen fest, so muss es gegebenenfalls ein hinreichendes Verständnis der Risiken für das betreffende bzw. die betreffenden Tochterunternehmen und Auswirkungen des betreffenden Tochterunternehmens bzw. der betreffenden Tochterunternehmen vermitteln.***

Die Unternehmen geben an, welche in die Konsolidierung einbezogenen Tochterunternehmen von der jährlichen oder konsolidierten Nachhaltigkeitsberichterstattung gemäß Artikel 19a Absatz 9 bzw. Artikel 29a Absatz 8 befreit sind.

- (5) Die Mutterunternehmen erstatten Bericht über die in den Absätzen 1 bis 3 dieses Artikels genannten Informationen gemäß den im Einklang mit Artikel **29b** angenommenen Standards für die Nachhaltigkeitsberichterstattung.

(6) *Die Unternehmensleitung des Mutterunternehmens unterrichtet die Arbeitnehmervertreter auf geeigneter Ebene und erörtert mit ihnen die einschlägigen Informationen und die Mittel zur Einholung und Überprüfung von Nachhaltigkeitsinformationen. Die Stellungnahme der Arbeitnehmervertreter wird gegebenenfalls den zuständigen Verwaltungs-, Leitungs- oder Aufsichtsorganen mitgeteilt.*

- (7) Wenn ein Mutterunternehmen die Anforderungen nach den Absätzen 1 bis 5 des vorliegenden Artikels erfüllt, wird davon ausgegangen, dass es die Anforderungen nach Artikel 19 Absatz 1 Unterabsatz 3 **und** Artikel 19a erfüllt.

- (8) ***Sofern die in Unterabsatz 2 des vorliegenden Absatzes festgelegten Bedingungen erfüllt sind, wird*** ein Mutterunternehmen, das auch ein Tochterunternehmen ist, von den in den Absätzen 1 bis 5 des vorliegenden Artikels festgelegten Pflichten befreit (***im Folgenden „befreites Mutterunternehmen“***), wenn dieses Mutterunternehmen und seine Tochterunternehmen in den konsolidierten Lagebericht eines anderen Unternehmens einbezogen werden und dieser konsolidierte Lagebericht gemäß Artikel 29 und dem vorliegenden Artikel erstellt wird. Ein Mutterunternehmen, das Tochterunternehmen eines in einem Drittland niedergelassenen Mutterunternehmens ist, wird ebenfalls von den in den Absätzen 1 bis 5 des vorliegenden Artikels festgelegten Pflichten befreit, wenn dieses Mutterunternehmen und seine Tochterunternehmen in ***die konsolidierte Nachhaltigkeitsberichterstattung*** dieses in einem Drittland niedergelassenen Mutterunternehmens einbezogen werden und ***diese konsolidierte Nachhaltigkeitsberichterstattung gemäß den nach Artikel 29b erlassenen Standards für die Nachhaltigkeitsberichterstattung oder*** in einer Weise durchgeführt wird, die diesen ***Standards für die Nachhaltigkeitsberichterstattung*** gleichwertig ist, was in einem gemäß Artikel 23 Absatz 4 ***Unterabsatz 3*** der Richtlinie 2004/109/EG erlassenen Durchführungsrechtsakt ***über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung*** festgestellt wurde.

Die Befreiung nach Unterabsatz 1 ist an folgende Bedingungen geknüpft:

- a) Der Lagebericht des befreiten Mutterunternehmens enthält alle folgenden Informationen:***
 - i) Namen und Sitz des Mutterunternehmens, das über Informationen auf Gruppenebene gemäß dem vorliegenden Artikel oder in einer Weise Bericht erstattet, die den nach Artikel 29b der vorliegenden Richtlinie erlassenen Standards für die Nachhaltigkeitsberichterstattung gleichwertig ist, was in einem gemäß Artikel 23 Absatz 4 Unterabsatz 3 der Richtlinie 2004/109/EG erlassenen Durchführungsrechtsakt über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung festgestellt wurde;***
 - ii) die Weblinks zum konsolidierten Lagebericht des Mutterunternehmens oder gegebenenfalls zu der konsolidierten Nachhaltigkeitsberichterstattung des Mutterunternehmens nach Unterabsatz 1 des vorliegenden Absatzes und zu dem Bestätigungsurteil nach Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa der vorliegenden Richtlinie oder zum Bestätigungsurteil nach Buchstabe b dieses Unterabsatzes;***
 - iii) einen Hinweis auf die Befreiung des Unternehmens von den in den Absätzen 1 bis 5 dieses Artikels genannten Pflichten.***

- b) *Ist das Mutterunternehmen in einem Drittland niedergelassen, so werden seine konsolidierten Nachhaltigkeitsberichterstattung und das Bestätigungsurteil, das von einer oder mehreren Personen oder Gesellschaften abgegeben wurde, die nach dem für das Mutterunternehmen geltenden einzelstaatlichen Recht zur Abgabe eines Urteils über die Bestätigung der Nachhaltigkeitsberichterstattung befugt sind, gemäß Artikel 30 und im Einklang mit dem Recht des Mitgliedstaats, dem das befreite Mutterunternehmen unterliegt, veröffentlicht.*
- c) *Ist das Mutterunternehmen in einem Drittland niedergelassen, werden die in Artikel 8 der Verordnung (EU) 2020/852 festgelegten Angaben über die Tätigkeiten des in der Union niedergelassenen Tochterunternehmens, das gemäß Artikel 19a Absatz 9 der vorliegenden Richtlinie von der Nachhaltigkeitsberichterstattung ausgenommen ist, in den Lagebericht des befreiten Mutterunternehmens oder in die von dem in einem Drittland niedergelassenen Mutterunternehmen durchgeführte konsolidierte Nachhaltigkeitsberichterstattung, aufgenommen.*

Der Mitgliedstaat, dessen einzelstaatlichem Recht das befreite Mutterunternehmen unterliegt, kann verlangen, dass der konsolidierte Lagebericht des Mutterunternehmens oder gegebenenfalls der konsolidierte Nachhaltigkeitsbericht des Mutterunternehmens in einer von diesem Mitgliedstaat akzeptierten Sprache offengelegt wird und dass alle erforderlichen Übersetzungen in diese Sprache bereitgestellt werden. Jede Übersetzung, die nicht beglaubigt wurde, muss eine entsprechende Erklärung enthalten.

Mutterunternehmen, die gemäß Artikel 37 von der Erstellung eines Lageberichts befreit sind, brauchen die in Unterabsatz 2 Buchstabe a Ziffern i bis iii dieses Absatzes genannten Informationen nicht vorzulegen, sofern diese Unternehmen den konsolidierten Lagebericht gemäß Artikel 37 offenlegen.

Für die Zwecke von Unterabsatz 1 und in Fällen, in denen Artikel 10 der Verordnung (EU) Nr. 575/2013 Anwendung findet, werden Kreditinstitute nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe b dieser Richtlinie, die einer Zentralorganisation ständig zugeordnet sind, welche sie unter den in Artikel 10 der Verordnung (EU) Nr. 575/2013 festgelegten Bedingungen beaufsichtigt, wie Tochterunternehmen dieser Zentralorganisation behandelt.

Für die Zwecke von Unterabsatz 1 werden Versicherungsunternehmen nach Artikel 1 Absatz 3 Unterabsatz 1 Buchstabe a der vorliegenden Richtlinie, die auf der Grundlage einer in Artikel 212 Absatz 1 Buchstabe c Ziffer ii der Richtlinie 2009/138/EG genannten finanziellen Beziehungen einer Gruppe angehören und gemäß Artikel 213 Absatz 2 Buchstaben a bis c der genannten Richtlinie der Gruppenaufsicht unterliegen, wie Tochterunternehmen des Mutterunternehmens der Gruppe behandelt.

■

- (9) (9) *Die Befreiung nach Absatz 8 gilt auch für Unternehmen von öffentlichem Interesse, die den Anforderungen dieses Artikels unterliegen, mit Ausnahme großer Unternehmen, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a dieser Richtlinie handelt.“*

(10) 8. *Folgendes Kapitel wird eingefügt:*

„KAPITEL

6a

STANDARDS FÜR DIE NACHHALTIGKEITSBERICHTERSTATTUNG

Artikel 29b

Standards für die Nachhaltigkeitsberichterstattung

(1) Die Kommission erlässt delegierte Rechtsakte nach Artikel 49 zur Ergänzung dieser Richtlinie, um Standards für die Nachhaltigkeitsberichterstattung festzulegen. In diesen Standards für die Nachhaltigkeitsberichterstattung wird festgelegt, über welche Informationen Unternehmen im Einklang mit den Artikeln 19a und 29a Bericht erstatten müssen, und gegebenenfalls, in welcher Struktur diese Informationen vorzulegen sind.

In den in Unterabsatz 1 des vorliegenden Absatzes genannten delegierten Rechtsakten legt die Kommission bis zum 30. Juni 2023 fest, über welche Informationen Unternehmen im Einklang mit Artikel 19a Absätze 1 und 2 und gegebenenfalls Artikel 29a Absätze 1 und 2 Bericht erstatten müssen, was zumindest die Informationen umfasst, die Finanzmarktteilnehmer, die den Offenlegungspflichten der Verordnung (EU) 2019/2088 unterliegen, benötigen, um diesen Verpflichtungen nachzukommen.

In den in Unterabsatz 1 genannten delegierten Rechtsakten legt die Kommission bis zum 30. Juni 2024 Folgendes fest:

- i) ergänzende Informationen, über die Unternehmen in Bezug auf Nachhaltigkeitsaspekte und die unter Artikel 19a Absatz 2 aufgeführten Bereiche der Berichterstattung erforderlichenfalls Bericht zu erstatten haben;*
- ii) Informationen, über die Unternehmen Bericht zu stellen haben, die für den Sektor, in dem sie tätig sind, spezifisch sind.*

Die Berichterstattungsanforderungen, die in den in Unterabsatz 1 genannten delegierten Rechtsakten festgelegt sind, treten frühestens vier Monate nach ihrem Erlass durch die Kommission in Kraft.

Beim Erlass delegierter Rechtsakte zur Festlegung der nach Unterabsatz 3 Ziffer ii erforderlichen Informationen achtet die Kommission besonders auf das Ausmaß der Risiken und Auswirkungen im Zusammenhang mit Nachhaltigkeitsaspekten für jeden Sektor, wobei sie der Tatsache Rechnung trägt, dass die Risiken und Auswirkungen für einige Sektoren höher sind als für andere.

Die Kommission überprüft mindestens alle drei Jahre nach deren Geltungsbeginn die gemäß diesem Artikel erlassenen delegierten Rechtsakte unter Berücksichtigung der fachlichen Stellungnahme der Europäischen Beratungsgruppe für Rechnungslegung (European Financial Reporting Advisory Group – EFRAG) und ändert diese delegierten Rechtsakte, falls dies nötig ist, um relevanten Entwicklungen, einschließlich Entwicklungen im Zusammenhang mit internationalen Standards, Rechnung zu tragen.

Die Kommission konsultiert mindestens einmal jährlich das Europäische Parlament und konsultiert die in Artikel 24 der Verordnung (EU) 2020/852 genannte Sachverständigengruppe der Mitgliedstaaten für nachhaltiges Finanzwesen und den in Artikel 6 der Verordnung (EG) Nr. 1606/2002 genannten Regelungsausschuss für Rechnungslegung gemeinsam zum Arbeitsprogramm der EFRAG im Hinblick auf die Entwicklung von Standards für die Nachhaltigkeitsberichterstattung.

- (2) Durch die Standards für die Nachhaltigkeitsberichterstattung wird die Qualität der Informationen sichergestellt, über die Bericht erstattet wird, indem darin vorgeschrieben wird, dass die Informationen verständlich, relevant, überprüfbar und vergleichbar sein und in wahrheitsgetreuer Weise dargestellt werden müssen. Die Standards für die Nachhaltigkeitsberichterstattung müssen einen unverhältnismäßigen Verwaltungsaufwand für Unternehmen vermeiden, unter anderem dadurch, dass die Arbeit globaler Standardsetzungsinitiativen für die Nachhaltigkeitsberichterstattung gemäß Absatz 5 Buchstabe a im größtmöglichen Umfang berücksichtigt wird.*

In den Standards für die Nachhaltigkeitsberichterstattung werden unter Berücksichtigung des jeweiligen Gegenstands des Standards für die Nachhaltigkeitsberichterstattung

- a) die Informationen präzisiert, die Unternehmen zu folgenden Umweltfaktoren offenlegen müssen:*

- i) *Klimaschutz, auch in Bezug auf Scope-1-, Scope-2- und gegebenenfalls Scope-3-Treibhausgasemissionen;*
 - ii) *Anpassung an den Klimawandel;*
 - iii) *Wasser- und Meeresressourcen;*
 - iv) *Ressourcennutzung und die Kreislaufwirtschaft;*
 - v) *Verschmutzung;*
 - vi) *Biodiversität und Ökosysteme;*
- b) *die Informationen präzisiert, die Unternehmen zu folgenden Sozial- und Menschenrechtsfaktoren offenlegen müssen:*
 - i) *Gleichbehandlung und Chancengleichheit für alle, einschließlich Geschlechtergerechtigkeit und gleichem Lohn bei gleichwertiger Arbeit, Ausbildung und Kompetenzentwicklung, Beschäftigung und Inklusion von Menschen mit Behinderungen, Maßnahmen gegen Gewalt und Belästigung am Arbeitsplatz sowie Vielfalt;*

- ii) *Arbeitsbedingungen, einschließlich sicherer Beschäftigung, Arbeitszeit, angemessene Löhne, sozialer Dialog, Vereinigungsfreiheit, Existenz von Betriebsräten, Tarifverhandlungen, einschließlich des Anteils der Arbeitnehmer, für die Tarifverträge gelten, Informations-, Anhörungs- und Mitbestimmungsrechte der Arbeitnehmer, Vereinbarkeit von Beruf und Privatleben sowie Gesundheit und Sicherheit;*
- iii) *Achtung der Menschenrechte, Grundfreiheiten, demokratischen Grundsätze und Standards, die in der Internationalen Charta der Menschenrechte und anderen grundlegenden Menschenrechtsübereinkommen der Vereinten Nationen, einschließlich des Übereinkommens der Vereinten Nationen über die Rechte von Menschen mit Behinderungen und der Erklärung der Vereinten Nationen über die Rechte der indigenen Völker, sowie in der Erklärung der Internationalen Arbeitsorganisation über grundlegende Prinzipien und Rechte bei der Arbeit und den grundlegenden Übereinkommen der IAO, der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, der europäischen Sozialcharta und der Charta der Grundrechte der Europäischen Union festgelegt sind;*
- c) *die Informationen präzisiert, die Unternehmen zu folgenden Governance-Faktoren offenlegen müssen:*

- i) *die Rolle der Verwaltungs-, Leitungs- und Aufsichtsorgane des Unternehmens im Zusammenhang mit Nachhaltigkeitsaspekten und ihre Zusammensetzung sowie ihr Fachwissen und ihre Fähigkeiten zur Wahrnehmung dieser Rolle oder ihr Zugang zu solchem Fachwissen und solchen Fähigkeiten;*
- ii) *die Hauptmerkmale der internen Kontroll- und Risikomanagementsysteme des Unternehmens in Bezug auf den Prozess der Nachhaltigkeitsberichterstattung und der Beschlussfassung;*
- iii) *Unternehmensethik und Unternehmenskultur, einschließlich der Bekämpfung von Korruption und Bestechung, des Schutzes von Hinweisgebern und des Tierwohls;*
- iv) *Tätigkeiten und Verpflichtungen des Unternehmens im Zusammenhang mit der Ausübung seines politischen Einflusses, einschließlich seiner Lobbytätigkeiten;*
- v) *die Pflege und die Qualität der Beziehungen zu Kunden, Lieferanten und Gemeinschaften, die von den Tätigkeiten des Unternehmens betroffen sind, einschließlich Zahlungspraktiken, insbesondere in Bezug auf verspätete Zahlungen an kleine und mittlere Unternehmen.*

- (3) *In den Standards für die Nachhaltigkeitsberichterstattung werden die zukunfts- und vergangenheitsbezogenen, qualitativen und quantitativen Informationen, über die die Unternehmen gegebenenfalls Bericht zu erstatten haben, spezifiziert.*

(4) *In den Standards für die Nachhaltigkeitsberichterstattung wird berücksichtigt, dass es für Unternehmen nicht immer problemlos möglich ist, Informationen bei Akteuren entlang ihrer gesamten Wertschöpfungskette einzuholen, insbesondere bei Akteuren, die nicht den Anforderungen an die Nachhaltigkeitsberichterstattung gemäß Artikel 19a oder 29a unterliegen, und bei Lieferanten aus Schwellenländern und aufstrebenden Märkten. In den Standards für die Nachhaltigkeitsberichterstattung werden Angaben zu Wertschöpfungsketten vorgegeben, die den Kapazitäten und Merkmalen von Unternehmen in Wertschöpfungsketten sowie dem Umfang und der Komplexität ihrer Tätigkeiten, insbesondere von Unternehmen, die nicht den Anforderungen an die Nachhaltigkeitsberichterstattung nach Artikel 19a oder 29a unterliegen, angemessen sind und entsprechen. In den Standards für die Nachhaltigkeitsberichterstattung werden keine Angaben festgelegt, die Unternehmen verpflichten würden, Informationen von kleinen und mittleren Unternehmen in ihrer Wertschöpfungskette einzuholen, die über die Informationen hinausgehen, die gemäß den Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen gemäß Artikel 29c anzugeben sind.*

Unterabsatz 1 gilt unbeschadet der Anforderungen der Union an Unternehmen, einen Due-Diligence-Prozess durchzuführen.

- (5) *Beim Erlass delegierter Rechtsakte gemäß Absatz 1 berücksichtigt die Kommission im größtmöglichen Umfang*
- a) *die Arbeit globaler Standardsetzungsinitiativen für die Nachhaltigkeitsberichterstattung und bestehende Standards und Rahmen für die Naturkapitalbilanzierung und die Bilanzierung von Treibhausgasen, verantwortungsvolles unternehmerisches Handeln, soziale Verantwortung der Unternehmen und nachhaltige Entwicklung;*
 - b) *die Informationen, die Finanzmarktteilnehmer benötigen, um ihren Offenlegungspflichten gemäß der Verordnung (EU) 2019/2088 und gemäß den nach der genannten Verordnung erlassenen delegierten Rechtsakten nachzukommen;*
 - c) *die Kriterien, Indikatoren und Methoden, die in den gemäß der Verordnung (EU) 2020/852 erlassenen delegierten Rechtsakten festgelegt sind, einschließlich der gemäß Artikel 10 Absatz 3, Artikel 11 Absatz 3, Artikel 12 Absatz 2, Artikel 13 Absatz 2, Artikel 14 Absatz 2 und Artikel 15 Absatz 2 der genannten Verordnung festgelegten technischen Bewertungskriterien und der Berichterstattungsanforderungen, die in dem gemäß Artikel 8 der genannten Verordnung erlassenen delegierten Rechtsakt festgelegt sind;*

- d) *die Offenlegungspflichten für Referenzwert-Administratoren in der Referenzwert-Erklärung und in der Referenzwert-Methodik sowie die Mindestanforderungen für die Konzipierung von EU-Referenzwerten für den klimabedingten Wandel und Paris-abgestimmten EU-Referenzwerten gemäß den Delegierten Verordnungen (EU) 2020/1816*, (EU) 2020/1817** und (EU) 2020/1818*** der Kommission;*
- e) *die Offenlegungen, die in den gemäß Artikel 434a der Verordnung (EU) Nr. 575/2013 erlassenen Durchführungsrechtsakten festgelegt sind;*

- f) die Empfehlung 2013/179/EU der Kommission****;
- g) die Richtlinie 2003/87/EG des Europäischen Parlaments und des Rates*****;
- h) die Verordnung (EU) 2021/1119;
- i) die Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates*****;
- j) die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates*****.

Artikel 29c

Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen

(1) Die Kommission erlässt bis zum 30. Juni 2024 delegierte Rechtsakte nach Artikel 49 zur Ergänzung dieser Richtlinie, um Standards für die Nachhaltigkeitsberichterstattung festzulegen, die den Kapazitäten und Merkmalen kleiner und mittlerer Unternehmen und dem Umfang und der Komplexität ihrer Tätigkeiten angemessen sind und entsprechen. In diesen Standards für die Nachhaltigkeitsberichterstattung ist für kleine und mittlere Unternehmen nach Artikel 2 Nummer 1 Buchstabe a spezifiziert, über welche Informationen gemäß Artikel 19a Absatz 6 Bericht zu erstatten ist.

Die Berichterstattungsanforderungen, die in den in Unterabsatz 1 genannten delegierten Rechtsakten festgelegt sind, treten frühestens vier Monate nach ihrem Erlass durch die Kommission in Kraft.

(2) Bei den Standards für die Nachhaltigkeitsberichterstattung für kleine und mittlere Unternehmen werden die in Artikel 29b Absätze 2 bis 5 festgelegten Kriterien berücksichtigt. Darüber hinaus wird soweit möglich die Struktur spezifiziert, in der diese Informationen vorzulegen sind.

(3) Die Kommission überprüft mindestens alle drei Jahre nach deren Geltungsbeginn die gemäß diesem Artikel erlassenen delegierten Rechtsakte unter Berücksichtigung der fachlichen Stellungnahme der EFRAG und ändert diese delegierten Rechtsakte, falls dies nötig ist, um relevanten Entwicklungen, einschließlich Entwicklungen im Zusammenhang mit internationalen Standards, Rechnung zu tragen.

-
- * *Delegierte Verordnung (EU) 2020/1816 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates hinsichtlich der Erläuterung in der Referenzwert-Erklärung, wie Umwelt-, Sozial- und Governance-Faktoren in den einzelnen Referenzwerten, die zur Verfügung gestellt und veröffentlicht werden, berücksichtigt werden (ABl. L 406 vom 3.12.2020, S. 1).*
- ** *Delegierte Verordnung (EU) 2020/1817 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates hinsichtlich des Mindestinhalts der Erläuterung, wie Umwelt-, Sozial- und Governance-Faktoren in der Referenzwert-Methodik berücksichtigt werden (ABl. L 406 vom 3.12.2020, S. 12).*
- *** *Delegierte Verordnung (EU) 2020/1818 der Kommission vom 17. Juli 2020 zur Ergänzung der Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates im Hinblick auf Mindeststandards für EU-Referenzwerte für den klimabedingten Wandel und für Paris-abgestimmte EU-Referenzwerte (ABl. L 406 vom 3.12.2020, S. 17).*
- **** *Empfehlung 2013/179/EU der Kommission vom 9. April 2013 für die Anwendung gemeinsamer Methoden zur Messung und Offenlegung der Umweltleistung von Produkten und Organisationen (ABl. L 124 vom 4.5.2013, S. 1).*

***** *Richtlinie 2003/87/EG des Europäischen Parlaments und des Rates vom 13. Oktober 2003 über ein System für den Handel mit Treibhausgasemissionszertifikaten in der Gemeinschaft und zur Änderung der Richtlinie 96/61/EG des Rates (ABl. L 275 vom 25.10.2003, S. 32).*

***** *Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates vom 25. November 2009 über die freiwillige Teilnahme von Organisationen an einem Gemeinschaftssystem für Umweltmanagement und Umweltbetriebsprüfung und zur Aufhebung der Verordnung (EG) Nr. 761/2001 sowie der Beschlüsse der Kommission 2001/681/EG und 2006/193/EG (ABl. L 342 vom 22.12.2009, S. 1).*

***** *Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. L 305 vom 26.11.2019, S. 17).“*

9. *Folgendes Kapitel wird eingefügt:*

„KAPITEL 6b

EINHEITLICHES ELEKTRONISCHES BERICHTSFORMAT

Artikel 29d

Einheitliches elektronisches Berichtsformat

- (1) Unternehmen, die den Anforderungen von Artikel 19a dieser Richtlinie unterliegen, stellen ihren Lagebericht im in Artikel 3 der Delegierten Verordnung (EU) 2019/815 der Kommission* dargelegten einheitlichen elektronischen Berichtsformat auf und zeichnen ihre Nachhaltigkeitsberichterstattung, einschließlich der Angaben nach Artikel 8 der Verordnung (EU) 2020/852, gemäß dem in jener Delegierten Verordnung dargelegten elektronischen Berichtsformat aus.***
- (2) Mutterunternehmen, die den Anforderungen von Artikel 29a unterliegen, stellen ihren konsolidierten Lagebericht im in Artikel 3 der Delegierten Verordnung (EU) 2019/815 dargelegten elektronischen Berichtsformat aus und zeichnen die Nachhaltigkeitsberichterstattung, einschließlich der Angaben nach Artikel 8 der Verordnung (EU) 2020/852, gemäß dem in jener Delegierten Verordnung dargelegten elektronischen Berichtsformat aus.***

**** Delegierte Verordnung (EU) 2019/815 der Kommission vom 17. Dezember 2018 zur Ergänzung der Richtlinie 2004/109/EG des Europäischen Parlaments und des Rates im Hinblick auf technische Regulierungsstandards für die Spezifikation eines einheitlichen elektronischen Berichtsformats (ABl. L 143 vom 29.5.2019, S. 1).“***

(11) 10. Artikel 30 Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten sorgen dafür, dass Unternehmen innerhalb einer angemessenen Frist, die zwölf Monate nach dem Bilanzstichtag nicht überschreiten darf, den ordnungsgemäß gebilligten Jahresabschluss und den Lagebericht gegebenenfalls in dem in Artikel 29d dieser Richtlinie genannten elektronischen Berichtsformat zusammen mit den Urteilen und der Erklärung des Abschlussprüfers oder der Prüfungsgesellschaft gemäß Artikel 34 dieser Richtlinie nach den Rechtsvorschriften der einzelnen Mitgliedstaaten im Einklang mit **Titel 1 Kapitel III** der Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates* offenlegen.

Die Mitgliedstaaten können von Unternehmen, die den Artikeln 19a und 29a unterliegen, verlangen, dass sie den Lagebericht der Öffentlichkeit auf ihrer Website kostenlos zur Verfügung stellen. Wenn ein Unternehmen keine Website betreibt, können die Mitgliedstaaten von ihm verlangen, dass es auf Anfrage eine schriftliche Kopie seines Lageberichts zur Verfügung stellt. ■

Wird das Urteil im Sinne von Artikel 34 Absatz 1 **Unterabsatz 2** Buchstabe aa von einem unabhängigen Erbringer von Bestätigungsleistungen abgegeben, ist dieses Urteil zusammen mit den in Unterabsatz 1 genannten **Dokumenten** offenzulegen.

Die Mitgliedstaaten können jedoch Unternehmen von der Pflicht zur Offenlegung eines Lageberichts befreien, wenn es möglich ist, eine vollständige oder teilweise Ausfertigung dieses Berichts einfach auf Antrag zu einem Entgelt zu erhalten, das die Verwaltungskosten nicht übersteigt.

Die Befreiung nach Unterabsatz 4 findet keine Anwendung auf Unternehmen, die den Anforderungen an die Nachhaltigkeitsberichterstattung nach den Artikeln 19a und 29a unterliegen.

* Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über bestimmte Aspekte des Gesellschaftsrechts (ABl. L 169 vom 30.6.2017, S. 46).“

- (a) ■
- (12) 11. Artikel 33 Absatz 1 erhält folgende Fassung:
- „(1) Die Mitgliedstaaten sorgen dafür, dass die Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane eines Unternehmens im Rahmen der ihnen durch einzelstaatliche Rechtsvorschriften übertragenen Zuständigkeiten die gemeinsame Aufgabe haben, sicherzustellen, dass die folgenden Dokumente im Einklang mit den Anforderungen dieser Richtlinie und gegebenenfalls mit den gemäß der Verordnung (EG) Nr. 1606/2002 angenommenen internationalen Rechnungslegungsstandards, mit der Delegierten Verordnung (EU) 2019/815, mit den Standards für die Nachhaltigkeitsberichterstattung nach Artikel **29b oder Artikel 29c** dieser Richtlinie und mit den Anforderungen des Artikels **29d** dieser Richtlinie aufgestellt und offengelegt werden:
- a) der Jahresabschluss, der Lagebericht und die Erklärung zur Unternehmensführung, wenn sie gesondert abgegeben wird; und
- b) der konsolidierte Abschluss, der konsolidierte Lagebericht und die konsolidierte Erklärung zur Unternehmensführung, wenn sie gesondert abgegeben wird.“

- (13) **12. Die Überschrift von Kapitel 8 erhält folgende Fassung:**
„ABSCHLUSSPRÜFUNG UND BESTÄTIGUNG DER
NACHHALTIGKEITSBERICHTERSTATTUNG“
- (14) 13. Artikel 34 wird wie folgt geändert:
- (a) a) Absatz 1 Unterabsatz 2 wird wie folgt geändert:
- (a) i) Buchstabe a Ziffer ii erhält folgende Fassung:
- „ii) ob der Lagebericht nach den geltenden rechtlichen Anforderungen,
ausgenommen der Anforderungen an die
Nachhaltigkeitsberichterstattung nach Artikel 19a dieser
Richtlinie, aufgestellt wurde;“
- (b) ii) Folgender Buchstabe wird eingefügt:

„aa) gegebenenfalls ein Urteil auf der Grundlage eines Auftrags zur Erlangung begrenzter Prüfungssicherheit darüber abzugeben, ob die Nachhaltigkeitsberichterstattung mit den Anforderungen dieser Richtlinie übereinstimmt, einschließlich der Frage, ob die Nachhaltigkeitsberichterstattung mit den nach Artikel **29b oder Artikel 29c** angenommenen Standards für die Berichterstattung übereinstimmt, und über das vom Unternehmen durchgeführte Verfahren zur Ermittlung von Informationen, über die nach diesen Standards für die Berichterstattung Bericht zu erstatten ist, ob die Anforderung zur Auszeichnung der Nachhaltigkeitsberichterstattung im Einklang mit Artikel **29d** eingehalten wird und ob die Anforderungen an die Berichterstattung nach Artikel 8 der Verordnung (EU) 2020/852 eingehalten werden;“

(b) b) Absatz 3 erhält folgende Fassung:

„(3) Die Mitgliedstaaten können ■ gestatten, **dass ein anderer Abschlussprüfer oder eine andere Prüfungsgesellschaft als der- oder diejenige(n), die die Abschlussprüfung durchführen**, das Urteil nach Absatz 1 Unterabsatz 2 Buchstabe aa **abgibt**.“

c) *Folgende Absätze werden angefügt:*

„(4) Die Mitgliedstaaten können einem in ihrem Hoheitsgebiet niedergelassenen unabhängigen Erbringer von Bestätigungsleistungen gestatten, das Urteil nach Absatz 1 Unterabsatz 2 Buchstabe aa abzugeben, sofern dieser unabhängige Erbringer von Bestätigungsleistungen Anforderungen unterliegt, die den in der Richtlinie 2006/43/EG festgelegten Anforderungen hinsichtlich der Bestätigung der Nachhaltigkeitsberichterstattung im Sinne von Artikel 2 Nummer 22 der genannten Richtlinie gleichwertig sind, insbesondere die Anforderungen an Folgendes:*

- a) Ausbildung und Eignungsprüfung, um sicherzustellen, dass unabhängige Erbringer von Bestätigungsleistungen das erforderliche Fachwissen auf dem Gebiet der Nachhaltigkeitsberichterstattung und deren Bestätigung erwerben;*
- b) kontinuierliche Fortbildung;*
- c) Qualitätssicherungssysteme;*
- d) Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis;*
- e) Bestellung und Abberufung;*

- f) Untersuchungen und Sanktionen;*
- g) die Organisation der Arbeit des unabhängigen Erbringers von Bestätigungsleistungen, insbesondere im Hinblick auf notwendige Mittel und Personal sowie die Führung von Mandantendateien und Akten, und*
- h) die Meldung von Unregelmäßigkeiten.*

Die Mitgliedstaaten stellen sicher, dass das Urteil in Fällen, in denen es nach Absatz 1 Unterabsatz 2 Buchstabe aa von einem unabhängigen Erbringer von Bestätigungsleistungen abgegeben wird, gemäß den Artikeln 26a, 27a und 28a der Richtlinie 2006/43/EG erstellt wird und dass der Prüfungsausschuss oder ein gesonderter Ausschuss gegebenenfalls die Unabhängigkeit des unabhängigen Erbringers von Bestätigungsleistungen gemäß Artikel 39 Absatz 6 Buchstabe e der Richtlinie 2006/43/EG überprüft und überwacht.

Die Mitgliedstaaten stellen sicher, dass unabhängige Erbringer von Bestätigungsleistungen, die vor dem 1. Januar 2024 gemäß der Verordnung (EG) Nr. 765/2008 für die Bestätigung der Nachhaltigkeitsberichterstattung akkreditiert wurden, nicht den Ausbildungs- und Prüfungsanforderungen nach Unterabsatz 1 Buchstabe a des vorliegenden Absatzes unterliegen.

Die Mitgliedstaaten stellen sicher, dass unabhängige Erbringer von Bestätigungsleistungen, die am 1. Januar 2024 gemäß den einschlägigen einzelstaatlichen Anforderungen das Akkreditierungsverfahren durchlaufen, im Hinblick auf die Bestätigung der Nachhaltigkeitsberichterstattung nicht den Ausbildungs- und Prüfungsanforderungen nach Unterabsatz 1 Buchstabe a unterliegen, sofern sie dieses Verfahren bis zum 1. Januar 2026 abschließen.

Die Mitgliedstaaten stellen sicher, dass die in den Unterabsätzen 3 und 4 genannten unabhängigen Erbringer von Bestätigungsleistungen im Rahmen der Weiterbildungsanforderung nach Unterabsatz 1 Buchstabe b die erforderlichen Kenntnisse auf dem Gebiet der Nachhaltigkeitsberichterstattung und deren Bestätigung erwerben.

Beschließt ein Mitgliedstaat gemäß Unterabsatz 1, einem unabhängigen Erbringer von Bestätigungsleistungen die Abgabe des Urteils nach Absatz 1 Unterabsatz 2 Buchstabe aa zu gestatten, so gestattet er dies auch einem anderen Abschlussprüfer als demjenigen, der die Abschlussprüfung durchführt, wie in Absatz 3 vorgesehen.

- (5) *Ab dem ... [vier Jahre nach Inkrafttreten dieser Änderungsrichtlinie] gestattet ein Mitgliedstaat, der von der Möglichkeit nach Absatz 4 Gebrauch gemacht hat (im Folgenden „Aufnahmemitgliedstaat“), es unabhängigen Erbringern von Bestätigungsleistungen, die in einem anderen Mitgliedstaat (im Folgenden „Herkunftsmitgliedstaat“) niedergelassen sind, die Bestätigung der Nachhaltigkeitsberichterstattung vorzunehmen.*

Der Herkunftsmitgliedstaat ist für die Beaufsichtigung der in seinem Hoheitsgebiet niedergelassenen unabhängigen Erbringer von Bestätigungsleistungen zuständig, es sei denn, der Aufnahmemitgliedstaat entscheidet, die von unabhängigen Erbringern von Bestätigungsleistungen in seinem Hoheitsgebiet durchgeführten Bestätigung der Nachhaltigkeitsberichterstattung zu beaufsichtigen.

Beschließt der Aufnahmemitgliedstaat, die Bestätigung der Nachhaltigkeitsberichterstattung, die in seinem Hoheitsgebiet von unabhängigen Erbringern von Bestätigungsleistungen durchgeführt wird, die in einem anderen Mitgliedstaat registriert sind, zu beaufsichtigen, so gilt für den Aufnahmemitgliedstaat Folgendes:

- a) *Er darf für derartige unabhängige Erbringer von Bestätigungsleistungen keine strengeren Anforderungen oder keine umfassendere Haftung vorsehen als sie nach einzelstaatlichem Recht für die Bestätigung der Nachhaltigkeitsberichterstattung von den unabhängigen Erbringern von Bestätigungsleistungen oder Abschlussprüfern verlangt werden, die in diesem Aufnahmemitgliedstaat niedergelassen sind; und*
 - b) *er muss die anderen Mitgliedstaaten von seinem Beschluss in Kenntnis setzen, die Bestätigung der Nachhaltigkeitsberichterstattung, die von unabhängigen Erbringern von Bestätigungsleistungen durchgeführt wird, die in anderen Mitgliedstaaten niedergelassen sind, zu beaufsichtigen.*
- (6) *Die Mitgliedstaaten stellen sicher, dass in Fällen, in denen ein Unternehmen nach dem Unionsrecht verpflichtet ist, Teile seiner Nachhaltigkeitsberichterstattung durch eine akkreditierte unabhängige dritte Partei überprüfen zu lassen, der Bericht der akkreditierten unabhängigen dritten Partei entweder als Anlage zum Lagebericht oder auf andere öffentlich zugängliche Weise bereitgestellt wird.*

* *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).“*

(15) **14. Folgendes Kapitel wird eingefügt:**

(16) **„KAPITEL 9a**

(17) **BERICHTERSTATTUNG BETREFFEND
DRITTLANDUNTERNEHMEN**

(18) **Artikel 40a**

Nachhaltigkeitsberichte betreffend Drittlandunternehmen

(1) **Ein Mitgliedstaat schreibt vor, dass ein in seinem Hoheitsgebiet niedergelassenes Tochterunternehmen, dessen oberstes Mutterunternehmen dem Recht eines Drittlandes unterliegt, einen Nachhaltigkeitsbericht offengelegt und zugänglich macht, der die in Artikel 29a Absatz 2 Buchstabe a Ziffern iii bis v, Buchstaben b bis f und gegebenenfalls Buchstabe h aufgeführten Informationen auf Gruppenebene dieses obersten Drittland-Mutterunternehmens enthält.**

Unterabsatz 1 gilt nur für große Tochterunternehmen sowie für kleine und mittlere Tochterunternehmen – mit Ausnahme von Kleinstunternehmen –, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a sind.

Ein Mitgliedstaat schreibt vor, dass eine in seinem Hoheitsgebiet ansässige Zweigniederlassung, die eine Zweigniederlassung eines dem Recht eines Drittlands unterliegenden Unternehmens ist, das entweder nicht Teil einer Gruppe ist oder auf oberster Ebene von einem Unternehmen gehalten wird, das nach dem Recht eines Drittlands geschaffen wurde, einen Nachhaltigkeitsbericht offenlegt und zugänglich macht, der die in Artikel 29a Absatz 2 Buchstabe a Ziffern iii bis v, Buchstaben b bis f und gegebenenfalls Buchstabe h aufgeführten Informationen auf Gruppenebene oder, falls dies nicht zutrifft, auf Einzelebene des Drittlandunternehmens enthält.

Die in Unterabsatz 3 genannte Vorschrift gilt für eine Zweigniederlassung nur, wenn das Drittlandunternehmen kein Tochterunternehmen im Sinne von Unterabsatz 1 hat und die Zweigniederlassung im vorangegangenen Geschäftsjahr Nettoumsatzerlöse von mehr als 40 Mio. EUR erzielt hat.

Die Unterabsätze 1 und 3 gelten nur für die in diesen Unterabsätzen genannten Tochterunternehmen oder Zweigniederlassungen, wenn das Drittlandunternehmen auf konsolidierter Ebene oder, falls dies nicht zutrifft, auf Gruppenebene in den beiden letzten aufeinander folgenden Geschäftsjahren in der Union Nettoumsatzerlöse von jeweils mehr als 150 Mio. EUR erzielt hat.

Die Mitgliedstaaten können von den in den Unterabsätzen 1 und 3 genannten Tochterunternehmen oder Zweigniederlassungen verlangen, dass sie ihnen Angaben über die von den Drittlandunternehmen in ihrem Gebiet und in der Union erzielten Nettoumsatzerlöse übermitteln.

- (2) Die Mitgliedstaaten schreiben vor, dass der von dem Tochterunternehmen oder der Zweigniederlassung gemäß Absatz 1 übermittelte Nachhaltigkeitsbericht im Einklang mit den gemäß Artikel 40b angenommenen Standards erstellt wird.*

Abweichend von Unterabsatz 1 des vorliegenden Absatzes kann der in Absatz 1 des vorliegenden Artikels genannte Nachhaltigkeitsbericht gemäß den nach Artikel 29b erlassenen Standards für die Nachhaltigkeitsberichterstattung oder in einer Weise erstellt werden, die diesen Standards für die Nachhaltigkeitsberichterstattung gleichwertig ist, was in einem gemäß Artikel 23 Absatz 4 Unterabsatz 3 der Richtlinie 2004/109/EG erlassenen Durchführungsrechtsakt über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung festgestellt wurde.

Wenn die in Unterabsatz 1 genannten Informationen, die für die Erstellung eines Nachhaltigkeitsberichts erforderlich sind, nicht vorliegen, fordert das in Absatz 1 genannte Tochterunternehmen oder die in Absatz 1 des vorliegenden Absatzes genannte Zweigniederlassung das Drittlandunternehmen auf, ihnen alle erforderlichen Informationen zu übermitteln, damit sie in der Lage sind, ihren Verpflichtungen nachzukommen.

Falls nicht alle erforderlichen Informationen zur Verfügung gestellt werden, erstellt das in Absatz 1 genannte Tochterunternehmen oder die in Absatz 1 genannte Zweigniederlassung den in Absatz 1 genannten Nachhaltigkeitsbericht und legt diesen offen, der alle in seinem bzw. ihrem Besitz befindlichen, erlangten oder erworbenen Informationen enthält, und gibt eine Erklärung ab, aus der hervorgeht, dass das Drittlandunternehmen die erforderlichen Informationen nicht bereitgestellt hat.

- (3) Die Mitgliedstaaten schreiben vor, dass der in Absatz 1 genannte Nachhaltigkeitsbericht zusammen mit einem Bestätigungsurteil offengelegt wird, das von einer oder mehreren Personen oder Gesellschaften abgegeben wurde, die nach dem einzelstaatlichen Recht, das für das Drittlandunternehmen oder für einen Mitgliedstaat gilt, zur Abgabe eines Urteils über die Bestätigung der Nachhaltigkeitsberichterstattung befugt ist bzw. sind.*

Falls das Drittlandunternehmen das Bestätigungsurteil gemäß Unterabsatz 1 nicht zur Verfügung stellt, gibt das Tochterunternehmen oder die Zweigniederlassung eine Erklärung ab, aus der hervorgeht, dass das Drittlandunternehmen das erforderliche Bestätigungsurteil nicht bereitgestellt hat.

- (4) Die Mitgliedstaaten können die Kommission jährlich über die Tochterunternehmen oder Zweigniederlassungen von Drittlandunternehmen, die die Offenlegungspflicht nach Artikel 40d erfüllt haben, sowie über die Fälle unterrichten, in denen ein Bericht offengelegt wurde, das Tochterunternehmen oder die Zweigniederlassung jedoch gemäß Absatz 2 Unterabsatz 4 des vorliegenden Artikels gehandelt hat. Die Kommission macht auf ihrer Website eine Liste der Drittlandunternehmen, die einen Nachhaltigkeitsbericht offenlegen, öffentlich zugänglich.**

Artikel 40b

Standards für die Nachhaltigkeitsberichterstattung für Drittlandunternehmen

- (19) Die Kommission erlässt bis spätestens 30. Juni 2024 einen delegierten Rechtsakt gemäß Artikel 49 zur Ergänzung dieser Richtlinie, um Standards für die Nachhaltigkeitsberichterstattung für Drittlandsunternehmen festzulegen, durch die präzisiert wird, welche Angaben die in Artikel 40a genannten Nachhaltigkeitsberichte enthalten müssen.**

Artikel 40c

Verantwortlichkeit für die Erstellung, Offenlegung und Zugänglichmachung der Nachhaltigkeitsberichte betreffend Drittlandunternehmen

Die Mitgliedstaaten sehen vor, dass die Zweigniederlassungen von Drittlandunternehmen die Verantwortung dafür tragen, nach bestem Wissen und Vermögen sicherzustellen, dass ihr Nachhaltigkeitsbericht gemäß Artikel 40a erstellt wird und dass dieser Bericht gemäß Artikel 40d offengelegt und zugänglich gemacht wird.

Die Mitgliedstaaten sehen vor, dass die Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane der Tochterunternehmen nach Artikel 40a die gemeinsame Verantwortung dafür tragen, nach bestem Wissen und Vermögen sicherzustellen, dass ihr Nachhaltigkeitsbericht gemäß Artikel 40a erstellt wird und dass dieser Bericht gemäß Artikel 40d offengelegt und zugänglich gemacht wird.

Artikel 40d

Offenlegung

- (1) Die in Artikel 40a Absatz 1 der vorliegenden Richtlinie genannten Tochterunternehmen und Zweigniederlassungen legen ihren Nachhaltigkeitsbericht zusammen mit dem Bestätigungsurteil und gegebenenfalls der in Artikel 40a Absatz 2 Unterabsatz 4 dieser Richtlinie genannten Erklärung innerhalb von zwölf Monaten nach dem Bilanzstichtag des Geschäftsjahres, für das der Bericht erstellt wird, gemäß den mit den Artikeln 14 bis 28 der Richtlinie (EU) 2017/1132 und gegebenenfalls mit Artikel 36 der genannten Richtlinie in Einklang stehenden Rechtsvorschriften eines jeden Mitgliedstaats offen.**
- (2) Wenn der Nachhaltigkeitsbericht zusammen mit dem Bestätigungsurteil und gegebenenfalls der Erklärung, die gemäß Absatz 1 des vorliegenden Artikels offengelegt wird, der Öffentlichkeit nicht kostenlos auf der Website des in Artikel 16 der Richtlinie (EU) 2017/1132 genannten Registers zugänglich gemacht werden, stellen die Mitgliedstaaten sicher, dass der Nachhaltigkeitsbericht zusammen mit dem Bestätigungsurteil und gegebenenfalls mit der Erklärung, die von den Unternehmen gemäß Absatz 1 des vorliegenden Artikels offengelegt wird, der Öffentlichkeit in mindestens einer der Amtssprachen der Union spätestens zwölf Monate nach dem Bilanzstichtag des Geschäftsjahres, für das der Bericht erstellt wird, auf der Website des Tochterunternehmens oder der Zweigniederlassung gemäß Artikel 40a Absatz 1 dieser Richtlinie kostenlos zugänglich gemacht wird.“**

(20) 15. Die Überschrift von Kapitel 11 erhält folgende Fassung:

„KAPITEL

11

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN“

(21) 16. Folgender Artikel wird eingefügt:

„Artikel 48i

Übergangsbestimmungen

(1) *Bis zum ... [sieben Jahre nach dem Datum des Inkrafttretens dieser Änderungsrichtlinie] gestatten die Mitgliedstaaten es einem Unions-Tochterunternehmen, das Artikel 19a oder 29a unterliegt und dessen Mutterunternehmen nicht den Rechtsvorschriften eines Mitgliedstaats unterliegt, eine konsolidierte Nachhaltigkeitsberichterstattung gemäß den Anforderungen des Artikels 29a zu erstellen, der alle Unions-Tochterunternehmen dieses Mutterunternehmens einschließt, die Artikel 19a oder 29a unterliegen.*

Bis zum ... [sieben Jahre nach dem Datum des Inkrafttretens dieser Änderungsrichtlinie] gestatten die Mitgliedstaaten, dass die in Unterabsatz 1 des vorliegenden Absatzes genannte konsolidierte Nachhaltigkeitsberichterstattung die in Artikel 8 der Verordnung (EU) 2020/852 festgelegten Offenlegungen enthält, die sich auf die Tätigkeiten aller Unions-Tochterunternehmen des in Unterabsatz 1 des vorliegenden Absatzes genannten Mutterunternehmens beziehen, die Artikel 19a oder 29a dieser Richtlinie unterliegen.

- (2) *Bei dem in Absatz 1 genannten Unions-Tochterunternehmen muss es sich um eines der Unions-Tochterunternehmen der Gruppe handeln, die – gegebenenfalls auf konsolidierter Basis – in mindestens einem der fünf vorangegangenen Geschäftsjahre in der Union die größten Umsatzerlöse erzielt hat.*
- (3) *Die in Absatz 1 des vorliegenden Artikels genannte konsolidierte Nachhaltigkeitsberichterstattung wird im Einklang mit Artikel 30 offengelegt.*
- (4) *Für die Zwecke der in Artikel 19a Absatz 9 und Artikel 29a Absatz 8 vorgesehenen Befreiung gilt die Berichterstattung gemäß Absatz 1 des vorliegenden Artikels als Berichterstattung eines Mutterunternehmens auf Gruppenebene in Bezug auf die in die Konsolidierung einbezogenen Unternehmen. Die Berichterstattung gemäß Absatz 1 Unterabsatz 2 des vorliegenden Artikels gilt als Erfüllung der Bedingungen in Artikel 19a Absatz 9 Unterabsatz 2 Buchstabe c bzw. in Artikel 29a Absatz 8 Unterabsatz 2 Buchstabe c.“*
- (22) 17. Artikel 49 wird wie folgt geändert:
- (a) a) Die Absätze 2 und 3 erhalten folgende Fassung:

- „(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 1 Absatz 2, Artikel 3 Absatz 13, **Artikel 29b, Artikel 29c, Artikel 40b und Artikel 46 Absatz 2** ■ wird der Kommission **für einen Zeitraum von fünf Jahren ab dem ... [Datum des Inkrafttretens dieser Änderungsrichtlinie]** 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 1 Absatz 2, Artikel 3 Absatz 13, **Artikel 29b, Artikel 29c, Artikel 40b und Artikel 46 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.“

(b) b) Folgender Absatz wird eingefügt:

„(3b) Beim Erlass delegierter Rechtsakte nach den Artikeln **29b** und **29c** berücksichtigt die Kommission die fachliche Stellungnahme der EFrag, sofern

- a) *eine solche Stellungnahme in einem einwandfreien Verfahren mit angemessener öffentlicher Aufsicht und Transparenz erstellt und dabei auf das Fachwissen einschlägiger Interessenträger zurückgegriffen wurde und sie mit ausreichenden öffentlichen Mitteln, so dass ihre Unabhängigkeit gewährleistet ist, und auf der Grundlage eines Arbeitsprogramms, zu dem die Kommission konsultiert wurde, erstellt wurde;*
- b) *einer solchen Stellungnahme Kosten-Nutzen-Analysen beigelegt sind, einschließlich Analysen der Auswirkungen der fachlichen Stellungnahme auf Nachhaltigkeitsaspekte;*
- c) *einer solchen Stellungnahme eine Erläuterung beigelegt ist, wie die in Artikel 29b Absatz 5 aufgeführten Elemente berücksichtigt werden;*
- d) *die Mitwirkung an der Arbeit der EFrag auf technischer Ebene auf Fachwissen im Bereich der Nachhaltigkeitsberichterstattung beruht und nicht von einem finanziellen Beitrag abhängig ist.*

Die Buchstaben a und d gelten unbeschadet der Beteiligung von öffentlichen Stellen und einzelstaatlichen Standardsetzungseinrichtungen an den technischen Arbeiten der EFRAG.

Die der fachlichen Stellungnahme der EFRAG beigefügten Dokumente sind zusammen mit dieser fachlichen Stellungnahme vorzulegen.

Die Kommission konsultiert **die in Artikel 24 der Verordnung (EU) 2020/852 genannte** Sachverständigengruppe der Mitgliedstaaten für nachhaltiges Finanzwesen **und den in Artikel 6 der Verordnung (EG) Nr. 1606/2002 genannten Regelungsausschuss für Rechnungslegung gemeinsam zu den Entwürfen delegierter Rechtsakte vor ihrer Annahme gemäß den Artikeln 29b und 29c dieser Richtlinie.**

Die Kommission holt die Stellungnahme der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA), **der Europäischen Bankenaufsichtsbehörde (EBA) und der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA)** zur fachlichen Stellungnahme der EFRAG ein, insbesondere im Hinblick auf deren Kohärenz mit der Verordnung (EU) 2019/2088 und den delegierten Rechtsakten, die gemäß jener Verordnung angenommen wurden. ESMA, EBA und EIOPA übermitteln ihre **Stellungnahmen** binnen zwei Monaten nach Eingang des Ersuchens der Kommission.

Darüber hinaus konsultiert die Kommission die Europäische
■ Umweltagentur, die Agentur der Europäischen Union für Grundrechte,
die ■ Europäische Zentralbank, den ■ Ausschuss der Europäischen
Aufsichtsstellen für Abschlussprüfer und die nach Artikel 20 der
Verordnung (EU) 2020/852 eingerichtete Plattform für ein nachhaltiges
Finanzwesen zu der von der EFRAG bereitgestellten fachlichen
Stellungnahme vor Annahme der in den Artikeln **29b und 29c dieser
Richtlinie** genannten delegierten Rechtsakte. Beschließt eine dieser
Stellen, eine Stellungnahme zu übermitteln, so legt sie diese binnen zwei
Monaten nach ihrer Konsultation durch die Kommission vor. “

- (c) c) Absatz 5 erhält folgende Fassung:
- „(5) Ein delegierter Rechtsakt, der gemäß Artikel 1 Absatz 2, Artikel 3
Absatz 13, **Artikel 29b, Artikel 29c oder Artikel 40b, oder** Artikel 46
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.“

(23) ■

Artikel 2
Änderung der Richtlinie 2004/109/EG

Die Richtlinie 2004/109/EG wird wie folgt geändert:

- (24) 1. In Artikel 2 Absatz 1 wird folgender Buchstabe angefügt:
- „r) „Nachhaltigkeitsberichterstattung“ ist die Nachhaltigkeitsberichterstattung gemäß Artikel 2 Nummer 18 der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates*,

* 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).“

- (25) 2. Artikel 4 wird wie folgt geändert:
- (a) a) Absatz 2 Buchstabe c erhält folgende Fassung:

„c) Erklärungen, in denen die beim Emittenten verantwortlichen Personen unter Angabe ihres Namens und ihrer Stellung versichern, dass der im Einklang mit den maßgebenden Rechnungslegungsstandards aufgestellte Abschluss ihres Wissens ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögenswerte und Verbindlichkeiten sowie der Finanz- und der Ertragslage des Emittenten und der Gesamtheit der in die Konsolidierung einbezogenen Unternehmen vermittelt und dass der Lagebericht den Geschäftsverlauf, das Geschäftsergebnis und die Lage der Gesamtheit der in die Konsolidierung einbezogenen Unternehmen so darstellt, dass ein den tatsächlichen Verhältnissen entsprechendes Bild entsteht, dass er die wesentlichen Risiken und Ungewissheiten, denen sie ausgesetzt sind, beschreibt, und, sofern angebracht, dass er in Einklang mit den Standards für die Nachhaltigkeitsberichterstattung nach Artikel 29b der Richtlinie 2013/34/EU **und mit den gemäß Artikel 8 Absatz 4 der Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates* angenommenen Spezifikationen** aufgestellt wurde.

* Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088 (ABl. L 198 vom 22.6.2020, S. 13).“

(b) b) Die Absätze 4 und 5 erhalten folgende Fassung:

„(4) Die Abschlüsse werden gemäß Artikel 34 **Absatz 1 Unterabsatz 1** und Artikel **34 Absatz 2** der Richtlinie **2013/34/EU** geprüft.

Der Abschlussprüfer gibt das Urteil und die Erklärung zum Lagebericht nach Artikel 34 Absatz 1 Unterabsatz 2 Buchstaben a und b und Artikel 34 Absatz 2 der Richtlinie 2013/34/EU ab.

Der von der oder den für die Durchführung der in Artikel 34 Absätze 1 und 2 der Richtlinie **2013/34/EU** festgelegten Arbeiten zuständigen Person oder Personen erteilte Bestätigungsvermerk **nach Artikel 28 der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates*** wird in vollem Umfang zusammen mit dem Jahresfinanzbericht offengelegt.

Gegebenenfalls wird gemäß Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa und Artikel 34 Absätze 2 bis 5 der Richtlinie 2013/34/EU ein Bestätigungsurteil über die Nachhaltigkeitsberichterstattung abgegeben.

Der Prüfungsvermerk über die Nachhaltigkeitsberichterstattung nach Artikel 28a der Richtlinie 2006/43/EG wird zusammen mit dem Jahresfinanzbericht vollständig offengelegt.

- (5) Der Lagebericht wird gemäß den Artikeln 19, 19a, 20 und Artikel 29d Absatz 1 der Richtlinie 2013/34/EU aufgestellt **und umfasst die gemäß Artikel 8 Absatz 4 der Verordnung (EU) 2020/852 angenommenen Spezifikationen**, wenn er von den in diesen Bestimmungen genannten Unternehmen aufgestellt wird.

Ist der Emittent verpflichtet, einen konsolidierten Abschluss aufzustellen, wird der konsolidierte Lagebericht gemäß den Artikeln 29 und 29a **und Artikel 29d Absatz 2** der Richtlinie 2013/34/EU aufgestellt **und umfasst die gemäß Artikel 8 Absatz 4 der Verordnung (EU) 2020/852 angenommenen Spezifikationen**, wenn er von den in diesen Bestimmungen genannten Unternehmen aufgestellt wird.

* 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).“

(26) 3. ■ Artikel 23 Absatz 4 *wird wie folgt geändert:*

a) *Die Unterabsätze 3 und 4 erhalten folgende Fassung:*

„Die Kommission fasst nach dem in Artikel 27 Absatz 2 dieser Richtlinie genannten Verfahren die notwendigen Beschlüsse ■ über die Gleichwertigkeit der Rechnungslegungsstandards *unter den in Artikel 30 Absatz 3 dieser Richtlinie festgelegten Bedingungen* und über die Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung nach Artikel 29b der Richtlinie 2013/34/EU, die von Emittenten mit Sitz in Drittländern angewandt werden. Kommt die Kommission zu dem Schluss, dass die Rechnungslegungsstandards oder die Standards für die Nachhaltigkeitsberichterstattung eines Drittlandes nicht gleichwertig sind, kann sie den betroffenen Emittenten die weitere Anwendung dieser *Standards* während einer angemessenen Übergangsperiode gestatten.

In Zusammenhang mit Unterabsatz 3 des vorliegenden Absatzes erlässt die Kommission im Wege delegierter Rechtsakte, die im Einklang mit Artikel 27 Absätze 2a, 2b und 2c angenommen werden, und unter den in den Artikeln 27a und 27b festgelegten Bedingungen zudem Maßnahmen zur Festlegung allgemeiner Kriterien für die Gleichwertigkeit von Rechnungslegungsstandards und Standards für die Nachhaltigkeitsberichterstattung, die für Emittenten aus mehr als einem Land relevant sind.“

- (27) **b) Folgender Unterabsatz wird angefügt:**
„Durch die Kriterien, die die Kommission zur Bewertung der Gleichwertigkeit der Standards für die Nachhaltigkeitsberichterstattung heranzieht, die von Emittenten mit Sitz in Drittländern gemäß Unterabsatz 3 verwendet werden, ist zumindest gewährleistet,
- a)** *dass die Standards für die Nachhaltigkeitsberichterstattung die Unternehmen verpflichten, Informationen über Umwelt-, Sozial- und Governance-Faktoren offenzulegen;*
- (28) **b)** *dass die Standards für die Nachhaltigkeitsberichterstattung die Unternehmen verpflichten, Informationen offenzulegen, die für das Verständnis ihrer nachhaltigkeitsrelevanten Auswirkungen sowie das Verständnis der Auswirkungen von Nachhaltigkeitsaspekten auf ihren Geschäftsverlauf, ihr Geschäftsergebnis und ihre Lage erforderlich sind.“*

(29) 4. Folgender Artikel wird eingefügt:

„Artikel 28d

Leitlinien der ESMA

Nach Konsultation der Europäischen Umweltagentur und der Agentur der Europäischen Union für Grundrechte gibt die ESMA im Einklang mit Artikel 16 der Verordnung (EU) Nr. 1095/2010 Leitlinien über die Beaufsichtigung der Nachhaltigkeitsberichterstattung durch die zuständigen nationalen Behörden heraus.“

Artikel 3

Änderung der Richtlinie 2006/43/EG

Die Richtlinie 2006/43/EG wird wie folgt geändert:

(30) 1. Artikel 1 erhält folgende Fassung:

„Artikel 1

Gegenstand

Diese Richtlinie regelt die Abschlussprüfung des Jahresabschlusses und des konsolidierten Abschlusses und die Bestätigung der jährlichen und konsolidierten Nachhaltigkeitsberichterstattung ■ .“

- (31) 2. Artikel 2 wird wie folgt geändert:
- (a) a) Die Nummern 2 **bis 6** erhalten folgende Fassung:
- „(2) „Abschlussprüfer“ ist eine natürliche Person, die von den zuständigen Stellen eines Mitgliedstaats nach dieser Richtlinie für die Durchführung von Abschlussprüfungen und **gegebenenfalls von** für die Bestätigung der Nachhaltigkeitsberichterstattung zugelassen wurde;
- (3) „Prüfungsgesellschaft“ ist eine juristische Person oder eine sonstige Einrichtung gleich welcher Rechtsform, die von den zuständigen Stellen eines Mitgliedstaats nach dieser Richtlinie für die Durchführung von Abschlussprüfungen und **gegebenenfalls von** für die Bestätigung der Nachhaltigkeitsberichterstattung zugelassen wurde;
- (4) ***„Prüfungsunternehmen aus einem Drittland“ ist ein Unternehmen gleich welcher Rechtsform, das die Prüfungen des Jahresabschlusses oder des konsolidierten Abschlusses oder gegebenenfalls die Bestätigung der Nachhaltigkeitsberichterstattung von in einem Drittland eingetragenen Gesellschaften durchführt und das nicht in einem Mitgliedstaat infolge einer Zulassung gemäß Artikel 3 als Prüfungsgesellschaft registriert ist;***

- (5) *„Prüfer aus einem Drittland“ ist eine natürliche Person, die die Prüfungen des Jahresabschlusses oder des konsolidierten Abschlusses oder gegebenenfalls die Bestätigung der Nachhaltigkeitsberichterstattung von in einem Drittland eingetragenen Gesellschaften durchführt und die nicht in einem Mitgliedstaat infolge einer Zulassung gemäß den Artikeln 3 und 44 als Abschlussprüfer registriert ist;*
- (6) *„Konzernabschlussprüfer“ sind der oder die Abschlussprüfer bzw. die Prüfungsgesellschaft oder -gesellschaften, die die Abschlussprüfung konsolidierter Abschlüsse durchführen oder gegebenenfalls die Bestätigung der Nachhaltigkeitsberichterstattung durchführen;“*
- (b) b) *folgende Nummer wird eingefügt:*
- „16a. „Verantwortliche(r) Nachhaltigkeitspartner“ ist/sind*
- a) *der oder die Abschlussprüfer, der/die von einer Prüfungsgesellschaft für einen bestimmten Bestätigungsauftrag hinsichtlich der Nachhaltigkeitsberichterstattung als vorrangig verantwortlich für die Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung im Auftrag der Prüfungsgesellschaft bestimmt ist/sind; oder*

- b) *im Fall der Bestätigung einer konsolidierten Nachhaltigkeitsberichterstattung mindestens der/die Abschlussprüfer, der/die von einer Prüfungsgesellschaft als vorrangig verantwortlich für die Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung auf Konzernebene bestimmt ist/sind, und der/die Abschlussprüfer, der/die als vorrangig verantwortlich auf der Ebene bedeutender Tochterunternehmen bestimmt ist/sind; oder*
- c) *der/die Abschlussprüfer, der/die den Prüfungsvermerk über die Nachhaltigkeitsberichterstattung nach Artikel 28a unterzeichnet/unterzeichnen;“*
- (c) c) Folgende Nummern werden angefügt:
- „21. „Nachhaltigkeitsberichterstattung“ ist die Nachhaltigkeitsberichterstattung gemäß Artikel 2 Nummer 18 der Richtlinie 2013/34/EU.
22. „Bestätigung der Nachhaltigkeitsberichterstattung“ ist die Durchführung von Verfahren, die zu dem Urteil des Abschlussprüfers oder der Prüfungsgesellschaft nach Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa und Artikel 34 Absatz 2 der Richtlinie 2013/34/EU führen.

23. *„Unabhängiger Erbringer von Bestätigungsleistungen“ ist eine Konformitätsbewertungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates* für die in Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa der Richtlinie 2013/34/EU genannte Konformitätsbewertung akkreditiert ist.*

* *Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und zur Aufhebung der Verordnung (EWG) Nr. 339/93 (ABl. L 218 vom 13.8.2008, S. 30).“*

(32) 3. Artikel 6 **erhält** folgende Fassung:

„Artikel 6

Ausbildung

- (1) Unbeschadet des Artikels 11 kann eine natürliche Person nur zur Durchführung von Abschlussprüfungen ■ zugelassen werden, wenn sie nach Erlangung der Hochschulreife oder einer entsprechenden Ausbildungsstufe eine theoretische und eine praktische Ausbildung absolviert und sich mit Erfolg einer staatlichen oder staatlich anerkannten beruflichen Eignungsprüfung auf dem Niveau eines Hochschulabschlusses oder eines entsprechenden Niveaus in dem betreffenden Mitgliedstaat unterzogen hat.
- (2) ***Zusätzlich zu der Zulassung zur Durchführung von Abschlussprüfungen gemäß Absatz 1 dieses Artikels kann eine natürliche Person zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen werden, wenn die zusätzlichen spezifischen Anforderungen von Artikel 7 Absatz 2, Artikel 8 Absatz 3, Artikel 10 Absatz 1 Unterabsatz 2 und Artikel 14 Absatz 2 Unterabsatz 4 dieser Richtlinie erfüllt sind.***

- (3) Die in Artikel 32 genannten zuständigen Behörden arbeiten im Hinblick auf eine Angleichung der in diesem Artikel genannten Anforderungen zusammen. Bei der Aufnahme dieser Zusammenarbeit tragen diese zuständigen Behörden den Entwicklungen im Prüfungswesen und im Berufsstand der Prüfer und insbesondere der Angleichung Rechnung, die bereits in dem Berufsstand erreicht wurde. Sie arbeiten mit dem Ausschuss der Europäischen Aufsichtsstellen für Abschlussprüfer (*im Folgenden „Ausschuss der Aufsichtsstellen“*) ■ und den in Artikel 20 der Verordnung (EU) Nr. 537/2014 genannten zuständigen Behörden zusammen, sofern es bei dieser Angleichung um die Abschlussprüfung und die Bestätigung der Nachhaltigkeitsberichterstattung bei Unternehmen von öffentlichem Interesse geht.“

■

(33) **4. Artikel 7 erhält folgende Fassung:**

„Artikel 7

Prüfung der beruflichen Eignung

- (1) Die in Artikel 6 genannte Eignungsprüfung garantiert die erforderlichen theoretischen Kenntnisse auf den für die Abschlussprüfung maßgebenden Sachgebieten sowie die Fähigkeit, diese Kenntnisse praktisch anzuwenden. Diese Eignungsprüfung muss zumindest teilweise schriftlich erfolgen.
- (2) ***Falls der Abschlussprüfer auch zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen werden soll, garantiert die in Artikel 6 genannte Eignungsprüfung die erforderlichen theoretischen Kenntnisse auf den für die Bestätigung der Nachhaltigkeitsberichterstattung maßgebenden Sachgebieten sowie die Fähigkeit, diese Kenntnisse praktisch anzuwenden. Diese Eignungsprüfung muss zumindest teilweise schriftlich erfolgen.“***

(34)

5. *In Artikel 8 wird folgender Absatz angefügt:*

„(3) Falls der Abschlussprüfer auch zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen werden soll, umfasst die in Absatz 1 genannte Prüfung der theoretischen Kenntnisse außerdem zumindest die folgenden Sachgebiete:

- a) gesetzliche Vorschriften und Standards für die Aufstellung der jährlichen und konsolidierten Nachhaltigkeitsberichterstattung;*
- b) Nachhaltigkeitsanalyse;*
- c) Due-Diligence-Prozesse mit Blick auf Nachhaltigkeitsaspekte;*
- d) rechtliche Anforderungen an und Standards für die Bestätigung der Nachhaltigkeitsberichterstattung nach Artikel 26a.“*

(35) 6. *In Artikel 10 Absatz 1 wird folgender Unterabsatz angefügt:*

„Falls der Abschlussprüfer oder der Auszubildende auch zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen werden soll, bestehen mindestens acht Monate der praktischen Ausbildung nach Absatz 1 in der Bestätigung jährlicher oder konsolidierter Nachhaltigkeitsberichterstattung oder anderen nachhaltigkeitsbezogenen Leistungen.“

(36) 7. Artikel 12 erhält folgende Fassung:

„Artikel 12

Kombination von praktischer und theoretischer Ausbildung

- (1) Die Mitgliedstaaten können vorsehen, dass Zeiten, in denen eine theoretische Ausbildung in den in Artikel 8 Absätze 1 und 2 genannten Sachgebieten absolviert wurde, auf die in Artikel 11 genannten Berufsjahre angerechnet werden, wenn diese Ausbildung mit einer durch den Mitgliedstaat anerkannten Prüfung abgeschlossen wurde. Diese Ausbildung muss mindestens ein Jahr dauern und darf höchstens mit vier Jahren auf die berufliche Tätigkeit angerechnet werden.*
- (2) Berufstätigkeit und praktische Ausbildung dürfen nicht kürzer sein als die theoretische Ausbildung zusammen mit der in Artikel 10 Absatz 1 Unterabsatz 1 vorgeschriebenen praktischen Ausbildung.“*

(37)

8. *In Artikel 14 Absatz 2 wird folgender Unterabsatz angefügt:*

„Falls der Abschlussprüfer auch zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen werden soll, erstreckt sich die Eignungsprüfung nach Unterabsatz 1 darauf, ob der Abschlussprüfer über angemessene Kenntnisse der Rechtsvorschriften des Aufnahmemitgliedstaats verfügt, soweit diese Kenntnisse für die Bestätigung der Nachhaltigkeitsberichterstattung relevant sind.“

(38) 9. Folgender Artikel wird eingefügt:

„Artikel 14a

■ *Vor dem 1. Januar 2024 zugelassene oder anerkannte Abschlussprüfer **und Personen, die am 1. Januar 2024 das Zulassungsverfahren für Abschlussprüfer durchlaufen***

Die Mitgliedstaaten stellen sicher, dass Abschlussprüfer, die vor dem 1. Januar 2024 für die Durchführung von Abschlussprüfungen zugelassen oder anerkannt wurden, nicht den Anforderungen von *Artikel 7 Absatz 2, Artikel 8 Absatz 3, Artikel 10 Absatz 1 Unterabsatz 2 und Artikel 14 Absatz 2 Unterabsatz 4* unterliegen.

Die Mitgliedstaaten stellen sicher, dass Personen, die am 1. Januar 2024 das in den Artikeln 6 bis 14 vorgesehene Zulassungsverfahren durchlaufen, nicht den Anforderungen von Artikel 7 Absatz 2, Artikel 8 Absatz 3, Artikel 10 Absatz 1 Unterabsatz 2 und Artikel 14 Absatz 2 Unterabsatz 4 unterliegen, sofern sie dieses Verfahren bis zum 1. Januar 2026 abschließen.

Die Mitgliedstaaten stellen sicher, dass vor dem 1. Januar 2026 zugelassene Abschlussprüfer, **die Bestätigung der Nachhaltigkeitsberichterstattung durchführen wollen**, die erforderlichen Kenntnisse über Nachhaltigkeitsberichterstattung und deren Bestätigung, **einschließlich der in Artikel 8 Absatz 3 aufgeführten Sachgebiete**, im Wege der kontinuierlichen Fortbildung nach Artikel 13 erwerben.“

(39) **10. Artikel 16 wird wie folgt geändert:**

(a) **a) Absatz 1 erhält folgende Fassung:**

„(1) Für Abschlussprüfer werden im öffentlichen Register zumindest die folgenden Angaben geführt:

- a) Name, Anschrift und Registrierungsnummer;
- b) gegebenenfalls Name, Anschrift, Internet-Adresse und Registrierungsnummer der Prüfungsgesellschaft(en), bei der/denen der Abschlussprüfer angestellt ist oder der/denen er als Partner angehört oder in ähnlicher Form verbunden ist;
- c) **Angabe, ob der Abschlussprüfer auch für die Bestätigung der Nachhaltigkeitsberichterstattung zugelassen ist;**

- d) *andere Registrierung(en) als Abschlussprüfer bei den zuständigen Stellen anderer Mitgliedstaaten und als Prüfer in Drittländern, einschließlich Name(n) der Zulassungsbehörde(n) und gegebenenfalls Registrierungsnummer(n), und Angabe, ob die Registrierung die Abschlussprüfung, die Bestätigung der Nachhaltigkeitsberichterstattung oder beides betrifft.“*
 - (b) *b) In Absatz 2 wird folgender Unterabsatz angefügt:
„Im Register wird angegeben, ob die Prüfer aus Drittländern nach Unterabsatz 1 für die Durchführung der Abschlussprüfung, die Bestätigung der Nachhaltigkeitsberichterstattung oder beides registriert sind.“*
- (40) 11. *Artikel 17 wird wie folgt geändert:*
 - (a) *a) Absatz 1 Buchstabe e erhält folgende Fassung:
„e) Name und Registrierungsnummer aller Abschlussprüfer, die bei der Prüfungsgesellschaft angestellt sind oder ihr als Partner angehören oder in ähnlicher Form mit ihr verbunden sind, und Angabe, ob sie auch zur Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung zugelassen sind;“*

b) *Absatz 1 Buchstabe i erhält folgende Fassung:*

„i) andere Registrierung(en) als Prüfungsgesellschaft bei den zuständigen Stellen anderer Mitgliedstaaten und als Prüfungsunternehmen in Drittländern, einschließlich Name(n) der Zulassungsbehörde(n), und gegebenenfalls Registrierungsnummer(n), und Angabe, ob die Registrierung die Abschlussprüfung, die Bestätigung der Nachhaltigkeitsberichterstattung oder beides betrifft;“

(b) c) *In Absatz 2 wird folgender Unterabsatz angefügt:*

„Im Register wird angegeben, ob die Prüfungsunternehmen aus Drittländern nach Unterabsatz 1 für die Durchführung der Abschlussprüfung, die Bestätigung der Nachhaltigkeitsberichterstattung oder beides registriert sind.“

(41) 12. Artikel 24b wird wie folgt geändert:

(a) a) Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten sorgen dafür, dass eine Prüfungsgesellschaft, die die Abschlussprüfung durchführt, zumindest einen verantwortlichen Prüfungspartner benennt. Die Prüfungsgesellschaft stellt dem verantwortlichen Prüfungspartner oder den verantwortlichen Prüfungspartnern die zur angemessenen Wahrnehmung seiner bzw. ihrer Aufgaben notwendigen Mittel und Personal mit der notwendigen Kompetenz und den notwendigen Fähigkeiten zur Verfügung.

Die Mitgliedstaaten sorgen dafür, dass eine Prüfungsgesellschaft, die die Bestätigung der Nachhaltigkeitsberichterstattung durchführt, zumindest einen verantwortlichen Nachhaltigkeitspartner benennt, bei dem es sich um den bzw. einen der verantwortlichen Prüfungspartner handeln kann. Die Prüfungsgesellschaft stellt dem verantwortlichen Nachhaltigkeitspartner oder den verantwortlichen Nachhaltigkeitspartnern die zur angemessenen Wahrnehmung seiner bzw. ihrer Aufgaben notwendigen Mittel und Personal mit der notwendigen Kompetenz und den notwendigen Fähigkeiten zur Verfügung.

Die Hauptkriterien, nach denen die Prüfungsgesellschaft den oder die zu benennenden verantwortlichen Prüfungspartner **und gegebenenfalls** den oder die **verantwortlichen Nachhaltigkeitspartner** bestimmt, sind die Sicherstellung der Qualität der Prüfung und Bestätigung, Unabhängigkeit und Kompetenz.

Der verantwortliche oder die verantwortlichen Prüfungspartner ist/sind aktiv an der Durchführung der Abschlussprüfung ■ beteiligt. **Der verantwortliche Nachhaltigkeitspartner ist aktiv an der Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung beteiligt.**“

- (b) b) Folgender Absatz wird eingefügt:
- „(2a) Der Abschlussprüfer wendet bei der Durchführung der Bestätigung der Nachhaltigkeitsberichterstattung ausreichend Zeit auf und sieht ausreichende Ressourcen vor, um seine Aufgaben angemessen wahrzunehmen.“

- (c) c) Absatz 4 **Buchstaben b und c erhalten** folgende Fassung:
- „b) **bei einer Prüfungsgesellschaft den/die Name(n) des verantwortlichen Prüfungspartners bzw. der verantwortlichen Prüfungspartner und gegebenenfalls den/die Name(n) des verantwortlichen Nachhaltigkeitspartners bzw. der verantwortlichen Nachhaltigkeitspartner,**
- c) für jedes Geschäftsjahr die für die Abschlussprüfung, für die Bestätigung der Nachhaltigkeitsberichterstattung und für andere Leistungen in Rechnung gestellten Honorare.“
- (d) d) **Folgender Absatz wird eingefügt:**
- „(5a) **Abschlussprüfer und Prüfungsgesellschaften legen für jeden Bestätigungsauftrag hinsichtlich der Nachhaltigkeitsberichterstattung eine Bestätigungsakte an.**
- Der Abschlussprüfer oder die Prüfungsgesellschaft dokumentiert zumindest die gemäß Artikel 22b aufgezeichneten Daten im Hinblick auf die Bestätigung der Nachhaltigkeitsberichterstattung.**
- Der Abschlussprüfer oder die Prüfungsgesellschaft bewahrt alle sonstigen Daten und Unterlagen auf, die zur Begründung des Prüfungsvermerks über die Nachhaltigkeitsberichterstattung nach Artikel 28a und zur Beobachtung der Einhaltung dieser Richtlinie und anderer geltender rechtlicher Anforderungen im Hinblick auf die Bestätigung der Nachhaltigkeitsberichterstattung von Bedeutung sind.**
- Die Bestätigungsakte wird spätestens 60 Tage nach Unterzeichnung des Prüfungsvermerks über die Nachhaltigkeitsberichterstattung nach Artikel 28a geschlossen.**
- Führt derselbe Abschlussprüfer die Abschlussprüfung des Jahresabschlusses und die Bestätigung der Nachhaltigkeitsberichterstattung durch, so kann die Bestätigungsakte in die Prüfungsakte aufgenommen werden.“**

- (e) **e) Absatz 6 erhält folgende Fassung:**
„Der Abschlussprüfer oder die Prüfungsgesellschaft bewahrt alle etwaigen schriftlichen Beschwerden über die Durchführung der ausgeführten Abschlussprüfungen und über die Durchführung jedes ausgeführten Bestätigungsauftrags hinsichtlich der Nachhaltigkeitsberichterstattung auf.“

- (42) 13. Artikel 25 erhält folgende Fassung:

„Artikel 25

Prüfungs- und Bestätigungshonorare

Die Mitgliedstaaten sorgen für eine angemessene Regelung, die gewährleistet, dass die Honorare für Abschlussprüfungen und die Bestätigung der Nachhaltigkeitsberichterstattung

- a) nicht von der Erbringung zusätzlicher Leistungen für das **Unternehmen, das Gegenstand der Abschlussprüfung oder der Bestätigung der Nachhaltigkeitsberichterstattung ist**, beeinflusst oder bestimmt werden; und
- b) an keinerlei Bedingungen geknüpft werden dürfen.“

(43) 14. folgende Artikel werden eingefügt:

„Artikel 25b

Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis bei der Bestätigung der Nachhaltigkeitsberichterstattung

Die Anforderungen der Artikel 21 bis 24a, die sich auf die Abschlussprüfung beziehen, sind entsprechend auf die Bestätigung der Nachhaltigkeitsberichterstattung anzuwenden.

Artikel 25c

Nichtprüfungsleistungen, die verboten sind, wenn der Abschlussprüfer bei einem Unternehmen von öffentlichem Interesse die Bestätigung der Nachhaltigkeitsberichterstattung durchführt

(1) Der Abschlussprüfer oder die Prüfungsgesellschaft, der bzw. die bei einem Unternehmen von öffentlichem Interesse die Bestätigung der Nachhaltigkeitsberichterstattung durchführt, und jedes Mitglied eines Netzwerks, dem der Abschlussprüfer bzw. die Prüfungsgesellschaft angehört, dürfen weder direkt noch indirekt für das Unternehmen von öffentlichem Interesse, das Gegenstand der Bestätigung der Nachhaltigkeitsberichterstattung ist, dessen Mutterunternehmen oder die von ihm beherrschten Unternehmen in der Union die in Artikel 5 Absatz 1 Unterabsatz 2 Buchstaben b und c sowie Buchstaben e bis k der Verordnung (EU) Nr. 537/2014 genannten verbotenen Nichtprüfungsleistungen erbringen, und zwar

- a) *innerhalb des Zeitraums zwischen dem Beginn des Zeitraums, der Gegenstand der Bestätigung der Nachhaltigkeitsberichterstattung ist, und der Abgabe des Prüfungsvermerks über die Nachhaltigkeitsberichterstattung und*
 - b) *in Bezug auf die in Artikel 5 Absatz 1 Unterabsatz 2 Buchstabe e der Verordnung (EU) Nr. 537/2014 genannten Leistungen innerhalb des Geschäftsjahrs, das dem in Buchstabe a des vorliegenden Absatzes genannten Zeitraum unmittelbar vorausgeht.*
- (2) *Ein Abschlussprüfer oder eine Prüfungsgesellschaft, der bzw. die bei Unternehmen von öffentlichem Interesse die Bestätigung der Nachhaltigkeitsberichterstattung durchführt, und – wenn der Abschlussprüfer bzw. die Prüfungsgesellschaft einem Netzwerk angehört – jedes Mitglied eines solchen Netzwerks dürfen für das Unternehmen von öffentlichem Interesse, dessen Nachhaltigkeitsberichterstattung bestätigt wird, für dessen Mutterunternehmen oder für die von ihm beherrschten Unternehmen andere Leistungen erbringen als die verbotenen Nichtprüfungsleistungen nach Absatz 1 dieses Artikels oder gegebenenfalls als die verbotenen Nichtprüfungsleistungen nach Artikel 5 Absatz 1 Unterabsatz 2 der Verordnung (EU) Nr. 537/2014 oder als die Leistungen, die nach Ansicht von Mitgliedstaaten eine Gefährdung ihrer Unabhängigkeit nach Artikel 5 Absatz 2 dieser Verordnung darstellen könnten, sofern der Prüfungsausschuss nach einer ordnungsgemäßen Beurteilung der Gefährdungen für die Unabhängigkeit und der ergriffenen Schutzmaßnahmen gemäß Artikel 22b dieser Richtlinie seine Zustimmung erteilt hat.*

(3) Wenn ein Mitglied eines Netzwerks, dem der Abschlussprüfer bzw. die Prüfungsgesellschaft, der bzw. die bei einem Unternehmen von öffentlichem Interesse die Bestätigung der Nachhaltigkeitsberichterstattung durchführt, angehört, für ein Unternehmen mit Sitz in einem Drittland, das von dem der Bestätigung der Nachhaltigkeitsberichterstattung unterzogenen Unternehmen von öffentlichem Interesse beherrscht wird, die verbotenen Nichtprüfungsleistungen nach Absatz 1 dieses Artikels erbringt, beurteilt der Abschlussprüfer bzw. die Prüfungsgesellschaft, ob diese Erbringung von Leistungen durch ein Mitglied des Netzwerks seine bzw. ihre Unabhängigkeit beeinträchtigt.

Wird seine bzw. ihre Unabhängigkeit beeinträchtigt, so wendet der Abschlussprüfer bzw. die Prüfungsgesellschaft Schutzmaßnahmen zur Verminderung der durch die Erbringung verbotener Nichtprüfungsleistungen nach Absatz 1 dieses Artikels in einem Drittland hervorgerufenen Gefahren an. Der Abschlussprüfer bzw. die Prüfungsgesellschaft darf die Bestätigung der Nachhaltigkeitsberichterstattung des Unternehmens von öffentlichem Interesse nur dann fortsetzen, wenn er bzw. sie gemäß Artikel 22b begründen kann, dass die Erbringung dieser Leistungen weder seine bzw. ihre fachliche Einschätzung noch den Prüfungsvermerk über die Nachhaltigkeitsberichterstattung beeinträchtigt.

Artikel 25d

Unregelmäßigkeiten

Artikel 7 der Verordnung (EU) Nr. 537/2014 gilt entsprechend für Abschlussprüfer bzw. Prüfungsgesellschaften, die bei Unternehmen von öffentlichem Interesse Bestätigungen der Nachhaltigkeitsberichterstattung durchführen.“

(44) 15. folgender Artikel wird eingefügt:

„Artikel 26a

Standards für die Bestätigung der Nachhaltigkeitsberichterstattung

(1) Die Mitgliedstaaten verpflichten die Abschlussprüfer und Prüfungsgesellschaften, die Bestätigung der Nachhaltigkeitsberichterstattung unter Beachtung der von der Kommission nach Absatz 3 angenommenen Standards für die Bestätigung durchzuführen. ■

(2) Die Mitgliedstaaten **können** nationale Standards, Verfahren oder Anforderungen für die Bestätigung so lange **anwenden**, wie die Kommission keinen Standard für die Bestätigung, der für denselben Bereich gilt, angenommen hat.

Die Mitgliedstaaten teilen der Kommission die nationalen Standards, Verfahren oder Anforderungen für die Bestätigung spätestens drei Monate vor deren Inkrafttreten mit.

- (3) Der Kommission nimmt spätestens am 1. Oktober 2026 delegierte Rechtsakte gemäß Artikel 48a zur Ergänzung dieser Richtlinie an, um Standards für **begrenzte** Prüfungssicherheit für die vom Abschlussprüfer und der Prüfungsgesellschaft oder den Prüfungsgesellschaften für seine bzw. ihre Schlussfolgerungen über die Prüfung der Nachhaltigkeitsberichterstattung durchzuführenden Verfahren, einschließlich Auftragsplanung, Risikoerwägungen und Reaktion auf Risiken, und die Art der in dem Prüfungsvermerk über die **Nachhaltigkeitsberichterstattung** oder gegebenenfalls im Bestätigungsvermerk zu berücksichtigenden Schlussfolgerungen festzulegen. ■

Die Kommission nimmt spätestens am 1. Oktober 2028 delegierte Rechtsakte gemäß Artikel 48a zur Ergänzung dieser Richtlinie an, um nach einer Bewertung, mit der festgestellt werden soll, ob hinreichende Prüfungssicherheit für die Prüfer und für die Unternehmen machbar ist, diese Richtlinie so zu ändern, dass sie Standards für die Erlangung hinreichender Prüfungssicherheit enthält. Unter Berücksichtigung der Ergebnisse dieser Bewertung und wenn es daher angemessen ist, wird in diesen delegierten Rechtsakten das Datum angegeben, ab dem das in Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa genannte Urteil auf einen Auftrag zur Erlangung hinreichender Prüfungssicherheit gestützt werden muss, der auf diesen Standards für die Erlangung hinreichender Prüfungssicherheit beruht.

Die Kommission darf die in den Unterabsätzen 1 und 2 genannten Standards für die Bestätigung nur annehmen, wenn sie

- a) in einem einwandfreien Verfahren mit angemessener öffentlicher Aufsicht und Transparenz erstellt wurden;

- b) bei der jährlichen oder konsolidierten Nachhaltigkeitsberichterstattung zu einem hohen Maß an Glaubwürdigkeit und Qualität beitragen; und
- c) dem Gemeinwohl der Union dienen.“



(45) 16. folgender Artikel wird eingefügt:

„Artikel 27a

Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung

(1) Die Mitgliedstaaten stellen sicher, dass im Falle von Bestätigungsaufträgen in Bezug auf die konsolidierte Nachhaltigkeitsberichterstattung eines Konzerns

- a) der Konzernabschlussprüfer in Bezug auf die konsolidierte Nachhaltigkeitsberichterstattung die volle Verantwortung für den Prüfungsvermerk über die Nachhaltigkeitsberichterstattung nach Artikel 28a trägt;**

- b) *der Konzernabschlussprüfer die von unabhängigen Erbringern von Bestätigungsleistungen, Prüfern aus einem Drittland, Abschlussprüfern, Prüfungsunternehmen aus einem Drittland oder Prüfungsgesellschaften für die Zwecke der Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung durchgeführten Bestätigungstätigkeiten bewertet und die Art, den Zeitplan und das Ausmaß der von diesen Prüfern durchgeführten Arbeit dokumentiert, wozu gegebenenfalls auch die Durchsicht von relevanten Teilen der Bestätigungsunterlagen dieser Prüfer durch den Konzernabschlussprüfer zählt, und*
- c) *der Konzernabschlussprüfer die von unabhängigen Erbringern von Bestätigungsleistungen, Prüfern aus einem Drittland, Abschlussprüfern, Prüfungsunternehmen aus einem Drittland oder Prüfungsgesellschaften für die Zwecke der Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung durchgeführten Bestätigungstätigkeiten überprüft und dokumentiert.*

Die von dem Konzernabschlussprüfer aufbewahrten Unterlagen müssen so beschaffen sein, dass die entsprechende zuständige Behörde die Arbeit des Konzernabschlussprüfers überprüfen kann.

Für die Zwecke von Unterabsatz 1 Buchstabe c dieses Absatzes verlangt der Konzernabschlussprüfer als Voraussetzung dafür, dass er sich auf die Arbeit von unabhängigen Erbringern von Bestätigungsleistungen, Prüfern aus einem Drittland, Abschlussprüfern, Prüfungsunternehmen aus einem Drittland oder Prüfungsgesellschaften stützen kann, dass die betreffenden unabhängigen Erbringer von Bestätigungsleistungen, Prüfer aus einem Drittland, Abschlussprüfer, Prüfungsunternehmen aus einem Drittland oder Prüfungsgesellschaften in die Weitergabe relevanter Unterlagen während der Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung einwilligen.

- (2) *Ist es dem Konzernabschlussprüfer nicht möglich, die Bestimmungen in Absatz 1 Unterabsatz 1 Buchstabe c zu erfüllen, so ergreift er geeignete Maßnahmen und unterrichtet die jeweils zuständige Behörde entsprechend. Solche Maßnahmen umfassen gegebenenfalls zusätzliche Bestätigungstätigkeiten bei dem betreffenden Tochterunternehmen, die entweder direkt oder im Wege einer Auslagerung durchgeführt werden.*

- (3) *Wird der Konzernabschlussprüfer in Bezug auf die Prüfung der konsolidierten Nachhaltigkeitsberichterstattung eines Konzerns einer Qualitätssicherungsprüfung oder Untersuchung unterzogen, so stellt er der zuständigen Behörde auf Verlangen die relevanten ihm vorliegenden Unterlagen zur Verfügung, die die von den betreffenden unabhängigen Erbringern von Bestätigungsleistungen, Prüfern aus einem Drittland, Abschlussprüfern, Prüfungsunternehmen aus einem Drittland oder Prüfungsgesellschaften für die Zwecke der Prüfung der konsolidierten Nachhaltigkeitsberichterstattung durchgeführten Bestätigungstätigkeiten betreffen, wozu auch sämtliche für die Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung relevanten Arbeitspapiere zählen.*

Die zuständige Behörde kann verlangen, dass die jeweils zuständigen Behörden gemäß Artikel 36 zusätzliche Unterlagen zu den von Abschlussprüfern oder Prüfungsgesellschaften für die Zwecke der Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung durchgeführten Bestätigungstätigkeiten zur Verfügung stellen.

Wird die Bestätigung der Nachhaltigkeitsberichterstattung eines Mutter- oder Tochterunternehmens eines Konzerns von einem oder mehreren Prüfern oder Prüfungsunternehmen aus einem Drittland durchgeführt, so kann die zuständige Behörde verlangen, dass die jeweils zuständigen Drittlandsbehörden im Rahmen der Vereinbarung zur Zusammenarbeit zusätzliche Unterlagen zu den von Prüfern oder Prüfungsunternehmen aus einem Drittland durchgeführten Bestätigungstätigkeiten zur Verfügung stellen.

Abweichend von Unterabsatz 3 trägt der Konzernabschlussprüfer für den Fall, dass ein unabhängiger Erbringer von Bestätigungsleistungen, ein oder mehrere Prüfer aus einem Drittland oder ein oder mehrere Prüfungsunternehmen aus einem Drittland, die nicht über eine Vereinbarung zur Zusammenarbeit verfügen, die Bestätigung der Nachhaltigkeitsberichterstattung eines Mutter- oder Tochterunternehmens eines Konzerns durchführen, zudem dafür Sorge, dass – sollte dies verlangt werden – die zusätzlichen Unterlagen zu den von diesem unabhängigen Erbringer von Bestätigungsleistungen, Prüfer oder Prüfungsunternehmen bzw. von diesen unabhängigen Erbringern von Bestätigungsleistungen, Prüfern oder Prüfungsunternehmen aus einem Drittland durchgeführten Bestätigungstätigkeiten samt der für die Bestätigung der konsolidierten Nachhaltigkeitsberichterstattung relevanten Arbeitspapiere ordnungsgemäß ausgehändigt werden. Zur Sicherstellung dieser Aushändigung bewahrt der Konzernabschlussprüfer eine Kopie dieser Unterlagen auf oder vereinbart andernfalls mit dem unabhängigen Erbringer von Bestätigungsleistungen, Prüfer oder Prüfungsunternehmen bzw. den unabhängigen Erbringern von Bestätigungsleistungen, Prüfern oder Prüfungsunternehmen aus einem Drittland, dass auf Antrag unbeschränkter Zugang zu diesen Unterlagen gestattet wird, oder er trifft sonstige geeignete Maßnahmen. Verhindern rechtliche oder andere Hindernisse, dass die die Bestätigung betreffenden Arbeitspapiere aus einem Drittland an den Konzernabschlussprüfer weitergegeben werden können, so müssen die vom Konzernabschlussprüfer aufbewahrten Unterlagen Nachweise dafür enthalten, dass er die geeigneten Verfahren durchgeführt hat, um Zugang zu den Bestätigungsunterlagen zu erhalten, sowie, im Fall anderer als durch die Rechtsvorschriften des betroffenen Drittlands entstandener rechtlicher Hindernisse, Nachweise für das Vorhandensein eines solchen Hindernisses.“

- (46) 17. Artikel 28 Absatz 2 **Buchstabe e erhält folgende Fassung:**
- (a) █
 - (b) „e) enthält **ein Prüfungsurteil** und eine Erklärung, die **jeweils** auf den gemäß **Artikel 34 Absatz 1** Unterabsatz 2 **Buchstaben a und b** der Richtlinie 2013/34/EU im Laufe der Prüfung durchgeführten Arbeiten basieren█“;
 - (c) █

(47) **18. folgender Artikel wird eingefügt:**

(a) **„Artikel 28a**

Prüfungsvermerk zur Nachhaltigkeitsberichterstattung

- (1) **Der oder die Abschlussprüfer bzw. die Prüfungsgesellschaft oder -gesellschaften legt/legen die Ergebnisse der Bestätigung der Nachhaltigkeitsberichterstattung in einem Prüfungsvermerk zur Nachhaltigkeitsberichterstattung dar. Dieser Vermerk wird entsprechend den Anforderungen der von der Kommission mittels nach Artikel 26a Absatz 3 delegierter Rechtsakte angenommenen Standards für die Bestätigung oder bis zum Erlass dieser Standards für die Bestätigung durch die Kommission im Einklang mit den nationalen Standards für die Bestätigung gemäß Artikel 26a Absatz 2 erstellt.**
- (2) **Der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung wird schriftlich abgefasst und**
- a) **nennt das Unternehmen, dessen jährliche oder konsolidierte Nachhaltigkeitsberichterstattung Gegenstand des Bestätigungsauftrags ist; gibt an, ob es sich um eine jährliche oder eine konsolidierte Nachhaltigkeitsberichterstattung handelt und nennt das Datum und den Zeitraum, auf den er sich bezieht; und gibt den Rahmen für die Nachhaltigkeitsberichterstattung an, der bei seiner Aufstellung verwendet wurde;**

- b) enthält eine Beschreibung des Umfangs der Bestätigung der Nachhaltigkeitsberichterstattung, die zumindest Angaben über die Standards für die Bestätigung enthält, nach denen die Bestätigung der Nachhaltigkeitsberichterstattung durchgeführt wurde;*
 - c) enthält das Urteil gemäß Artikel 34 Absatz 1 Unterabsatz 2 Buchstabe aa der Richtlinie 2013/34/EU.*
- (3) Wurde die Bestätigung der Nachhaltigkeitsberichterstattung von mehr als einem Abschlussprüfer oder einer Prüfungsgesellschaft durchgeführt, so einigen sich diese auf die Ergebnisse der Bestätigung der Nachhaltigkeitsberichterstattung und erstellen einen gemeinsamen Bericht und ein gemeinsames Urteil. Bei Uneinigkeit gibt jeder Abschlussprüfer bzw. jede Prüfungsgesellschaft in einem gesonderten Absatz des Prüfungsvermerks zur Nachhaltigkeitsberichterstattung ein eigenes Urteil ab und legt die Gründe für die Uneinigkeit dar.*

(4) Der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung ist vom Abschlussprüfer, der die Bestätigung der Nachhaltigkeitsberichterstattung durchführt, unter Angabe des Datums zu unterzeichnen. Wird die Bestätigung der Nachhaltigkeitsberichterstattung von einer Prüfungsgesellschaft durchgeführt, so wird der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung zumindest von dem Abschlussprüfer oder den Abschlussprüfern, der bzw. die die Bestätigung der Nachhaltigkeitsberichterstattung für die Prüfungsgesellschaft durchgeführt hat bzw. haben, unterzeichnet. Sind mehr als ein Abschlussprüfer oder eine Prüfungsgesellschaft gleichzeitig beauftragt worden, so wird der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung von allen Abschlussprüfern oder zumindest von den Abschlussprüfern, die die Bestätigung der Nachhaltigkeitsberichterstattung für jede Prüfungsgesellschaft durchgeführt haben, unterzeichnet. Unter besonderen Umständen können die Mitgliedstaaten vorsehen, dass diese Unterschrift(en) nicht öffentlich bekannt gemacht werden muss bzw. müssen, weil eine solche Offenlegung zu einer absehbaren und ernst zu nehmenden Gefahr für die persönliche Sicherheit einer Person führen würde.

In jedem Fall müssen die jeweils zuständigen Behörden die Namen der beteiligten Personen kennen.

(5) Die Mitgliedstaaten können verlangen, dass der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung als gesonderter Abschnitt in den Bestätigungsvermerk aufgenommen wird, falls derselbe Abschlussprüfer die Abschlussprüfung des Jahresabschlusses und die Bestätigung der Nachhaltigkeitsberichterstattung durchführt.

- (6) ***Der Bericht des Abschlussprüfers oder der Prüfungsgesellschaft zur konsolidierten Nachhaltigkeitsberichterstattung hat den Anforderungen nach den Absätzen 1 bis 5 zu genügen.“***
- (48) 19. Artikel 29 wird wie folgt geändert:
- (a) a) Absatz 1 Buchstabe d erhält folgende Fassung:
- „d) die Personen, die die Qualitätssicherungsprüfungen durchführen, müssen über eine angemessene fachliche Ausbildung und einschlägige Erfahrungen auf den Gebieten der Abschlussprüfung und Rechnungslegung und ***gegebenenfalls*** der Nachhaltigkeitsberichterstattung und der Bestätigung der Nachhaltigkeitsberichterstattung ***oder anderen nachhaltigkeitsbezogenen Dienstleistungen*** verfügen und darüber hinaus eine spezielle Ausbildung für Qualitätssicherungsprüfungen absolviert haben;“
- (b) b) Absatz 1 Buchstabe f erhält folgende Fassung:
- „f) die Qualitätssicherungsprüfung muss auf der Grundlage angemessener Überprüfungen von ausgewählten Prüfungsakten und ***gegebenenfalls Bestätigungsakten eine Beurteilung der Einhaltung einschlägiger Standards für die Bestätigung und Unabhängigkeitsanforderungen und eine Beurteilung der Quantität und der Qualität von eingesetzten Ressourcen, der berechneten Prüfungshonorare und Honorare für die Bestätigung der Nachhaltigkeitsberichterstattung sowie des internen Qualitätssicherungssystems der Prüfungsgesellschaft umfassen;“***

- (c) c) Absatz 1 Buchstabe h erhält folgende Fassung:
„h) Qualitätssicherungsprüfungen müssen auf der Grundlage einer Risikoanalyse und im Fall von Abschlussprüfern und Prüfungsgesellschaften, die Abschlussprüfungen im Sinne des Artikels 2 Absatz 1 Buchstabe a und gegebenenfalls Bestätigungen der Nachhaltigkeitsberichterstattung durchführen, mindestens alle sechs Jahre stattfinden;“
- (d) d) Absatz 2 Buchstabe a **erhält folgende Fassung:**
„a) Die Qualitätssicherungsprüfer verfügen über eine angemessene fachliche Ausbildung und einschlägige Erfahrungen auf den Gebieten der Abschlussprüfung und Rechnungslegung und **gegebenenfalls** der Nachhaltigkeitsberichterstattung und der Bestätigung der Nachhaltigkeitsberichterstattung oder anderen nachhaltigkeitsbezogenen Dienstleistungen und haben eine spezielle Ausbildung in Qualitätssicherungsprüfungen absolviert.“
- (e) e) **folgender Absatz wird eingefügt:**
„(2a) Die Mitgliedstaaten können Personen, die Qualitätssicherungsprüfungen im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung durchführen, bis zum 31. Dezember 2025 von der Anforderung befreien, über einschlägige Erfahrung auf dem Gebiet der Nachhaltigkeitsberichterstattung und der Bestätigung der Nachhaltigkeitsberichterstattung oder anderer nachhaltigkeitsbezogener Dienstleistungen zu verfügen.“

- (49) 20. Artikel 30 Absätze 1 und 2 erhalten folgende Fassung:
- „(1) Die Mitgliedstaaten sorgen für wirksame Untersuchungen und Sanktionen, um eine unzureichende Durchführung von Abschlussprüfungen und Bestätigung der Nachhaltigkeitsberichterstattung aufzudecken, zu berichtigen und zu verhindern.
- (2) Unbeschadet ihrer zivilrechtlichen Haftungsvorschriften sehen die Mitgliedstaaten wirksame, verhältnismäßige und abschreckende Sanktionen für Abschlussprüfer und Prüfungsgesellschaften vor, die sich bei der Durchführung von Abschlussprüfungen oder Bestätigungen der Nachhaltigkeitsberichterstattung nicht an die Vorschriften halten, die zur Umsetzung dieser Richtlinie und gegebenenfalls der Verordnung (EU) Nr. 537/2014 angenommen wurden.
- Die Mitgliedstaaten können beschließen, für Verstöße, die bereits dem einzelstaatlichen Strafrecht unterliegen, keine Vorschriften für verwaltungsrechtliche Sanktionen festzulegen. In diesem Fall teilen sie der Kommission die einschlägigen strafrechtlichen Vorschriften mit.“

- (50) 21. *in Artikel 30a Absatz 1 wird folgender Buchstabe eingefügt:*
„ca) ein dem Abschlussprüfer, der Prüfungsgesellschaft oder dem verantwortlichen Nachhaltigkeitspartner auferlegtes vorübergehendes Verbot der Durchführung von Bestätigungen der Nachhaltigkeitsberichterstattung und/oder der Unterzeichnung von Prüfungsvermerken zur Nachhaltigkeitsberichterstattung von bis zu drei Jahren;“
- (51) 22. *in Artikel 30a Absatz 1 wird folgender Buchstabe eingefügt:*
„da) eine Erklärung, dass der Prüfungsvermerk zur Nachhaltigkeitsberichterstattung nicht die Anforderungen des Artikels 28a dieser Richtlinie erfüllt;“
- (52) **I**

(53) 23. Artikel 32 wird wie folgt geändert:

a) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Die zuständige Behörde wird von Nichtberufsausübenden geleitet, die in den für Abschlussprüfungen und gegebenenfalls für Bestätigungen der Nachhaltigkeitsberichterstattung relevanten Bereichen über entsprechende Kenntnisse verfügen. Diese Personen werden in einem unabhängigen und transparenten Verfahren ausgewählt.“

b) Absatz 4 Buchstabe b erhält folgende Fassung:

„b) die Annahme von Berufsgrundsätzen, von Standards für die interne Qualitätssicherung von Prüfungsgesellschaften, von Prüfungsstandards sowie von Standards für die Bestätigung der Nachhaltigkeitsberichterstattung zu beaufsichtigen, es sei denn, diese Standards werden von anderen mitgliedstaatlichen Behörden angenommen oder genehmigt;“

(54) 24. folgender Artikel wird eingefügt:

„Artikel 36a

■ Gegenseitige Anerkennung der mitgliedstaatlichen Regelungen für die Bestätigung der Nachhaltigkeitsberichterstattung

Die Anforderungen der Artikel ■ 34 und 36, die sich auf die Abschlussprüfung beziehen, sind entsprechend ■ auf die Bestätigung der Nachhaltigkeitsberichterstattung anzuwenden.“

- (55) 25. Artikel 37 wird wie folgt geändert:
- (56) a) In Absatz 1 wird folgender Unterabsatz angefügt:
„Unterabsatz 1 gilt auch für die Bestellung des Abschlussprüfers oder der Prüfungsgesellschaft zum Zweck der Bestätigung der Nachhaltigkeitsberichterstattung.“
- (57) b) in Absatz 2 wird folgender Unterabsatz angefügt:
„Unterabsatz 1 gilt auch für die Bestellung des Abschlussprüfers oder der Prüfungsgesellschaft zum Zweck der Bestätigung der Nachhaltigkeitsberichterstattung.“

(58) c) *Absatz 3 erhält folgende Fassung:*

„(3) Jegliche Vertragsklausel, die die Auswahlmöglichkeiten der Gesellschafterversammlung oder der Aktionärshauptversammlung des geprüften Unternehmens gemäß Absatz 1 in Bezug auf Ernennung eines Abschlussprüfers oder einer Prüfungsgesellschaft zur Durchführung der Abschlussprüfung und gegebenenfalls der Bestätigung der Nachhaltigkeitsberichterstattung bei diesem Unternehmen auf bestimmte Kategorien oder Listen von Abschlussprüfern oder Prüfungsgesellschaften beschränkt, ist untersagt. Jede bestehende Klausel dieser Art ist nichtig.

Die Mitgliedstaaten sorgen dafür, dass Aktionäre oder Gesellschafter großer Unternehmen, für die die Artikel 19a und 29a der Richtlinie 2013/34/EU gelten, ausgenommen in Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie genannte Unternehmen, die mehr als 5 % der Stimmrechte oder 5 % des Kapitals des Unternehmens ausmachen, einzeln oder gemeinsam das Recht haben, Beschlussentwürfe einzureichen, die in der Gesellschafterversammlung oder der Aktionärshauptversammlung anzunehmen sind, in der verlangt wird, dass eine akkreditierte dritte Partei, die nicht zu derselben Prüfungsgesellschaft oder demselben Netzwerk wie der Abschlussprüfer oder die Prüfungsgesellschaft, die die Abschlussprüfung vornimmt, einen Bericht über bestimmte Bestandteile der Nachhaltigkeitsberichterstattung ausarbeitet und dass dieser Bericht der Gesellschafterversammlung bzw. Aktionärshauptversammlung zur Verfügung gestellt wird.“

- (59) 26. Artikel 38 wird wie folgt geändert:
- (60) a) Absatz 1 erhält folgende Fassung:
- „(1) Die Mitgliedstaaten stellen sicher, dass Abschlussprüfer oder Prüfungsgesellschaften nur bei Vorliegen triftiger Gründe abberufen werden können. Meinungsverschiedenheiten über Bilanzierungsmethoden, Prüfverfahren oder gegebenenfalls die Nachhaltigkeitsberichterstattung oder entsprechende Bestätigungsverfahren sind kein triftiger Grund für eine Abberufung.“
- (61) b) in Absatz 2 wird folgender Unterabsatz angefügt:
- (62) „Die Unterrichtungspflicht nach Unterabsatz 1 gilt auch für die Bestätigung der Nachhaltigkeitsberichterstattung.“
- (63) c) in Absatz 3 wird folgender Unterabsatz angefügt:
- (64) „Unterabsatz 1 gilt auch für die Bestätigung der Nachhaltigkeitsberichterstattung.“
- (65) 27. Artikel 39 wird wie folgt geändert:
- a) Folgender Absatz wird eingefügt:
- „(4a) Die Mitgliedstaaten können gestatten, dass die dem Prüfungsausschuss übertragenen Aufgaben im Zusammenhang mit der Nachhaltigkeitsberichterstattung und im Zusammenhang mit der Bestätigung der Nachhaltigkeitsberichterstattung von dem Verwaltungs- oder Aufsichtsorgan in seiner Gesamtheit oder von einem vom Verwaltungs- oder Aufsichtsorgan eigens eingerichteten Gremium wahrgenommen werden.“

b) Absatz 6 Buchstaben a bis e erhalten folgende Fassung:

- „a) das Verwaltungs- oder Aufsichtsorgan des geprüften Unternehmens über das Ergebnis der Abschlussprüfung und **gegebenenfalls** das Ergebnis der Bestätigung der Nachhaltigkeitsberichterstattung zu unterrichten und darzulegen, wie die Abschlussprüfung und die Bestätigung der Nachhaltigkeitsberichterstattung zur Integrität der Rechnungslegung **bzw. der** Nachhaltigkeitsberichterstattung beigetragen haben und welche Rolle der Prüfungsausschuss in diesem Prozess gespielt hat;
- b) den Rechnungslegungsprozess und **gegebenenfalls** der Nachhaltigkeitsberichterstattungsprozess, einschließlich des Prozesses der elektronischen Berichterstattung nach Artikel **29d der Richtlinie 2013/34/EU** und des vom Unternehmen durchgeführten Prozesses zur Ermittlung der Informationen, über die Bericht erstattet wurde, im Einklang mit den nach Artikel **29b** der genannten Richtlinie angenommenen Standards für die Nachhaltigkeitsberichterstattung, zu beobachten und Empfehlungen oder Vorschläge zur Gewährleistung ihrer Integrität zu unterbreiten;
- c) die Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems sowie gegebenenfalls der internen Revision des Unternehmens, die die Rechnungslegung und **gegebenenfalls** die Nachhaltigkeitsberichterstattung des Unternehmens berühren, einschließlich des Prozesses der elektronischen Berichterstattung nach Artikel **29d der Richtlinie 2013/34/EU**, zu beobachten, ohne dass seine Unabhängigkeit verletzt wird;

- d) die Abschlussprüfung des Jahresabschlusses und des konsolidierten Abschlusses und **gegebenenfalls** die Bestätigung der jährlichen und konsolidierten Nachhaltigkeitsberichterstattung zu beobachten, insbesondere deren Leistung unter Berücksichtigung der Erkenntnisse und Schlussfolgerungen der zuständigen Behörde nach Artikel 26 Absatz 6 der Verordnung (EU) Nr. 537/2014;
- e) die Unabhängigkeit der Abschlussprüfer oder Prüfungsgesellschaften gemäß den Artikeln 22, 22a, 22b, 24a, 24b, 25b, **25c und 25d** dieser Richtlinie sowie **gemäß** Artikel 6 der Verordnung (EU) Nr. 537/2014 und insbesondere die Angemessenheit der für das geprüfte Unternehmen erbrachten Nichtprüfungsleistungen gemäß Artikel 5 jener Verordnung zu überprüfen und zu beobachten;“

- (66) 28. Artikel 45 wird wie folgt geändert:
- (a) a) Absatz 1 erhält folgende Fassung:
- „(1) Die zuständigen Behörden eines Mitgliedstaats registrieren gemäß den Artikeln 15, 16 und 17 der vorliegenden Richtlinie alle Prüfer und Prüfungsunternehmen aus Drittländern, wenn diese Prüfer oder Prüfungsunternehmen aus Drittländern einen Bestätigungsvermerk zu dem Jahresabschluss oder konsolidierten Abschluss **oder** gegebenenfalls **einen Prüfungsvermerk** zur jährlichen oder konsolidierten Nachhaltigkeitsberichterstattung eines Unternehmens mit Sitz außerhalb der Union erteilen, dessen übertragbare Wertpapiere zum Handel an einem geregelten Markt dieses Mitgliedstaats im Sinne von Artikel 4 Absatz 1 Nummer 21 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates* zugelassen sind, es sei denn, das Unternehmen ist ein Emittent ausschließlich ausstehender Schuldtitel, die eines der folgenden Merkmale aufweisen:
- a) Diese Titel wurden vor dem 31. Dezember 2010 zum Handel an einem geregelten Markt in einem Mitgliedstaat im Sinne von Artikel 4 Absatz 1 Nummer 21 der Richtlinie 2014/65/EU mit einer Mindeststückelung von 50 000 EUR am Ausgabetag oder, wenn es sich um Schuldtitel handelt, die auf eine andere Währung als Euro lauten, mit einer Mindeststückelung, deren Wert am Ausgabetag mindestens 50 000 EUR entspricht, zugelassen.

- b) Diese Titel wurden ab dem 31. Dezember 2010 zum Handel an einem geregelten Markt in einem Mitgliedstaat im Sinne von Artikel 4 Absatz 1 Nummer 21 der Richtlinie 2014/65/EU mit einer Mindeststückelung von 100 000 EUR am Ausgabetag oder, wenn es sich um Schuldtitel handelt, die auf eine andere Währung als Euro lauten, mit einer Mindeststückelung, deren Wert am Ausgabetag mindestens 100 000 EUR entspricht, zugelassen.

* 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).“

- (b) **b) die Absätze 4 bis 6 erhalten folgende Fassung:**
„(4) Unbeschadet des Artikels 46 haben Bestätigungsvermerke zu Jahresabschlüssen oder konsolidierten Abschlüssen oder gegebenenfalls Prüfungsvermerke zu jährlicher oder konsolidierter Nachhaltigkeitsberichterstattung nach Absatz 1 des vorliegenden Artikels, die von in dem Mitgliedstaat nicht registrierten Prüfern oder Prüfungsunternehmen aus Drittländern erteilt werden, in diesem Mitgliedstaat keinerlei Rechtswirkung.

- (5) *Ein Mitgliedstaat kann ein Prüfungsunternehmen aus einem Drittland zum Zweck der Abschlussprüfung nur registrieren, wenn*
- a) *die Mehrheit der Mitglieder des Verwaltungs- bzw. Leitungsorgans des Prüfungsunternehmens aus einem Drittland Voraussetzungen erfüllt, die den Vorgaben der Artikel 4 bis 10 – mit Ausnahme von Artikel 7 Absatz 2, Artikel 8 Absatz 3 und Artikel 10 Absatz 1 Unterabsatz 2 – gleichwertig sind;*
 - b) *der Prüfer aus einem Drittland, der die Prüfung im Auftrag des Prüfungsunternehmens aus einem Drittland durchführt, Voraussetzungen erfüllt, die den Vorgaben der Artikel 4 bis 10 – mit Ausnahme von Artikel 7 Absatz 2, Artikel 8 Absatz 3 und Artikel 10 Absatz 1 Unterabsatz 2 – gleichwertig sind;*
 - c) *die Prüfungen des Jahresabschlusses bzw. konsolidierten Abschlusses nach Absatz 1 dieses Artikels in Übereinstimmung mit den internationalen Prüfungsstandards gemäß Artikel 26 und den in den Artikeln 22, 22b und 25 niedergelegten Anforderungen oder gleichwertigen Standards und Anforderungen durchgeführt werden;*

- d) *das Prüfungsunternehmen aus einem Drittland auf seiner Website einen jährlichen Transparenzbericht veröffentlicht, der die in Artikel 13 der Verordnung (EU) Nr. 537/2014 genannten Informationen enthält, oder gleichwertige Anforderungen an die Offenlegung erfüllt.*

Ein Mitgliedstaat kann ein Prüfungsunternehmen aus einem Drittland zum Zweck der Bestätigung der Nachhaltigkeitsberichterstattung nur registrieren, wenn

- a) *die Mehrheit der Mitglieder des Verwaltungs- bzw. Leitungsorgans des Prüfungsunternehmens aus einem Drittland Voraussetzungen erfüllt, die den Vorgaben der Artikel 4 bis 10 gleichwertig sind;*
- b) *der Prüfer aus einem Drittland, der die Bestätigung im Auftrag des Prüfungsunternehmens aus einem Drittland durchführt, Voraussetzungen erfüllt, die den Vorgaben der Artikel 4 bis 10 gleichwertig sind;*

- c) *die Bestätigung der jährlichen oder konsolidierten Nachhaltigkeitsberichterstattung nach Absatz 1 in Übereinstimmung mit den Standards für die Bestätigung gemäß Artikel 26a und den in den Artikeln 22, 22b, 25 und 25b niedergelegten Anforderungen oder gleichwertigen Standards und Anforderungen durchgeführt wird;*
 - d) *das Prüfungsunternehmen aus einem Drittland auf seiner Website einen jährlichen Transparenzbericht veröffentlicht, der die in Artikel 13 der Verordnung (EU) Nr. 537/2014 genannten Informationen enthält, oder gleichwertige Anforderungen an die Offenlegung erfüllt.*
- (5a) Ein Mitgliedstaat darf einen Prüfer aus einem Drittland **zum Zweck der Abschlussprüfung** nur registrieren, wenn er die Anforderungen nach Absatz 5 **Unterabsatz 1 Buchstaben b, c und d dieses Artikels** erfüllt.
- Ein Mitgliedstaat darf einen Prüfer aus einem Drittland zum Zweck der Bestätigung der Nachhaltigkeitsberichterstattung nur registrieren, wenn er die Anforderungen nach Absatz 5 Unterabsatz 2 Buchstaben b, c und d dieses Artikels erfüllt.*

(6) *Um einheitliche Bedingungen für die Anwendung von Absatz 5 Unterabsatz 1 Buchstabe c und Absatz 5 Unterabsatz 2 Buchstabe c dieses Artikels zu gewährleisten, wird die Kommission ermächtigt, über die darin genannte Gleichwertigkeit im Wege von Durchführungsrechtsakten zu entscheiden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.*

Bis zu einer solchen Entscheidung der Kommission können die Mitgliedstaaten die Gleichwertigkeit im Sinne von Absatz 5 Unterabsatz 1 Buchstabe c und Absatz 5 Unterabsatz 2 Buchstabe c dieses Artikels selbst beurteilen.

Die Kommission wird zum Erlass delegierter Rechtsakte gemäß Artikel 48a zur Ergänzung dieser Richtlinie ermächtigt, um allgemeine Kriterien für die Beurteilung der Gleichwertigkeit festzulegen, die bei der Beurteilung der Frage heranzuziehen sind, ob die Abschlussprüfungen und gegebenenfalls die Bestätigungen der Nachhaltigkeitsberichterstattung nach Absatz 1 im Einklang mit den internationalen Prüfungsstandards nach Artikel 26 bzw. den Standards für die Bestätigung der Nachhaltigkeitsberichterstattung entsprechend der Definition in Artikel 26a und den in den Artikeln 22, 24 und 25 niedergelegten Anforderungen durchgeführt wurden. Die Mitgliedstaaten ziehen bei der Beurteilung der Gleichwertigkeit auf nationaler Ebene diese für alle Drittländer geltenden Kriterien heran.“

- (67) 29. Artikel 48a wird wie folgt geändert:
- (a) a) In Absatz 2 wird folgender Unterabsatz angefügt:
„Die Befugnis zum Erlass der in Artikel 26a Absatz 2 genannten delegierten Rechtsakte wird der Kommission auf unbestimmte Zeit übertragen.“
- (b) b) Absatz 3 erhält folgende Fassung:
„(3) Die Befugnisübertragung gemäß Artikel 26 Absatz 3, Artikel 26a Absatz 3, Artikel 45 Absatz 6, Artikel 46 Absatz 2 und Artikel 47 Absatz 3 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.“
- (c) c) Absatz 5 erhält folgende Fassung:
„(5) Ein delegierter Rechtsakt, der gemäß Artikel 26 Absatz 3, Artikel 26a Absatz 3, Artikel 45 Absatz 6, Artikel 46 Absatz 2 oder Artikel 47 Absatz 3 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von vier 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 4

Änderung der Verordnung (EU) Nr. 537/2014

Die Verordnung (EU) Nr. 537/2014 wird wie folgt geändert:

1. Artikel 4 Absatz 2 Unterabsatz 2 erhält folgende Fassung:

„Bestätigungen der Nachhaltigkeitsberichterstattung und andere als die in Artikel 5 Absatz 1 genannten Nichtprüfungsleistungen, die nach Unionsrecht oder nationalem Recht erforderlich sind, sind für die Zwecke der in Unterabsatz 1 des vorliegenden Absatzes genannten Beschränkungen ausgenommen.“

2. Artikel 5 wird wie folgt geändert:

a) Absatz 1 Unterabsatz 2 Buchstabe c erhält folgende Fassung:

„c) Buchhaltung und Erstellung von Unterlagen der Rechnungslegung und von Abschlüssen sowie Erstellung von Nachhaltigkeitsberichterstattung;“

b) in Absatz 4 wird nach Unterabsatz 1 folgender Unterabsatz eingefügt:

„Die Billigung des Prüfungsausschusses nach Unterabsatz 1 ist für die Durchführung von Bestätigungen der Nachhaltigkeitsberichterstattung nicht erforderlich.“

I

Artikel 5

Umsetzung

- (1) Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um den Artikeln 1 bis 3 dieser Richtlinie spätestens bis zum ... **[18 Monate nach dem Inkrafttreten dieser Richtlinie]** nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit.
- (2) Die Mitgliedstaaten wenden die **erforderlichen Vorschriften an, um Artikel 1, mit Ausnahme von Nummer 14, nachzukommen:**
 - a) **auf am oder nach dem 1. Januar 2024 beginnende Geschäftsjahre**
 - i) **für große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU, bei denen es sich um Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 der genannten Richtlinie handelt und die am Bilanzstichtag die durchschnittliche Zahl von 500 während des Geschäftsjahres Beschäftigten überschreiten;**
 - ii) **für Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 der Richtlinie 2013/34/EU, bei denen es sich um Mutterunternehmen einer großen Gruppe im Sinne von Artikel 3 Absatz 7 der genannten Richtlinie handelt und die am Bilanzstichtag auf konsolidierter Basis die durchschnittliche Zahl von 500 während des Geschäftsjahres Beschäftigten überschreiten;**

- b) *auf am oder nach dem 1. Januar 2025 beginnende Geschäftsjahre*
 - i) *für große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU, die nicht unter Buchstabe a Ziffer i dieses Unterabsatzes fallen;*
 - ii) *für Mutterunternehmen einer großen Gruppe im Sinne von Artikel 3 Absatz 7 der Richtlinie 2013/34/EU, die nicht unter Buchstabe a Ziffer ii dieses Unterabsatzes fallen;*
- c) *auf am oder nach dem 1. Januar 2026 beginnende Geschäftsjahre*
 - i) *für kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der Richtlinie 2013/34/EU, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie sind und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der genannten Richtlinie handelt;*
 - ii) *für kleine und nicht komplexe Institute gemäß der Definition in Artikel 4 Absatz 1 Nummer 145 der Verordnung (EU) Nr. 575/2013, sofern sie große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU sind oder kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der genannten Richtlinie sind, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie sind und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der genannten Richtlinie handelt;*

- iii) für firmeneigene Versicherungsunternehmen gemäß der Definition in Artikel 13 Nummer 2 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates⁷⁴, und firmeneigene Rückversicherungsunternehmen gemäß der Definition in Artikel 13 Nummer 5 der genannten Richtlinie, sofern es sich um große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU handelt oder es sich um kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der genannten Richtlinie handelt, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie sind und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der genannten Richtlinie handelt.

Auf am oder nach dem 1. Januar 2028 beginnende Geschäftsjahre wenden die Mitgliedstaaten die erforderlichen Vorschriften an, um Artikel 1 Absatz 14 nachzukommen.

Die Mitgliedstaaten wenden die erforderlichen Vorschriften an, um Artikel 2 nachzukommen:

- a) auf am oder nach dem 1. Januar 2024 beginnende Geschäftsjahre
- i) für Emittenten im Sinne von Artikel 2 Absatz 1 Buchstabe d der Richtlinie 2004/109/EG, bei denen es sich um große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU handelt und die am Bilanzstichtag die durchschnittliche Zahl von 500 während des Geschäftsjahres Beschäftigten überschreiten;
 - ii) für Emittenten im Sinne von Artikel 2 Absatz 1 Buchstabe d der Richtlinie 2004/109/EG, bei denen es sich um Mutterunternehmen einer großen Gruppe im Sinne von Artikel 3 Absatz 7 der Richtlinie 2013/34/EU handelt und die am Bilanzstichtag auf konsolidierter Basis die durchschnittliche Zahl von 500 während des Geschäftsjahres Beschäftigten überschreiten;

⁷⁴

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).

- b) *auf am oder nach dem 1. Januar 2025 beginnende Geschäftsjahre*
- i) *für Emittenten im Sinne von Artikel 2 Absatz 1 Buchstabe d der Richtlinie 2004/109/EG, bei denen es sich um große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU handelt und die nicht unter Buchstabe a Ziffer i dieses Unterabsatzes fallen;*
 - ii) *für Emittenten im Sinne von Artikel 2 Absatz 1 Buchstabe d der Richtlinie 2004/109/EG, bei denen es sich um Mutterunternehmen einer großen Gruppe im Sinne von Artikel 3 Absatz 7 der Richtlinie 2013/34/EU handelt und die nicht unter Buchstabe a Ziffer ii dieses Unterabsatzes fallen;*
- c) *auf am oder nach dem 1. Januar 2026 beginnende Geschäftsjahre*
- i) *für Emittenten im Sinne von Artikel 2 Absatz 1 Buchstabe d der Richtlinie 2004/109/EG, die kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der Richtlinie 2013/34/EU und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der Richtlinie 2013/34/EU handelt;*
 - ii) *für in Artikel 4 Absatz 1 Nummer 145 der Verordnung (EU) Nr. 575/2013 als kleine und nicht komplexe Institute definierte Emittenten, sofern es sich um große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU handelt oder es sich um kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der genannten Richtlinie handelt, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie sind und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der genannten Richtlinie handelt;*

iii) für in Artikel 13 Nummer 2 der Richtlinie 2009/138/EG als firmeneigene Versicherungsunternehmen oder in Artikel 13 Nummer 5 der genannten Richtlinie als firmeneigene Rückversicherungsunternehmen definierte Emittenten, sofern es sich um große Unternehmen im Sinne von Artikel 3 Absatz 4 der Richtlinie 2013/34/EU handelt oder es sich um kleine und mittlere Unternehmen im Sinne von Artikel 3 Absätze 2 und 3 der genannten Richtlinie handelt, die Unternehmen von öffentlichem Interesse im Sinne von Artikel 2 Nummer 1 Buchstabe a der genannten Richtlinie sind und bei denen es sich nicht um Kleinstunternehmen im Sinne von Artikel 3 Absatz 1 der genannten Richtlinie handelt.

Auf am oder nach dem 1. Januar 2024 beginnende Geschäftsjahre wenden die Mitgliedstaaten die erforderlichen Vorschriften an, um Artikel 3 nachzukommen.

- (3) Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in diesen Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf die vorliegende Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.
- (4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 6

Überprüfung und Berichterstattung

- (1) ***Die Kommission legt dem Europäischen Parlament und dem Rat einen Bericht über die Umsetzung dieser Änderungsrichtlinie vor, der unter anderem Folgendes umfasst:***
 - a) eine Bewertung der Erreichung der Ziele dieser Änderungsrichtlinie, einschließlich der Konvergenz der Berichterstattungsverfahren zwischen Mitgliedstaaten;***
 - b) eine Bewertung der Zahl der kleinen und mittleren Unternehmen, die freiwillig die in Artikel 29c der Richtlinie 2013/34/EU genannten Standards für die Nachhaltigkeitsberichterstattung anwenden;***

- c) *eine Bewertung, ob und wie der Anwendungsbereich der durch diese Änderungsrichtlinie geänderten Vorschriften weiter ausgedehnt werden sollte, insbesondere in Bezug auf kleine und mittlere Unternehmen und Drittlandsunternehmen, die ohne ein Tochterunternehmen oder eine Zweigniederlassung im Gebiet der Union unmittelbar im Binnenmarkt der Union tätig sind;*
- d) *eine Bewertung der Anwendung der durch diese Änderungsrichtlinie eingeführten Berichterstattungsanforderungen auf Tochterunternehmen und Zweigniederlassungen von Drittlandsunternehmen, einschließlich einer Bewertung der Zahl der Drittlandsunternehmen, die ein Tochterunternehmen oder eine Zweigniederlassung besitzen, die gemäß Artikel 40a der Richtlinie 2013/34/EU Bericht erstattet; eine Bewertung des Durchsetzungsmechanismus und der in dem genannten Artikel festgelegten Schwellenwerte;*
- e) *eine Bewertung, ob und wie die Barrierefreiheit der Nachhaltigkeitsberichte, die von in den Anwendungsbereich dieser Änderungsrichtlinie fallenden Unternehmen veröffentlicht werden, für Menschen mit Behinderungen sichergestellt werden kann.*

Der Bericht wird bis zum 30. April 2029 und danach alle drei Jahre veröffentlicht und gegebenenfalls durch Legislativvorschläge ergänzt.

- (2) *Bis zum 31. Dezember 2028 überprüft die Kommission den Konzentrationsgrad des Marktes für die Bestätigung der Nachhaltigkeitsprüfung und erstattet darüber Bericht. Bei der Überprüfung werden die für unabhängige Erbringer von Bestätigungsleistungen geltenden nationalen Regelungen berücksichtigt, und es wird bewertet, ob und inwieweit die genannten nationalen Regelungen zur Öffnung des Marktes für Bestätigungsleistungen beitragen.*

Bis zum 31. Dezember 2028 prüft die Kommission mögliche rechtliche Maßnahmen, um eine ausreichende Diversifizierung des Marktes für die Bestätigung der Nachhaltigkeitsprüfung und eine angemessene Qualität der Nachhaltigkeitsberichterstattung zu gewährleisten. Die Kommission überprüft die in Artikel 34 der Richtlinie 2013/34/EU genannten Maßnahmen und bewertet, ob sie auf weitere große Unternehmen ausgeweitet werden müssen.

Der Bericht wird dem Europäischen Parlament und dem Rat bis zum 31. Dezember 2028 übermittelt und gegebenenfalls durch Legislativvorschläge ergänzt.

Artikel 7
Inkrafttreten und Anwendung

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

Artikel 4 dieser Richtlinie wird ab dem 1. Januar 2024 auf am oder nach dem 1. Januar 2024 beginnende Geschäftsjahre angewandt.

Artikel 8
Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Artikel 4 ist in allen seinen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu ... am ...

Im Namen des Europäischen Parlaments
Die Präsidentin

Im Namen des Rates
Der Präsident/Die Präsidentin



ANGENOMMENE TEXTE

P9_TA(2022)0381

Digitales Finanzwesen: Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 (COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2020)0595),
- gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0304/2020),
- unter Hinweis auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 4. Juni 2021⁷⁵,
- unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 24. Februar 2021⁷⁶,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 29. Juni 2022 gemachte Zusage, den Standpunkt des Parlaments gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,
- gestützt auf Artikel 59 seiner Geschäftsordnung,

⁷⁵ ABl. C 343 vom 26.8.2021, S. 1.

⁷⁶ ABl. C 155 vom 30.4.2021, S. 38.

- unter Hinweis auf den Bericht des Ausschusses für Wirtschaft und Währung (A9-0341/2021),
 1. legt den folgenden Standpunkt in erster Lesung fest;
 2. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend verändert oder beabsichtigt, ihn entscheidend zu verändern;
 3. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 10. November 2022 im Hinblick auf den Erlass der Verordnung (EU) 2022/... des Europäischen Parlaments und des Rates 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) Nr. 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 Zentralbank⁷⁷,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses⁷⁸,

gemäß dem ordentlichen Gesetzgebungsverfahren⁷⁹,

⁷⁷ ABl. C 343 vom 26.8.2021, S. 1.

⁷⁸ ABl. C 155 vom 30.4.2021, S. 38.

⁷⁹ Standpunkt des Europäischen Parlaments 10. November 2022.

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-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 Cyberrisiken¹, 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 Finanzunternehmen² 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 Finanzmärkte³.

- (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 Rates⁸⁰ eingerichtete Europäische Aufsichtsbehörde** (Europäische Bankenaufsichtsbehörde, EBA), die **mit der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates⁸¹ eingerichtete Europäische Aufsichtsbehörde** (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, EIOPA) und die **mit der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates⁸² 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.

⁸⁰ **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).**

⁸¹ **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).**

⁸² **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).**

- (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 kosteneffizienten 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 **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 Rates⁸³ **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) .../... des Europäischen Parlaments und des Rates⁸⁴⁺ 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.**

⁸³ 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).

⁸⁴ **Richtlinie (EU) .../... des Europäischen Parlaments und des Rates vom ... über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L ... vom ..., S. ...).**

⁺ **ABl.: Bitte im Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen sowie in der Fußnote die Nummer, das Datum der Annahme und die Amtsblattfundstelle jener Richtlinie einfügen.**

- (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) .../...**⁺ eine stärkere Harmonisierung dar. Folglich verkörpert diese Verordnung eine *Lex specialis* zur **Richtlinie (EU)**⁺. Es ist **zugleich** von entscheidender Bedeutung, dass eine enge Beziehung zwischen dem Finanzsektor und dem **derzeit in der Richtlinie (EU) .../...**⁺ **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.

+

ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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) .../...**⁺ 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) .../...⁺ benannten oder eingerichteten zuständigen Behörden um fachliche Beratung ersuchen und Kooperationsvereinbarungen schließen können, mit denen wirksame und schnelle Koordinierungsmechanismen sichergestellt werden sollen.**

■

⁺ **ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.**

- (19) *Ange­si­chts der en­gen Ver­flech­ten­gen zwis­chen der digi­ta­len Re­si­li­enz und der phy­si­chen Re­si­li­enz von Fi­nanz­un­ter­neh­men ist in der vor­lie­gen­den Ver­ord­nung und in der Rich­tlinie (EU) .../... des Euro­päi­schen Par­la­ments und des Rates⁸⁵⁺ ein kohä­ren­ter An­satz in Be­zug auf die Re­si­li­enz kri­ti­scher Ein­rich­ten­gen er­for­der­lich. Da das IKT-Risikoma­nage­ment und die Mel­de­pflich­ten nach der vor­lie­gen­den Ver­ord­nung der phy­si­chen Re­si­li­enz von Fi­nanz­un­ter­neh­men um­fas­send Re­ch­nung tra­gen, sol­ten die in den Ka­pi­te­ln III und IV der Rich­tlinie (EU) .../...⁺⁺ fest­ge­leg­ten Ver­pflich­ten­gen 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) .../...⁺⁺⁺ 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 **be­rei­tel­len, und** sol­lte **■** als Ergänz­ung zu der Be­auf­si­chti­gung ge­mäß der **Rich­tlinie (EU) .../...⁺⁺⁺** 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.

⁸⁵ **Rich­tlinie (EU) .../... des Euro­päi­schen Par­la­ments und des Rates über die Re­si­li­enz kri­ti­scher Ein­rich­ten­gen und zur Auf­he­bung der Rich­tlinie 2008/114/EG des Rates (ABl. L ... vom ..., S. ...).**

⁺ **ABl.: Bitte im Text die Nummer der Rich­tlinie in Dok­u­ment PE-CONS 51/22 (2020/0365(COD)) ein­fü­gen sowie in der Fuß­note die Nummer, das Da­tum der Annahme und die Amts­blatt­fund­stelle jener Rich­tlinie ein­fü­gen.**

⁺⁺ **ABl.: Bitte in den Text die Nummer der Rich­tlinie in Dok­u­ment PE-CONS 51/22 (2020/0365(COD)) ein­fü­gen.**

⁺⁺⁺ **ABl.: Bitte in den Text die Nummer der Rich­tlinie in Dok­u­ment PE-CONS 32/22 (2020/0359(COD)) ein­fü­gen.**

- (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 ■ Kleinunternehmen **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 Rates⁸⁶ 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.**

⁸⁶ 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 wachsam, 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 Rates⁸⁷ eingerichtete Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Kooperationsgruppe im Sinne der **Richtlinie (EU) .../...**⁺ 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.

⁸⁷ 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) (OJ L 151 7.6.2019, S. 15).

⁺ **ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS .../22 (2020/0359(COD)) einfügen.**

- (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 Rates⁸⁸ 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.*

⁸⁸ *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).*

- (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) .../...⁺ 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.**

⁺

ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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.**
- (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 Rates⁸⁹ **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.**

⁸⁹ 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 Rates⁹⁰ und Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates 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 der Richtlinie (EU) 2013/36 des Europäischen Parlaments und des Rates⁹¹ 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.*

⁹⁰ 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)

⁹¹ 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).

- (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 Rates⁹², Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates⁹³ und Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt nicht mehr als 15 Versorgungsanwärttern 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.*

⁹² *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).*

⁹³ *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).*

- (41) *Um diese Verordnung an den Anwendungsbereich der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates⁹⁴ 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.*

⁹⁴ *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).*

- (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 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 letzten 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 Rates⁹⁵ 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) .../...⁺ **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

⁹⁵ 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).

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

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-Vorfalles.*
- (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 Rates⁹⁶ 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.*

⁹⁶

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).

- (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 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 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.*

Cyberfälle 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 Rates⁹⁷, 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.*

⁹⁷

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).

- (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 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)../...⁺ 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.*

⁺ **ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.**

- (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).../...⁺ 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*.

⁺ **ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.**

- (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) .../...⁺ 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.*

⁺ **ABL.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.**

- (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 bekanntmachen. 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 des Rates 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 Rechtsetzung⁹⁸ 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.

⁹⁸

ABl. L 123 vom 12.5.2016, S. 1.

- (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.
- (101) Da weitere Anforderungen bereits durch delegierte Rechtsakte und Durchführungsrechtsakte auf der Grundlage technischer Regulierungs- und Durchführungsstandards in den Verordnungen (EG) Nr. 1060/2009⁹⁹, (EU) Nr. 648/2012¹⁰⁰, (EU) Nr. 600/2014¹⁰¹ bzw. (EU) Nr. 909/2014¹⁰² 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

⁹⁹ 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).

¹⁰⁰ **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).**

¹⁰¹ **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).**

¹⁰² **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).**

von delegierten Rechtsakten und Durchführungsrechtsakten zur Übernahme und Aktualisierung bestehender IKT-Risikomanagementvorschriften vorzulegen.

- (102) *Da die vorliegende Verordnung in Verbindung mit der Richtlinie (EU) .../... des Europäischen Parlaments und des Rates¹⁰³⁺⁺ 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) 2016/1011¹⁰⁴ 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.

¹⁰³ *Richtlinie (EU) .../... des Europäischen Parlaments und des Rates vom ... 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 (ABl. L ... vom ..., S...).*

⁺⁺ *ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS .../22 (2020/0268(COD)) einfügen.*

¹⁰⁴ *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).*

(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.*

- (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 Rates¹⁰⁵ konsultiert und hat am 10. Mai 2021 eine Stellungnahme abgegeben¹⁰⁶ —*

HABEN FOLGENDE VERORDNUNG ERLASSEN:

¹⁰⁵ 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).

¹⁰⁶ ABl. C 229 vom 15.6.2021, S. 16.

Kapitel I
Allgemeine Bestimmungen

Artikel 1
Gegenstand

- (1) Um ein hohes gemeinsames Niveau an **digitaler operativer 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 operativen 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) .../...**⁺, 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.**

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS .../22 (2020/0359(COD)) einfügen.

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 Versorgungsanwärttern 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“** Netz- und Informationssystem im Sinne von **Artikel 6 Nummer 1 der Richtlinie .../...⁺**;
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 .../...⁺**;

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

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 des Europäischen Parlaments und des Rates¹⁰⁷;
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;

¹⁰⁷ 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).

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**¹⁰⁸, 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 Rates¹⁰⁹;

¹⁰⁸ 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).

¹⁰⁹ 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).

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 Rates¹¹⁰ 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 des Europäischen Parlaments und des Rates;*

¹¹⁰ 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).

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;
49. „Versicherungsvermittler“ einen Versicherungsvermittler im Sinne von Artikel 2 **Absatz 1** Nummer 3 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates¹¹¹;
50. „Versicherungsvermittler in Nebentätigkeit“ einen Versicherungsvermittler in Nebentätigkeit im Sinne von Artikel 2 **Absatz 1** Nummer 4 der Richtlinie (EU) 2016/97;

¹¹¹ 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).

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 Versorgungsanwärttern betreibt;*
54. „Ratingagentur“ eine Ratingagentur im Sinne von Artikel 3 Absatz 1 Buchstabe a 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**¹¹²;
59. „Verbriefungsregister“ ein Verbriefungsregister im Sinne von Artikel 2 Nummer 23 der Verordnung (EU) 2017/2402 **des Europäischen Parlaments und des Rates**¹¹³;
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**;

¹¹² 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).

¹¹³ 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).

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.*

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 Kleinunternehmen 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**.

- I
- (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 Revisions**funktionen** 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 Auswirkungstoleranz 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 Kleinunternehmen 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-Sicherheits**richtlinien**, -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 Kleinunternehmen 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 ... [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung] 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 Betriebsstabilität digitaler Systeme 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;
- I**
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 ... [12 Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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 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 ... [12 Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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 ... **[12 Monate** nach dem Tag des Inkrafttretens **dieser Verordnung]**.

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 Artikel [X] der Richtlinie (EU).../...⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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) .../...⁺ benannten oder eingerichteten CSIRT erstatten können.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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 Unterabsatz 1 Buchstabe a Nummer 2 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 Artikel [X] der Richtlinie (EU) .../...⁺ benannt oder eingerichtet werden;**

⁺ AB1.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

- d) *die in Artikel 3 der Richtlinie Nr. 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 Rates¹¹⁴ 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.*

¹¹⁴ 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 Unterabsatzes Buchstabe a Nummer 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) .../...⁺. 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**.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

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 ... [**18 Monate** nach dem Tag des Inkrafttretens **dieser Verordnung**].

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 der Kommission, dem Europäischen Parlament und dem Rat den in Absatz 1 genannten Bericht bis zum ... [**24 Monate** nach dem Tag des Inkrafttretens **dieser Verordnung**].

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) .../...⁺ 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.***

⁺ AB1.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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 Kleinunternehmen 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 ... [**18** Monate **nach** dem Tag des **Inkrafttretens dieser Verordnung**].

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 Buchstabe g 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 ... [**12 Monate** nach dem Tag des Inkrafttretens dieser Verordnung].

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 ... [**12 Monate** nach dem Tag des **Inkrafttretens dieser Verordnung**].

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 Kleinunternehmen 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 ... [**18 Monate** nach dem Tag des Inkrafttretens **dieser Verordnung**].

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 Buchstabe 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 ... [18 Monate nach** dem Tag des **Inkrafttretens dieser Verordnung]** 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 Artikel [X] der Richtlinie (EU) .../...⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS .../22 (2020/0359(COD)) einfügen.

- (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 ... [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung]** 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) .../...**⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

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 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).../...⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

- (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:*
- i) Schwere und Dauer der Nichteinhaltung;*
 - ii) ob die Nichteinhaltung vorsätzlich oder fahrlässig begangen wurde;*

iii) 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 unterworfenen 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 sekundären 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 nationalen 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 bereitgestellt 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 ... **[18 Monate nach dem Tag des Inkrafttretens dieser Verordnung]** 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 Artikel [8] der Richtlinie (EU) .../...⁺ 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.*

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument PE-CONS 32/22 (2020/0359(COD)) einfügen.

- (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) .../...⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

- (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 ... [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung]** 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**¹¹⁵ 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;

¹¹⁵ 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).

- 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;
- 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) .../...**⁺ 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) .../...**⁺ 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) .../...**⁺ 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) .../...**⁺ benannten oder eingerichteten CSIRT wenden **und mit ihnen Informationen austauschen.**

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

- (3) *Die zuständigen Behörden können gegebenenfalls die gemäß der Richtlinie (EU) .../...⁺ 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) .../...⁺ 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.*

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

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 Nr. 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 abzuweichen 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 ... [24 Monate nach Tag des dem Inkrafttretens **dieser Verordnung**] 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) .../...⁺ 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.

⁺ ABl.: Bitte in den Text die Nummer der Richtlinie in Dokument **PE-CONS 32/22 (2020/0359(COD))** einfügen.

- (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, Auskunftersuchen, 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 ... [12 Monate nach dem Tag des Inkrafttretens dieser Verordnung] 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 ... [] fünf Jahre nach dem Tag des Inkrafttretens dieser Verordnung [] 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 Buchstaben 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 ... [sechs Monate nach dem Tag des Inkrafttretens dieser Verordnung] 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 Absatz 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 ... [drei Jahre nach dem Tag des Inkrafttretens dieser Verordnung] 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 Rates¹¹⁶ geändert wird.*

¹¹⁶

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, 9.6.2006, p.87)

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) .../...** des Europäischen Parlaments und des Rates⁺.“

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom...] 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) Nr. 2016/1011 (ABl. L ..., TT.MM.JJJJ, S. ...).“

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) .../...⁺⁺ verfügt oder wenn sie keine Entscheidungsprozesse oder keine Organisationsstruktur nach Maßgabe jener Nummer schafft oder unterhält.“

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum, Titel und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

⁺⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

Artikel 60

Änderungen der Verordnung (EG) 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) .../...** des Europäischen Parlaments und des Rates^{*+} betrieben werden.

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom...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) Nr. 2016/1011 (ABl. L ..., TT.MM.JJJJ, S. ...).“

b) Absatz 6 wird gestrichen;

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum, Titel und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

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) .../...** ⁺ **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.“

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../...⁺ 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) .../...⁺ 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;

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../...⁺ 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) .../...⁺ 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;*

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../...⁺ (DORA) betrieben werden;“

ii) *wird Buchstabe f 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) .../...⁺ 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;“

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

Artikel 61

Änderungen der Verordnung (EG) 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) .../... 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/xx des Europäischen Parlaments und des Rates vom...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) Nr. 2016/1011 (ABl. L ..., TT.MM.JJJJ, S. ...).“

2. Absatz 2 wird gestrichen;

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum, Titel und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

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) .../...⁺ 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) .../...⁺ vorgesehen.“

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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 (EG) 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) .../... des Europäischen Parlaments und des Rates*⁺ festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen.“

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom...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) Nr. 2016/1011 (ABl. L ..., TT.MM.JJJJ, S. ...).“

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) .../...⁺⁺ festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen.“

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum, Titel und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

⁺⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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:**

„Ein ARM muss die in der Verordnung (EU) .../...⁺ 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.“

⁺

ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../... des Europäischen Parlaments und des Rates*.“

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom...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) Nr. 2016/1011 (ABl. L ..., TT.MM.JJJJ, S. ...).“

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 ... [24 Monate nach █ Inkrafttreten **dieser Verordnung**].

Diese Verordnung ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu am ...

Im Namen des Europäischen Parlaments
Die Präsidentin

Im Namen des Rates
Der Präsident/Die Präsidentin

⁺ ABl.: Bitte die Nummer der in Dokument PE- CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum, Titel und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.



ANGENOMMENE TEXTE

P9_TA(2022)0382

Digitales Finanzwesen: Änderung der Richtlinie hinsichtlich der Anforderungen an die digitale Betriebsstabilität

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, 2015/2366/EU und (EU) 2016/2341 (COM(2020)0596 – C9-0303/2020 – 2020/0268(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2020)0596),
- gestützt auf Artikel 294 Absatz 2, Artikel 53 Absatz 1 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0303/2020),
- gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 4. Juni 2021¹¹⁷,
- unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 24. Februar 2021¹¹⁸,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 29. Juni 2022 gemachte Zusage, den genannten Standpunkt gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,
- gestützt auf Artikel 59 seiner Geschäftsordnung,

¹¹⁷ ABl. C 343 vom 26.8.2021, S. 1.

¹¹⁸ ABl. C 155 vom 30.4.2021, S. 38.

- unter Hinweis auf die Stellungnahme des Rechtsausschusses,
 - unter Hinweis auf den Bericht des Ausschusses für Wirtschaft und Währung (A9-0340/2021),
1. legt den folgenden Standpunkt in erster Lesung fest,
 2. schlägt vor, den Gesetzgebungsakt „DORA-Richtlinie“ zu nennen,
 3. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern,
 4. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 10. November 2022 im Hinblick auf den Erlass der Richtlinie (EU) 2022/... des Europäischen Parlaments und des Rates 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 Zentralbank¹¹⁹,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses¹²⁰,

gemäß dem ordentlichen Gesetzgebungsverfahren¹²¹,

¹¹⁹ ABl. C 343 vom 26.8.2021, S. 1.

¹²⁰ ABl. C 155 vom 30.4.2021, S. 38.

¹²¹ Standpunkt des Europäischen Parlaments vom 10. November 2022.

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 Potentials des digitalen Finanzwesens leisten, indem Innovationen vorangetrieben 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.

- (3) Auf Unionsebene enthalten derzeit die Richtlinien ■ 2009/65/EG¹²², 2009/138/EG¹²³, 2011/61/EU¹²⁴, 2013/36/EU¹²⁵, **2014/59/EU¹²⁶**, 2014/65/EU¹²⁷, (EU) 2015/2366¹²⁸ und (EU) 2016/2341¹²⁹ 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) .../... des Europäischen Parlaments und des Rates ■ ¹³⁰⁺ behoben. Um die Kohärenz mit der genannten Verordnung zu

¹²² 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).

¹²³ 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).

¹²⁴ 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).

¹²⁵ 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).

¹²⁶ **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).**

¹²⁷ 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).

¹²⁸ 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).

¹²⁹ 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).

¹³⁰ Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).

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 unternehmerischen 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.***

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

- (4) Im Bereich der Bankdienstleistungen enthält die Richtlinie 2013/36/EU ¹³¹ 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 ¹³¹ im Einklang mit den Anforderungen der Verordnung (EU) .../...⁺ ¹³¹ 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 Rates¹³¹ eingerichtet wurden. Um Rechtsklarheit zu schaffen und sicherzustellen, dass die Bankenaufsichtsbehörden 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) .../...⁺ 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.***

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

¹³¹ ***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) *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) .../...⁺ in Einklang gebracht werden.*



⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

- (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) .../...⁺ ■ 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) .../...⁺ 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) .../...⁺ ■ angeglichen werden.

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

- (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) .../...⁺ ■ 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) .../...⁺ ■ 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.

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

- (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 Dokumenten¹³² 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:

¹³²

ABl. C 369 vom 17.12.2011, S. 14.

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) .../... 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) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

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.“

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) .../... des Europäischen Parlaments und des Rates*⁺ [] .

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 [] (ABl. L ... vom ..., S. ...).“

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

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) .../... 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.

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

- (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) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“

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) .../... des Europäischen Parlaments und des Rates*+,

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

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) .../...⁺ eingerichtet und verwaltet werden, sowie eine Vergütungspolitik und -praxis, die mit einem soliden und wirksamen Risikomanagement vereinbar und diesem förderlich sind, zählen.“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ **eingerrichtet, 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) .../...⁺ aufgedeckt werden.**“

⁺

ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../... des Europäischen Parlaments und des Rates^{*,+};

** Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“*

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

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) .../...⁺ 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) .../...⁺ 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) .../...⁺;“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 42/22 (2020/0266(COD)) einfügen.

ii) *Folgende Nummer wird eingefügt:*

„14a. Ergebnisse der von Instituten im Einklang mit der Verordnung (EU) .../...⁺ 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 .../...⁺ durchgeführten Tests der digitalen operationalen Resilienz zu berücksichtigen sind;“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../... 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) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“

⁺ ABl.: Bitte im Text die Nummer der in Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

- 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) .../...⁺ 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.“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ ■ 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.

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

Die Wertpapierfirma verfügt über wirksame Vorkehrungen zur Fortführung der Geschäftstätigkeiten, einschließlich gemäß **Artikel 11** der Verordnung (EU) .../...⁺ 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) .../...⁺ ■ 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;“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

I

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) .../...⁺ **I**, 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;

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ 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) .../...⁺ einschließen**, um im Fall von Störungen in seinen Handelssystemen die Kontinuität seines Geschäftsbetriebs zu gewährleisten.“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ 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.“

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

- 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) .../... des Europäischen Parlaments und des Rates⁺, aus der hervorgeht, dass diese Unternehmenssteuerung und interne Kontrollmechanismen verhältnismäßig, angemessen, zuverlässig und ausreichend sind;*

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 (ABl. L ... vom ..., S. ...).“

+

ABl.: Bitte im Text die Nummer der im Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

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) .../...⁺ 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) .../...⁺;“

⁺

ABL.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../... 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.

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ 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;“**

I

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../...⁺ **■ Rechnung zu tragen.“**

⁺ ABl.: Bitte im Text die Nummer der Verordnung in Dokument PE-CONS 41/22 (2020/0266(COD)) einfügen.

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) .../... des Europäischen Parlaments und des Rates**⁺.

* Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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) Nr. 2016/1011 **■** (ABl. L ... vom ..., S. ...).“

⁺ ABl.: Bitte im Text die Nummer der im Dokument PE-CONS 41/22 2020/0266(COD) enthaltenen Verordnung und in der Fußnote die Nummer, das Datum und die Amtsblattfundstelle der genannten Verordnung einfügen.

Artikel 9

Umsetzung

- (1) Spätestens am ... [24 Monate nach dem Tag des Inkrafttretens dieser Änderungsrichtlinie] 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 ... [24 Monate nach dem Tag des Inkrafttretens **der in Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung**] 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 ... am ...

Im Namen des Europäischen Parlaments

Die Präsidentin

Im Namen des Rates

Der Präsident/Die Präsidentin



ANGENOMMENE TEXTE

P9_TA(2022)0383

Hohes gemeinsames Cybersicherheitsniveau in der Union

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2020)0823),
- gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0422/2020),
- gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 11. April 2022¹³³,
- unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 27. April 2021¹³⁴,
- nach Anhörung des Ausschusses der Regionen,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung vom zuständigen Ausschuss angenommen wurde, und auf die vom Vertreter des Rates mit Schreiben vom 22. Juni 2022 gemachte Zusage, den Standpunkt des Parlaments gemäß Artikel 294 Absatz 4 des Vertrags über die Arbeitsweise der Europäischen Union zu billigen,

¹³³ ABl. C 233 vom 16.6.2022, S. 22.

¹³⁴ ABl. C 286 vom 16.7.2021, S. 170.

- gestützt auf Artikel 59 seiner Geschäftsordnung,
 - unter Hinweis auf die Stellungnahmen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres, des Ausschusses für auswärtige Angelegenheiten, des Ausschusses für Binnenmarkt und Verbraucherschutz sowie des Ausschusses für Verkehr und Tourismus,
 - unter Hinweis auf den Bericht des Ausschusses für Industrie, Forschung und Energie (A9-0313/2021),
1. legt den folgenden Standpunkt in erster Lesung fest;
 2. fordert die Kommission auf, es erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;
 3. beauftragt seinen Präsidenten, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 10. November 2022 im Hinblick auf den Erlass der Richtlinie (EU) 2022/... des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (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 Zentralbank¹³⁵,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses¹³⁶,

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren¹³⁷,

¹³⁵ ABl. C 233 vom 16.6.2022, S. 22.

¹³⁶ ABl. C 286 vom 16.7.2021, S. 170.

¹³⁷ Standpunkt des Europäischen Parlaments vom 10. November 2022.

in Erwägung nachstehender Gründe:

- (1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates¹³⁸ 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.

¹³⁸ 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).

- (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 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 Kommission¹³⁹ 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 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 oder für bestimmte Sektoren oder Arten von Diensten hindeuten, in den Anwendungsbereich dieser Richtlinie fallen.**

¹³⁹

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).

- (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 Rates¹⁴⁰ 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.*

¹⁴⁰

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 Rates¹⁴¹, **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 Netzwerk- 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.*

¹⁴¹ 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 Dienstqualität (ABl. L 15 vom 21.1.1998, S. 14).

(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 Rates¹⁴² und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates¹⁴³ 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.

¹⁴² **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).**

¹⁴³ **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).**

- (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.*
- (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 Domännennamen-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 Domännennamen-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) .../... des Europäischen Parlaments und des Rates¹⁴⁴⁺ 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 .../...⁺⁺ 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 .../...⁺⁺ zulässig, dass die Europäischen Aufsichtsbehörden und die gemäß der Verordnung .../...⁺⁺ zuständigen nationalen Behörden sich an **der Tätigkeit** der Kooperationsgruppe beteiligen und mit den zentralen Anlaufstellen sowie den nationalen CSIRTs und den zuständigen Behörden gemäß dieser Richtlinie Informationen austauschen und zusammenarbeiten. Die gemäß der Verordnung .../...⁺⁺ 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**

¹⁴⁴ Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... 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 (ABl. L ..., vom ..., S. ...).

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

⁺⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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. 300/2008¹⁴⁵ und (EU) 2018/1139¹⁴⁶ 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.*

¹⁴⁵ *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).*

¹⁴⁶ *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).*

- (30) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU)¹⁴⁷⁺ ■ des Europäischen Parlaments und des Rates und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten Einrichtungen, die gemäß der Richtlinie (EU) .../...⁺⁺ 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 Mitgliedstaates** zwischen seinen gemäß der vorliegenden Richtlinie zuständigen **Behörden** und denen gemäß Richtlinie (EU) .../...⁺⁺ 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) .../...⁺⁺ 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) .../...⁺⁺ **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.**

¹⁴⁷ Richtlinie (EU) .../... des Europäischen Parlaments und des Rates vom ... über die Resilienz kritischer Einrichtungen (ABl. L ... vom ..., S. ...).

⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text sowie Nummer, Datum und Amtsblattfundstelle dieser Richtlinie in den Fußnotentext einfügen.

⁺⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

Gegebenenfalls sollten die gemäß der Richtlinie (EU) .../...⁺⁺ 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) .../...⁺⁺ als kritische Einrichtung eingestuft wird, auszuüben. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) .../...⁺⁺ 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, ICV und VI der Richtlinie (EU) .../...⁺ festgelegten Verpflichtungen nicht für solche Einrichtungen.**
- (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-Namensserver gelten.**

⁺ **ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.**

- (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 .../...⁺ zuständigen Behörden entgegennehmen, die **sie** gegebenenfalls gemäß der vorliegenden Richtlinie an die **CSIRTs oder die** zuständigen Behörden ■ weiterleiten können sollten.

⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS .../22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

- (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 Netzwerk- 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 Administratorebene 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 vernetzter oder intelligenter 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 Rates¹⁴⁸ eingeführt wurde, zur Teilnahme an ihrer Arbeit einzuladen.

¹⁴⁸

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).

- (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 Kommission¹⁴⁹ 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 Rates¹⁵⁰ (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.

¹⁴⁹ 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).

¹⁵⁰ **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).**

- (69) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 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.*
- (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 Rates¹⁵¹ 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.*

¹⁵¹ 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).

- (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 eingestufte 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.*

- (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 Netzwerk- 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) .../...⁺ im Einklang stehen.*

⁺

ABl.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

- (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 Rates¹⁵² 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.

¹⁵²

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

- (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.*

- (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 Inhaltzustellnetzen, 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 Kommission¹⁵³ – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln. **Bei solchen koordinierten Riskobewertungen 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.**

¹⁵³ Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

- (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 Netze und Informationssysteme auferlegt werden, und um diese Einrichtungen und die zuständigen Behörden nach der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates¹⁵⁴ 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.

¹⁵⁴ 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).

(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.*

- (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 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, dass 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 Rates¹⁵⁵ 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.*

¹⁵⁵ 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).

- (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.
- (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 Domännennamen-Registrierungsdaten sollten die TLD-Namenregister und Einrichtungen, die Domännennamen-Registrierungsdienste ■, die Integrität und Verfügbarkeit von Domännennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten TLD-Namenregister und Einrichtungen, die Domännennamen-Registrierungsdienste erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit dem Datenschutzrecht der Union genaue und vollständige Domännennamen-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 Domännennamen-Registrierungsdienste erbringen, sollten verhältnismäßige Verfahren für die Überprüfung der Domännennamen-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 Domännennamen-Registrierungsdienste erbringen, sollten insbesondere mindestens eine Kontaktmöglichkeit des Domäneninhabers überprüfen.***

(112) TLD-Namenregister und die Einrichtungen, die Domännennamen-Registrierungsdienste **erbringen**, sollten Domännennamen-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 Domännennamen-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 Domännennamen-Registrierungsdienste **erbringen**, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager rechtmäßigen Zugang zu bestimmten Domännennamen-Registrierungsdaten natürlicher Personen im Einklang mit dem Datenschutzrecht der Union erhalten. Die Mitgliedstaaten sollten TLD-Namenregister und die Einrichtungen, die Domännennamen-Registrierungsdienste **erbringen**, verpflichten, Anträge **auf** Offenlegung von Domännennamen-Registrierungsdaten **von berechtigten Zugangsnachfragern** unverzüglich zu beantworten. TLD-Namenregister und die Einrichtungen, die Domännennamen-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 Domännennamen-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-Dienstanbieter, TLD-Namenregister, Einrichtungen, die Domännennamen-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 Domännennamen-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 Domännennamen-Registrierungsdienste erbringt, ein Anbieter von Cloud-Computing-Diensten, ein Anbieter von Rechenzentren, ein Anbieter von Inhaltzustellnetzen, 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 Inhaltzustellnetzen, 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 eingestufte 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 Haftungs Vorschriften.

- (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 berechnigte 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 der Verordnung (EU) 2016/679. 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 **II**, 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 Rechtsetzung¹⁵⁶ 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.

¹⁵⁶

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 Rates¹⁵⁷ 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 25 der Verordnung (EU) .../... des Europäischen Parlaments und des Rates¹⁵⁸⁺ benannt sind, als wesentliche Einrichtungen im Sinne dieser Richtlinie ermittelt werden könnten.**

¹⁵⁷ 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).

¹⁵⁸ Verordnung (EU)/... des Europäischen Parlaments und des Rates vom ... über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L, ..., S. ...).

⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS 30/22 (2020/0361(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum und Amtsblattfundstelle dieser Verordnung in den Fußnotentext einfügen.

- (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 Rates¹⁵⁹ angehört und hat am 11. März 2021 eine Stellungnahme¹⁶⁰ abgegeben —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

¹⁵⁹ 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).

¹⁶⁰ ***ABl. C 183 vom 11.5.2021, S. 3.***

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) .../...⁺ als kritische Einrichtungen eingestuft wurden;
 - c) **Vorschriften und** Pflichten zum Austausch von Cybersicherheitsinformationen;
 - d) **Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.**

⁺ **ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.**

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 Domänennamenssystem-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) .../...**⁺ 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.

⁺ **ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.**

- (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 5 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 5 und 6 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) .../...⁺ 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.*

⁺ *ABl.: Bitte die Nummer der im Dokument PE-CONS .../22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.*

- (12) Diese Richtlinie gilt unbeschadet der **Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG**, der Richtlinien 2011/93/EU¹⁶¹ und 2013/40/EU¹⁶² des Europäischen Parlaments und des Rates **sowie** der Richtlinie .../...⁺.
- (13) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union oder der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden **im Einklang mit dieser Richtlinie** nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs relevanten und angemessenen Umfang beschränkt. Beim Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der betreffenden kritischen Einrichtungen geschützt.

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

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

¹⁶¹ 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).

¹⁶² 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).

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

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) .../...⁺ 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 ... [Inkrafttreten dieser Richtlinie] 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.*

⁺ **ABl.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.**

- (3) *Bis zum ... [27 Monate nach Inkrafttreten dieser Richtlinie] erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domännennamen-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 ... [27 Monate nach Inkrafttreten dieser Richtlinie] 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 ... [27 Monate nach Inkrafttreten dieser Richtlinie] 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 ... [sechs Monate nach dem Inkrafttreten dieser Richtlinie] 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 Rates¹⁶³;*
17. *„technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012;*

¹⁶³ 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-Namensservern, 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 Namensserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namensserver, 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 Rates¹⁶⁴;
24. **„Vertrauensdienst“ einen Vertrauensdienst im Sinne des Artikels 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;**

¹⁶⁴

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).

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 Rates¹⁶⁵;
29. „Online-Suchmaschine“ eine Online-Suchmaschine im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates¹⁶⁶;
30. „Cloud-Computing-Dienst“ einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer ■ Rechenressourcen ermöglicht, ***auch wenn diese Ressourcen auf mehrere Standorte verteilt sind;***
31. „Rechenzentrumsdienst“ einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;

¹⁶⁵ 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).

¹⁶⁶ 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).

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 Domännennamen-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

KOORDINIERTER 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) .../...⁺ 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;**

⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

- 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 personenbezogene 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 Netze 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) .../...⁺ zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972, den gemäß der Richtlinie (EU) .../...⁺⁺ zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden.***

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

⁺⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

- (5) Die Mitgliedstaaten stellen sicher, dass ihre **im Rahmen dieser Richtlinie** zuständigen Behörden **und ihre** nach der Richtlinie (EU) .../...⁺ 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) .../...⁺ 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) .../...⁺⁺ und der Richtlinie (EU) 2018/1725** 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.**

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

⁺⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../...⁺ zuständigen Behörden** können sich **gemäß Artikel 47 Absatz 1 jener Verordnung** an den Tätigkeiten der Kooperationsgruppe beteiligen.

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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) .../...⁺ eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den ***Informationsaustausch*** zu fördern ***und zu erleichtern*** .

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

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 ... [24 Monate nach Inkrafttreten dieser Richtlinie] 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 ... [18 Monate nach dem Tag des Inkrafttretens dieser Richtlinie] 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 Sektorebene, 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 ... [24 Monate nach Inkrafttreten dieser Richtlinie] **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 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 eingestufteter 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 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 ... [21 Monate nach Inkrafttreten dieser Richtlinie] 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 Inhaltzustellnetzen, 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.

I

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 4 Buchstabe b unterrichtet der 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) .../...⁺ 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) .../...⁺ 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 ... [21 Monate nach Inkrafttreten dieser Richtlinie] erlässt die Kommission in Bezug auf DNS-Dienstanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltzustellnetzen, 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.

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

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 VZUSTÄNDIGKEIT 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 Inhaltzustellnetzen, 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 Domännennamen-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 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 ... [24 Monate nach Inkrafttreten dieser Richtlinie] 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 Domännennamen-Registrierungsdaten

- (1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domännennamensystems zu leisten, **verpflichten** die Mitgliedstaaten, dass die **TLD-Namenregister** und die Einrichtungen, die Domännennamen-Registrierungsdienste **erbringen**, genaue und vollständige Domännennamen-Registrierungsdaten in einer eigenen Datenbank **im Einklang mit dem** Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen **erbringen**.
- (2) **Für die Zwecke des Absatzes 1 schreiben** die Mitgliedstaaten **vor**, dass die **Datenbank** der Domännennamen-Registrierungsdaten die **erforderlichen** Angaben enthält, anhand derer die Inhaber der Domännennamen und die Kontaktstellen, die die Domännennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. **Diese Informationen müssen Folgendes umfassen:**
 - a) **den Domännennamen;**
 - 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 Domännennamen 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 Durchsetzungsmaßnahmen bei 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 28 **■** ;
- 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 abzuweichen;

- d) die betreffenden Einrichtungen anzuweisen, entsprechend bestimmter 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 bestimmter Vorgaben öffentlich bekannt zu machen;

I

i) **gemäß einzelstaatlichem Recht** zusätzlich zu **jedlichen 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 die zuständigen Behörden befugt sind,

a) die Zertifizierung oder Genehmigung für einen Teil oder alle von einer 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 Durchsetzungsmaßnahmen verhängt 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 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) .../...⁺ als kritische Einrichtungen eingestuft wurden, diese Richtlinie erfüllen – die gemäß der Richtlinie (EU) .../...⁺ ■ zuständigen Behörden **innerhalb desselben** Mitgliedstaats ■ unterrichten. **Gegebenenfalls können die** gemäß der Richtlinie (EU) .../...⁺ zuständigen Behörden ■ **die gemäß der vorliegenden Richtlinie** zuständigen Behörden **ersuchen**, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine **Einrichtung, die gemäß der Richtlinie (EU) .../...⁺ 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) .../...⁺⁺ 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) .../...⁺⁺ benannt wurden, diese Richtlinie erfüllen – das gemäß Artikel 32 Absatz 1 der Verordnung (EU) .../...⁺⁺ eingerichtete Überwachungsforum unterrichten.**

⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 51/22 (2020/0365(COD)) enthaltenen Richtlinie in den Text einfügen.

⁺⁺ ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.

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, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung Verpflichtungen zur Übermittlung von Informationen an die **zuständigen Behörden** nach Artikel 28 **erforderlich** sind;
- 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 bestimmter 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 bestimmter Vorgaben öffentlich bekannt zu machen;

■

- h) **gemäß einzelstaatlichem Recht** zusätzlich zu **jedigen 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) .../...⁺⁺ 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) .../...⁺⁺ benannt wurden, diese Richtlinie erfüllen – das gemäß Artikel 32 Absatz 1 der Verordnung (EU) .../...⁺⁺ eingerichtete Überwachungsforum unterrichten.**

⁺⁺ **ABL.: Bitte die Nummer der im Dokument PE-CONS 41/22 (2020/0266(COD)) enthaltenen Verordnung in den Text einfügen.**

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 **jedlichen 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 ... [21 Monate nach Inkrafttreten dieser Richtlinie] 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 ... [**24 Monate** nach Inkrafttreten dieser Richtlinie] 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 Auskunftersuchen 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 ... [***Datum des Inkrafttretens dieser Richtlinie***] 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 ... [57 Monate nach Inkrafttreten dieser Richtlinie] 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 ... [21 Monate nach dem Tag des Inkrafttretens dieser Richtlinie] **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 ... [einen Tag nach dem im ersten Unterabsatz genannten Datum] an.

- (2) Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf 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 ... [in Artikel 41 Absatz 1 Unterabsatz 2 genanntes Datum]** gestrichen.

Artikel 43

Änderung der Richtlinie (EU) 2018/1972

In der Richtlinie (EU) 2018/1972 werden **die Artikel 40 und 41 mit Wirkung vom ... [in Artikel 41 Absatz 1 Unterabsatz 2 genanntes Datum]** gestrichen.

Artikel 44

Aufhebung

Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom ... [in Artikel 41 Absatz 1 Unterabsatz 2 genanntes Datum] 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 ... am ...

Im Namen des Europäischen Parlaments *Im Namen des Rates*

Die Präsidentin

Der Präsident

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 ¹⁶⁷ , 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

¹⁶⁷

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).

Sektor	Teilsektor	Art der Einrichtung
		des Europäischen Parlaments und des Rates ¹⁶⁸
		— Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten — Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b) Fernwärme und -kälte	— Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates ¹⁶⁹
	c) Erdöl	— Betreiber von Erdöl-Fernleitungen

¹⁶⁸ 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).

¹⁶⁹ 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).

Sektor	Teilsektor	Art der Einrichtung
		— 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 ¹⁷⁰
	d) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ¹⁷¹
		— 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

¹⁷⁰ 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).

¹⁷¹ 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).

Sektor	Teilsektor	Art der Einrichtung
		— Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		— Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		— Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	— Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ¹⁷² , Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU)

¹⁷²

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).

Sektor	Teilsektor	Art der Einrichtung
		Nr. 1315/2013 des Europäischen Parlaments und des Rates ¹⁷³ 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 ¹⁷⁴ bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ¹⁷⁵
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1

¹⁷³ 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).

¹⁷⁴ 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).

¹⁷⁵ 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).

Sektor	Teilsektor	Art der Einrichtung
		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 ¹⁷⁶ 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 ¹⁷⁷ , 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

¹⁷⁶ 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).

¹⁷⁷ 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).

Sektor	Teilsektor	Art der Einrichtung
		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ¹⁷⁸
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ¹⁷⁹ , 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

¹⁷⁸ 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).

¹⁷⁹ 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).

Sektor	Teilsektor	Art der Einrichtung
		Europäischen Parlaments und des Rates ¹⁸⁰
3. Bankwesen		Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ¹⁸¹
4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ¹⁸²
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ¹⁸³
5. Gesundheitswesen		— Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie

¹⁸⁰ 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).

¹⁸¹ 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).

¹⁸² 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).

¹⁸³ 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).

Sektor	Teilsektor	Art der Einrichtung
		2011/24/EU des Europäischen Parlaments und des Rates ¹⁸⁴
		— EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) .../... des Europäischen Parlaments und des Rates ¹⁸⁵⁺
		— 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 ¹⁸⁶ 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,

¹⁸⁴ 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).

¹⁸⁵ Verordnung (EU) .../... des Europäischen Parlaments und des Rates vom ... zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L vom ..., S. ...).

⁺ ABl.: Bitte die Nummer der im Dokument PE-CONS .../22 (2020/0322(COD)) enthaltenen Verordnung in den Text sowie Nummer, Datum und Amtsblatfundstelle dieser Verordnung in den Fußnotentext einfügen.

¹⁸⁶ 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).

Sektor	Teilsektor	Art der Einrichtung
		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 ¹⁸⁷ („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 2020/2184 des Europäischen Parlaments und des Rates ¹⁸⁸ , 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

¹⁸⁷ 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).

¹⁸⁸ 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).

Sektor	Teilsektor	Art der Einrichtung
		Sinne des Artikels 2 Nummern 1, 2 und 3 der Richtlinie 91/271/EWG des Rates ¹⁸⁹ 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 Inhaltzustellnetzen
		— Vertrauensdiensteanbieter
		— Anbieter öffentlicher elektronischer Kommunikationsnetze oder

¹⁸⁹

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).

Sektor	Teilsektor	Art der Einrichtung
		— Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
9. Verwaltung von IKT-Diensten (Business-to-Business)		— Anbieter verwalteter Dienste — Anbieter verwalteter Sicherheitsdienste
10. öffentliche Verwaltung		— Einrichtungen der öffentlichen Verwaltung von Zentralregierungen <i>entsprechend der Definition eines Mitgliedstaat gemäß nationalem Recht</i> — Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene <i>entsprechend der Definition eines Mitgliedstaat gemäß nationalem Recht</i> ■
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

Sektor	Teilsektor	Art der Einrichtung
		unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

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 ¹⁹⁰ , 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 ¹⁹¹ , 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		Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des

¹⁹⁰ 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).

¹⁹¹ 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).

Sektor	Teilsektor	Art der Einrichtung
Lebensmitteln		Europäischen Parlaments und des Rates ¹⁹² , 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 ¹⁹³ 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 ¹⁹⁴ 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

¹⁹² 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).

¹⁹³ 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).

¹⁹⁴ 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).

Sektor	Teilsektor	Art der Einrichtung
		Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6. Anbieter digitaler Dienste		— Anbieter von Online-Marktplätzen
		— Anbieter von Online-Suchmaschinen
		— Anbieter von Plattformen für Dienste sozialer Netzwerke
7. Forschung		Forschungseinrichtungen

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 9 Absätze 1, 2 und 3
Artikel 9 Absatz 4	Artikel 10 Absatz 9
Artikel 9 Absatz 5	Artikel 10 Absatz 10

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
Artikel 10 Absätze 1 und 2 und Absatz 3 Unterabsatz 1	Artikel 11 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
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

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
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 37 Absatz 1 Buchstaben a und b
Artikel 17 Absatz 3	Artikel 26 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 Absätze 1 und 2	Artikel 39
Artikel 23	Artikel 40
Artikel 24	-

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Anhang I Nummer 1	Artikel 11 Absatz 1
Anhang I Nummer 2 Buchstabe a Ziffern i bis iv	Artikel 11 Absatz 2 Buchstaben a bis d
Anhang I Nummer 2 Buchstabe a Ziffer v	Artikel 11 Absatz 2 Buchstabe f
Anhang I Nummer 2 Buchstabe b	Artikel 11 Absatz 3
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



ANGENOMMENE TEXTE

P9_TA(2022)0376

Abkommen EU-Ukraine über die Beförderung von Gütern im Straßenverkehr

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Entwurf eines Beschlusses des Rates über den Abschluss – im Namen der Europäischen Union – des Abkommens zwischen der Europäischen Union und der Ukraine über die Beförderung von Gütern im Straßenverkehr (11050/2022 – C9-0299/2022 – 2022/0200(NLE))

(Zustimmung)

Das Europäische Parlament,

- unter Hinweis auf den Entwurf eines Beschlusses des Rates (11050/2022),
 - unter Hinweis auf den Entwurf eines Kooperationsabkommens zwischen der Europäischen Union und ihren Mitgliedstaaten und der Ukraine (10151/2022),
 - unter Hinweis auf das vom Rat gemäß Artikel 91 und Artikel 218 Absatz 6 Unterabsatz 2 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union unterbreitete Ersuchen um Zustimmung (C9-0299/2022),
 - gestützt auf Artikel 105 Absätze 1 und 4 und Artikel 114 Absatz 7 seiner Geschäftsordnung,
 - unter Hinweis auf die Empfehlung des Ausschusses für Verkehr und Tourismus (A9-0263/2022),
1. gibt seine Zustimmung zu dem Abschluss des Abkommens;
 2. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat, der Kommission sowie den Regierungen und Parlamenten der Mitgliedstaaten und der Ukraine zu übermitteln.



ANGENOMMENE TEXTE

P9_TA(2022)0377

Abkommen EU-Moldau über die Beförderung von Gütern im Straßenverkehr

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens – im Namen der Europäischen Union – zwischen der Europäischen Union und der Republik Moldau über die Beförderung von Gütern im Straßenverkehr (11052/2022 – C9-0304/2022 – 2022/0201(NLE))

(Zustimmung)

Das Europäische Parlament,

- unter Hinweis auf den Entwurf eines Beschlusses des Rates (11052/2022),
 - unter Hinweis auf den Entwurf eines Abkommens zwischen der Europäischen Union und der Republik Moldau (10152/2022),
 - unter Hinweis auf das vom Rat gemäß Artikel 91 und Artikel 218 Absatz 6 Unterabsatz 2 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union unterbreitete Ersuchen um Zustimmung (C9-0304/2022),
 - gestützt auf Artikel 105 Absätze 1 und 4 und Artikel 114 Absatz 7 seiner Geschäftsordnung,
 - unter Hinweis auf die Empfehlung des Ausschusses für Verkehr und Tourismus (A9-0262/2022),
1. gibt seine Zustimmung zu dem Abschluss des Abkommens;
 2. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat, der Kommission sowie den Regierungen und Parlamenten der Mitgliedstaaten und der Republik Moldau zu übermitteln.



ANGENOMMENE TEXTE

P9_TA(2022)0378

Abschluss eines Abkommens im Rahmen des GATS über die Änderung der Listen spezifischer Verpflichtungen

Legislative Entschließung des Europäischen Parlaments vom 10. November 2022 zu dem Entwurf eines Beschlusses des Rates über den Abschluss – im Namen der Europäischen Union – eines Abkommens über die Änderung der Listen spezifischer Verpflichtungen im Rahmen des Allgemeinen Übereinkommens über den Handel mit Dienstleistungen zur Einbeziehung von Anhang 1 der Erklärung über den Abschluss der Verhandlungen über die innerstaatliche Regelung von Dienstleistungen vom 2. Dezember 2021 (09982/2022 – C9-0224/2022 – 2022/0174(NLE))

(Zustimmung)

Das Europäische Parlament,

- unter Hinweis auf den Entwurf eines Beschlusses des Rates (09982/2022),
 - unter Hinweis auf den Entwurf eines Abkommens über die Änderung der Listen spezifischer Verpflichtungen im Rahmen des Allgemeinen Übereinkommens über den Handel mit Dienstleistungen zur Einbeziehung von Anhang 1 der Erklärung über den Abschluss der Verhandlungen über die innerstaatliche Regelung von Dienstleistungen vom 2. Dezember 2021 (09982/2022),
 - unter Hinweis auf das vom Rat gemäß Artikel 91, Artikel 100 Absatz 2, Artikel 207 Absatz 4 Unterabsatz 1 und Artikel 218 Absatz 6 Unterabsatz 2 Buchstabe a Ziffer v des Vertrags über die Arbeitsweise der Europäischen Union unterbreitete Ersuchen um Zustimmung (C9-0224/2022),
 - gestützt auf Artikel 105 Absätze 1 und 4 und Artikel 114 Absatz 7 seiner Geschäftsordnung,
 - unter Hinweis auf die Empfehlung des Ausschusses für internationalen Handel (A9-0257/2022),
1. gibt seine Zustimmung zu dem Abschluss des Abkommens;
 2. beauftragt seine Präsidentin, den Standpunkt des Parlaments dem Rat und der Kommission sowie den Regierungen und Parlamenten der Mitgliedstaaten und der Welthandelsorganisation zu übermitteln.



Европейски парламент Parlamento Europeo Evropský parlament Europa-Parlamentet Europäisches Parlament
Euroopa Parlament Ευρωπαϊκό Κοινοβούλιο European Parliament Parlement européen Parlaimint na hEorpa
Europski parlament Parlamento europeo Eiropas Parlaments Europos Parlamentas Európai Parlament
Parlament Ewropew Europees Parlement Parlament Europejski Parlamento Europeu Parlamentul European
Európsky parlament Evropski parlament Euroopan parlamentti Europaparlamentet

www.parlament.gv.at