EUROPÄISCHE
KOMMISSION

Brüssel, den 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

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

(Text von Bedeutung für den EWR)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

- Gründe und Ziele des Vorschlags

Der vorliegende Vorschlag ist Teil des Pakets zur Digitalisierung des Finanzsektors, eines Maßnahmenpakets, das darauf abzielt, das Innovations- und Wettbewerbspotenzial des digitalen Finanzwesens weiter zu erschließen und zu fördern und gleichzeitig mögliche Risiken zu mindern. Er steht im Einklang mit den Prioritäten der Kommission, Europa für das digitale Zeitalter zu rüsten und eine zukunftsfähige Wirtschaft im Dienste der Menschen aufzubauen. Das Paket zur Digitalisierung des Finanzsektors umfasst eine neue Strategie für ein digitales Finanzwesen[1], mit der sichergestellt werden soll, dass die EU die digitale Revolution als Chance nutzt, mit innovativen europäischen Unternehmen als Vorreiter vorantreibt und so dafür sorgt, dass Verbraucher und Unternehmen in Europa von den Vorteilen eines digitalen Finanzwesens profitieren können. Neben dem vorliegenden Vorschlag umfasst das Paket zudem einen Vorschlag für eine Verordnung über Märkte für Kryptowerte[2], einen Vorschlag für eine Verordnung über eine Pilotregelung für auf der Distributed-Ledger-Technologie (DLT) basierende Marktinfrastrukturen[3] sowie einen Vorschlag für eine Richtlinie, mit der bestimmte einschlägige EU-Vorschriften für Finanzdienstleistungen klargestellt bzw. geändert werden sollen.[4]Digitalisierung und Betriebsstabilität im Finanzsektor sind zwei Seiten derselben Medaille: Mit Digital- bzw. Informations- und Kommunikationstechnologien (IKT) sind Chancen, aber auch Risiken verbunden. Diese müssen insbesondere in Phasen mit Marktverwerfungen gut verstanden und gesteuert werden.

Infolgedessen haben sich Politik und Aufsichtsbehörden verstärkt mit Risiken befasst, die aus der Abhängigkeit von IKT erwachsen. Dabei wurde insbesondere versucht, die Resilienz von Unternehmen durch die Festlegung von Standards und eine koordinierte Regulierung und Beaufsichtigung zu verbessern. Diese Bemühungen erfolgten auf internationaler und europäischer Ebene, sowohl über verschiedene Branchen hinweg als auch für eine Reihe bestimmter Sektoren, darunter Finanzdienstleistungen.

Dennoch bleiben IKT-Risiken eine Herausforderung für die Betriebsstabilität, die Leistungsfähigkeit und die Stabilität des Finanzsystems der EU. Mit der nach der Finanzkrise von 2008 durchgeführten Reform wurde in erster Linie die finanzielle Resilienz[5] des Finanzsektors der EU gestärkt, während IKT-Risiken nur indirekt in einigen Bereichen im Rahmen der Maßnahmen zur Minderung operationeller Risiken im weiteren Sinne angegangen wurden.

---

1 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine Strategie für ein digitales Finanzwesen in der EU (COM(2020) 591 final), 24. September 2020.

2 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM(2020) 593.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Pilotregelung für auf der Distributed-Ledger-Technologie basierende Marktinfrastrukturen, COM(2020) 594.

4 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, (EU) 2015/2366 und (EU) 2016/2341, COM(2020) 596.

5 Die einzelnen verabschiedeten Maßnahmen zielten grundsätzlich darauf ab, Kapitalressourcen und Liquidität von Finanzunternehmen zu erhöhen und Markt- und Kreditrisiken zu senken.

Mit den Änderungen der EU-Finanzdienstleistungsvorschriften nach der Krise wurde zwar ein einheitliches Regelwerk eingeführt, das große Teile der finanziellen Risiken im Zusammenhang mit Finanzdienstleistungen abdeckt, doch wurde die digitale Betriebsstabilität nicht in vollem Umfang berücksichtigt. Die für die digitale Betriebsstabilität ergriffenen Maßnahmen wiesen eine Reihe von Merkmalen auf, die ihre Wirksamkeit einschränkten. So wurden sie häufig als Richtlinien für eine Mindestharmonisierung oder grundsatzbasierte Verordnungen konzipiert, sodass im Binnenmarkt ein erheblicher Spielraum für unterschiedliche Ansätze entstand. Darüber hinaus wurde im Zusammenhang mit der Erfassung operationeller Risiken nur ein begrenzter oder unvollständiger Schwerpunkt auf IKT-Risiken gelegt. Hinzu kommt, dass sich diese Maßnahmen über die sektorspezifischen Rechtsvorschriften für Finanzdienstleistungen hinweg unterscheiden. Folglich war das Tätigwerden auf Unionsebene nicht umfassend auf die Bedingungen abgestimmt, die europäische Finanzunternehmen benötigen, um operationelle Risiken so zu steuern, dass die Folgen IKT-bezogener Vorfälle abgefedert und entsprechende Gegen- und Wiederherstellungsmaßnahmen ergriffen werden. Auch wurden die Finanzaufsichtsbehörden nicht mit dem optimalen Instrumentarium ausgestattet, um ihrem Auftrag zur Verhinderung einer Instabilität des Finanzwesens infolge der Entstehung dieser IKT-bedingten Risiken gerecht zu werden.

Dass auf EU-Ebene noch immer keine detaillierten und umfassenden Vorschriften über die digitale Betriebsstabilität bestehen, hat zu einer Vielzahl nationaler Regulierungsinitiativen (z. B. zur Prüfung der digitalen Betriebsstabilität) und Aufsichtskonzepte (z. B. mit Blick auf die Abhängigkeit von IKT-Drittanbietern) geführt. Gleichwohl haben Maßnahmen auf Ebene der Mitgliedstaaten angesichts des grenzüberschreitenden Charakters von IKT-Risiken nur eine begrenzte Wirkung. Darüber hinaus haben die unkoordinierten nationalen Initiativen zu Überschneidungen, Inkohärenzen, Doppelanforderungen, hohen Verwaltungs- und Befolgungskosten – insbesondere für grenzüberschreitend tätige Finanzunternehmen – oder dazu geführt, dass IKT-Risiken nicht erkannt und somit nicht angegangen werden. Durch diesen Umstand wird der Binnenmarkt fragmentiert, die Stabilität und Integrität des EU-Finanzsektors untergraben und der Schutz von Verbrauchern und Anlegern gefährdet.

Daher ist es notwendig, einen detaillierten und umfassenden Rahmen für die digitale Betriebsstabilität von EU-Finanzunternehmen zu schaffen. Mit diesem Rahmen wird die Dimension des Managements des digitalen Risikos aus dem einheitlichen Regelwerk vertieft. Insbesondere wird hierdurch das IKT-Risikomanagement von Finanzunternehmen verbessert und gestrafft, während gleichzeitig eine gründliche Prüfung von IKT-Systemen eingeführt und das Bewusstsein von Aufsichtsbehörden für Cyberrisiken und IKT-bezogene Vorfälle, mit denen Finanzunternehmen konfrontiert sind, geschärft und Befugnisse für Finanzaufsichtsbehörden eingerichtet werden, damit diese Risiken überwachen können, die auf die Abhängigkeit von Finanzunternehmen von IKT-Drittanbietern zurückzuführen sind. Mit dem Vorschlag wird ein kohärenter Mechanismus für die Meldung von Vorfällen geschaffen, der dazu beitragen wird, den Verwaltungsaufwand für Finanzunternehmen zu verringern und die Beaufsichtigung wirksamer zu machen.

- Kohärenz mit den bestehenden Vorschriften in diesem Bereich

Dieser Vorschlag ist Teil umfassenderer Arbeiten auf europäischer und internationaler Ebene zur Stärkung der Cybersicherheit bei Finanzdienstleistungen und zur Bewältigung allgemeinerer operationeller Risiken.[6]

Der Vorschlag knüpft darüber hinaus an das gemeinsame fachliche Gutachten[7] der Europäischen Aufsichtsbehörden (ESA) aus dem Jahr 2019 an, mit dem ein kohärenterer Ansatz zur Bewältigung von IKT-Risiken im Finanzbereich gefordert und der Kommission empfohlen wurde, die digitale Betriebsstabilität der Finanzdienstleistungsbranche durch eine sektorspezifische Initiative der EU in verhältnismäßiger Weise zu stärken. Die Empfehlung der ESA war eine Antwort auf den FinTech-Aktionsplan der Kommission von 2018[8] .

- Kohärenz mit der Politik der Union in anderen Bereichen

Wie Kommissionspräsidentin von der Leyen in ihren politischen Leitlinien[9] betont hat und in der Mitteilung „Gestaltung der digitalen Zukunft Europas“[10] dargelegt, ist es für Europa von entscheidender Bedeutung, alle Chancen des digitalen Zeitalters innerhalb sicherer und ethischer Grenzen zu nutzen und seine Industrie und Innovationskapazität zu stärken. In der europäischen Datenstrategie[11] sind vier Säulen – Datenschutz, Grundrechte, Sicherheit und Cybersicherheit – als wesentliche Voraussetzungen für eine Gesellschaft dargelegt, die durch die Nutzung von Daten Handlungskapazitäten aufbaut. Das Europäische Parlament arbeitet seit Kurzem an einem Bericht über das digitale Finanzwesen, in dem unter anderem ein gemeinsamer Ansatz für die Widerstandsfähigkeit des Finanzsektors gegenüber Cyberangriffen gefordert wird.[12]Ein Rechtsrahmen zur Stärkung der digitalen Betriebsstabilität der EU-Finanzunternehmen steht im Einklang mit diesen politischen Zielen. Mit dem Vorschlag würden darüber hinaus politische Maßnahmen zur Erholung von der Coronakrise unterstützt, zumal mit ihm sichergestellt wäre, dass die verstärkte Abhängigkeit vom digitalen Finanzwesen mit Betriebsstabilität einhergeht.

Mit der Initiative blieben die Vorteile des horizontalen Rahmens für Cybersicherheit (z. B. die Richtlinie über die Sicherheit von Netz- und Informationssystemen, NIS-Richtlinie) erhalten, indem der Finanzsektor innerhalb des Geltungsbereichs dieses Rahmens bliebe. Zudem wäre der Finanzsektor weiterhin eng in das NIS-Kooperationsgremium eingebunden, und die Finanzaufsichtsbehörden wären in der Lage, einschlägige Informationen innerhalb des bestehenden NIS-Ökosystems auszutauschen. Auch stünde die Initiative im Einklang mit der

---

6 Basler Ausschuss für Bankenaufsicht, *Cyber-resilience: Range of practices (*Cyber-Resilienz*,* eine Reihe von Praktiken), Dezember 2018 und *Principles for sound management of operational risk* (Leitlinien für die robuste Steuerung operationeller Risiken*, PSMOR*), Oktober 2014.

7 Gemeinsames Gutachten der Europäischen Aufsichtsbehörden an die Kommission zur Notwendigkeit legislativer Verbesserungen in Bezug auf die Anforderungen an das Management von IKT-Risiken im EU-Finanzsektor, JC 2019 26 (2019).

8 Europäische Kommission, *FinTech-Aktionsplan*, COM(2018) 109 final.

9 Präsidentin Ursula von der Leyen, Politische Leitlinien für die künftige Europäische Kommission 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf.

10 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „*Gestaltung der digitalen Zukunft Europas*“, COM(2020) 67 final.

11 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, *Eine europäische Datenstrategie*, COM(2020) 66 final.

12 „Bericht mit Empfehlungen an die Kommission zum digitalen Finanzwesen: neu auftretende Risiken bei Kryptoanlagen – Herausforderungen in Bezug auf Regulierung und Aufsicht im Bereich Finanzdienstleistungen, Finanzinstitute und Finanzmärkte (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

Richtlinie über europäische kritische Infrastrukturen („EKI“), die derzeit überarbeitet wird, um den Schutz und die Widerstandsfähigkeit kritischer Infrastrukturen gegen nicht cyberbedingte Bedrohungen zu verbessern. Schließlich steht der Vorschlag voll im Einklang mit der EU-Strategie für eine Sicherheitsunion[13], mit der angesichts der hohen Abhängigkeit des Finanzsektors von IKT-Diensten und dessen hoher Anfälligkeit für Cyberangriffe eine Initiative für die digitale Betriebsstabilität des Finanzsektors gefordert wurde.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- Rechtsgrundlage

Der Verordnungsvorschlag stützt sich auf Artikel 114 AEUV.

Er beseitigt Hindernisse und verbessert die Errichtung und das Funktionieren des Binnenmarkts für Finanzdienstleistungen, indem die Vorschriften für das IKT-Risikomanagement, die Berichterstattung, Prüfungen und für das Risiko durch IKT-Drittanbieter harmonisiert werden. Die derzeitigen Unterschiede in diesem Bereich auf legislativer und aufsichtsrechtlicher Ebene sowie auf nationaler und EU-Ebene sind Hindernisse für den Binnenmarkt für Finanzdienstleistungen, da grenzüberschreitend tätige Finanzunternehmen bei Nichtüberschneidung mit unterschiedlichen aufsichtsrechtlichen Anforderungen bzw. Erwartungen konfrontiert sind, was ihre Ausübung der Niederlassungs- und Dienstleistungsfreiheit behindern könnte. Des Weiteren verzerren unterschiedliche Vorschriften den Wettbewerb zwischen Finanzunternehmen desselben Typs in verschiedenen Mitgliedstaaten. Überdies kann mit Blick auf die Ausübung der Freiheiten des Binnenmarkts für Finanzdienstleistungen eine abschreckende Wirkung entstehen, wenn in Bereichen, in denen keine, eine teilweise oder begrenzte Harmonisierung besteht, unterschiedliche nationale Vorschriften oder Herangehensweisen entwickelt werden, die entweder bereits in Kraft sind oder gerade auf nationaler Ebene verabschiedet und umgesetzt werden. Das gilt insbesondere, insofern dies Rahmen für operationelle Tests im digitalen Bereich und die Aufsicht über kritische IKT-Drittanbieter betrifft.

Da der Vorschlag Auswirkungen auf mehrere Richtlinien des Europäischen Parlaments und des Rates hat, die auf der Grundlage von Artikel 53 Absatz 1 AEUV angenommen wurden, wird gleichzeitig ein Vorschlag für eine Richtlinie angenommen, um den erforderlichen Änderungen dieser Richtlinien Rechnung zu tragen.

- Subsidiarität

Aufgrund der ausgeprägten Vernetzung von Finanzdienstleistungen, der umfassenden grenzüberschreitenden Tätigkeit von Finanzunternehmen und der großen Abhängigkeit des gesamten Finanzsektors von IKT-Drittanbietern liegt eine hohe digitale Betriebsstabilität im gemeinsamen Interesse, damit die Solidität der EU-Finanzmärkte erhalten bleibt. Unterschiede infolge uneinheitlicher oder teilweiser Regelungen, Überschneidungen oder mehrfache Anforderungen, die auf dieselben Finanzunternehmen anwendbar sind, die

[13] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, *EU-Strategie für eine Sicherheitsunion*, COM(2020) 605 final.

grenzüberschreitend tätig sind oder über mehrere Zulassungen[14] im gesamten Binnenmarkt verfügen, können nur auf Unionsebene wirksam angegangen werden.

Durch den Vorschlag wird die digitale operationelle Komponente eines umfassend integrierten und vernetzten Sektors harmonisiert, der in den meisten anderen wichtigen Bereichen bereits einem einheitlichen Regelwerk und einer einheitlichen Aufsicht unterliegt. In Bereichen wie der Meldung IKT-bezogener Vorfälle ließen sich der Verwaltungsaufwand und die finanziellen Kosten, die mit der Meldung desselben IKT-bezogenen Vorfalls an verschiedene Behörden der Union und der Mitgliedstaaten verbunden sind, nur durch harmonisierte Unionsvorschriften senken. Maßnahmen auf Unionsebene sind auch deswegen erforderlich, um die gegenseitige Anerkennung der Ergebnisse umfassender Tests der digitalen Betriebsstabilität für grenzüberschreitend tätige Unternehmen zu erleichtern, die in Ermangelung von Unionsvorschriften in den einzelnen Mitgliedstaaten unterschiedlichen Rahmen unterliegen oder unterliegen können. Unterschiede bei den Testansätzen, die Mitgliedstaaten eingeführt haben, können nur durch Maßnahmen auf Unionsebene angegangen wurden. Ferner sind EU-weite Maßnahmen erforderlich, um dem Mangel an angemessenen Aufsichtsbefugnissen zur Überwachung der von IKT-Drittanbietern ausgehenden Risiken, darunter auch Konzentrations- und Ansteckungsrisiken für den EU-Finanzsektor, entgegenzuwirken.

- Verhältnismäßigkeit

Die vorgeschlagenen Vorschriften gehen nicht über das zur Erreichung der Ziele des Vorschlags erforderliche Maß hinaus. Sie decken nur die Aspekte ab, die die Mitgliedstaaten nicht alleine umsetzen können und deren Verwaltungsaufwand und Kosten in einem angemessenen Verhältnis zu den besonderen und allgemeinen Zielen stehen, die erreicht werden sollen.

Die Verhältnismäßigkeit wird im Hinblick auf Umfang und Intensität durch die Verwendung qualitativer und quantitativer Bewertungskriterien gewährleistet. Während die neuen Vorschriften für alle Finanzunternehmen gelten, soll mit diesen Kriterien sichergestellt werden, dass sie gleichzeitig auf Risiken und Bedürfnisse ihrer besonderen Merkmale in Bezug auf Größe und Unternehmensprofile zugeschnitten sind. Die Verhältnismäßigkeit ist auch in den Vorschriften für das IKT-Risikomanagement, die Prüfung der digitalen Resilienz, die Meldung schwerwiegender IKT-bezogener Vorfälle und die Aufsicht über kritische IKT-Drittanbieter verankert.

- Wahl des Instruments

Die Maßnahmen, die für die Regelung des IKT-Risikomanagements, die Meldung IKT-bezogener Vorfälle, die Prüfung und Beaufsichtigung kritischer IKT-Drittanbieter erforderlich sind, müssen in einer Verordnung festgeschrieben werden, damit sichergestellt ist, dass die detaillierten Anforderungen unbeschadet der Verhältnismäßigkeit und der in dieser Verordnung vorgesehenen besonderen Vorschriften wirksam und unmittelbar einheitlich anwendbar sind. Die Kohärenz bei der Bewältigung digitaler operationeller Risiken trägt dazu bei, das Vertrauen in das Finanzsystem zu stärken und dessen Stabilität zu wahren. Da die Nutzung einer Verordnung hilft, die aufsichtsrechtliche Komplexität zu verringern, die aufsichtliche Konvergenz fördert und die Rechtssicherheit erhöht, trägt diese Verordnung

[14] Es ist möglich, dass ein und dasselbe Finanzunternehmen eine Lizenz für eine Bank, eine Wertpapierfirma und ein Zahlungsinstitut besitzt, die jeweils von einer anderen Aufsichtsbehörde in einem oder mehreren Mitgliedstaaten ausgestellt wurde.

auch dazu bei, die Befolgungskosten von Finanzunternehmen zu begrenzen (insbesondere sofern diese grenzüberschreitend tätig sind), was im Gegenzug zur Beseitigung von Wettbewerbsverzerrungen beitrüge.

Des Weiteren werden mit dieser Verordnung legislative Unterschiede und ungleiche nationale Regulierungs- oder Aufsichtskonzepte für IKT-Risiken und somit Hindernisse für den Binnenmarkt für Finanzdienstleistungen beseitigt, insbesondere mit Blick auf die reibungslose Ausübung der Niederlassungsfreiheit und die Erbringung von Dienstleistungen für grenzüberschreitend tätige Finanzinstitute.

Schließlich wurde das einheitliche Regelwerk größtenteils über Verordnungen entwickelt, und seine Aktualisierung mit der Komponente „digitale Betriebsstabilität“ sollte über das gleiche Rechtsinstrument erfolgen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften

Auf dem Gebiet der Finanzdienstleistungen gibt es bislang keine Rechtsvorschriften der Union, in denen die Betriebsstabilität und die umfassende Behandlung digitalisierungsbezogener Risiken im Mittelpunkt steht; das ist auch dann der Fall, wenn das operationelle Risiko in den Rechtsvorschriften allgemeiner mit dem Unterkapitel IKT-Risiken behandelt wird. Die Maßnahmen der Union haben bislang dazu beigetragen, Bedürfnisse und Probleme anzugehen, die im Nachgang zur Finanzkrise 2008 aufgetreten sind: So waren Kreditinstitute nicht ausreichend kapitalisiert, Finanzmärkte nicht ausreichend integriert, während die Harmonisierung bis dahin auf einem minimalen Stand gehalten wurde. IKT-Risiken wurden damals nicht als Priorität betrachtet, sodass sich die Rechtsrahmen für die verschiedenen Teilsektoren des Finanzsektors in unkoordinierter Weise weiterentwickelten. Dennoch wurde mit den Maßnahmen der Union das Ziel erreicht, die Finanzstabilität zu gewährleisten und ein einheitliches Paket harmonisierter Aufsichts- und Marktverhaltensregeln festzulegen, die auf Finanzunternehmen in der gesamten EU anwendbar sind. Da es mit den Faktoren, mit denen die legislativen Maßnahmen der Union in der Vergangenheit vorangetrieben wurden, nicht möglich war, spezifische oder umfassende Vorschriften zu erlassen, um die weitverbreitete Nutzung digitaler Technologien und die damit verbundenen Risiken im Finanzbereich anzugehen, erscheint die Durchführung einer expliziten Evaluierung schwierig. In jeder Säule dieser Verordnung spiegeln sich eine implizite Bewertung und entsprechende Gesetzesänderungen wider.

- Konsultation der Interessenträger

Die Kommission hat während des gesamten Prozesses für die Ausarbeitung dieses Vorschlags Interessenträger konsultiert, darunter insbesondere:

i) Die Kommission führte eine spezielle öffentliche Konsultation zu diesem Thema durch (19. Dezember 2019 - 19. März 2020);[15]

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

ii) Die Kommission konsultierte die Öffentlichkeit im Rahmen einer Folgenabschätzung in der Anfangsphase (19. Dezember 2019 - 16. Januar 2020);[16]

iii) Die Kommissionsdienststellen konsultierten die Sachverständigen der Mitgliedstaaten in der Sachverständigengruppe für Bankwesen, Zahlungsverkehr und Versicherungswesen (EGBPI) zweimal (am 18. Mai 2020 und am 16. Juli 2020);[17]

iv) Die Dienststellen der Kommission führten im Rahmen der Veranstaltungsreihe „Digital Finance Outreach 2020“ (19. Mai 2020) ein spezielles Webinar zur digitalen Betriebsstabilität durch.

Ziel der öffentlichen Konsultation war es, die Kommission über die Entwicklung eines potenziellen sektorübergreifenden EU-Rahmens für die digitale Betriebsstabilität im Bereich der Finanzdienstleistungen zu unterrichten. Den Antworten war eine breite Unterstützung für die Einführung eines speziellen Rahmens mit Maßnahmen, die sich auf die vier Bereiche konzentrieren, die Gegenstand der Konsultation sind, zu entnehmen; außerdem wurde betont, dass die Verhältnismäßigkeit gewahrt und die Wechselwirkung mit den horizontalen Vorschriften der NIS-Richtlinie sorgfältig angegangen und erläutert werden muss. Die Kommission erhielt zwei Antworten auf die Folgenabschätzung in der Anfangsphase, in deren Rahmen sich die Befragten mit spezifischen Aspekten ihres Tätigkeitsbereichs befassten.

Die Mitgliedstaaten bekundeten auf der EGBPI-Sitzung vom 18. Mai 2020, die Stärkung der digitalen Betriebsstabilität des Finanzsektors durch die Maßnahmen, die über die von der Kommission skizzierten vier Elemente erfolgen sollen, umfassend zu unterstützen. Ferner betonten die Mitgliedstaaten, dass die neuen Vorschriften unmissverständlich mit den Vorschriften über operationelle Risiken (im Rahmen der EU-Rechtsvorschriften über Finanzdienstleistungen) und mit den horizontalen Vorschriften über Cybersicherheit (NIS-Richtlinie) verknüpft werden müssen. Auf der zweiten Sitzung hoben einige Mitgliedstaaten die Notwendigkeit hervor, die Verhältnismäßigkeit zu gewährleisten und die besonderen Umstände von kleinen Unternehmen oder Tochtergesellschaften größerer Konzerne zu berücksichtigen und den an der Aufsicht beteiligten zuständigen nationalen Behörden ein umfassendes Mandat zu übertragen.

Darüber hinaus sind Rückmeldungen von Sitzungen mit Interessenträgern und EU-Behörden und -Institutionen in diesen Vorschlag eingeflossen und in diesem berücksichtigt. Die Interessenträger, darunter auch IKT-Drittanbieter, haben insgesamt Unterstützung geleistet. Eine Analyse der eingegangenen Rückmeldungen zeigt, dass bei der Ausarbeitung der Vorschriften die Verhältnismäßigkeit gewahrt und ein grundsatz- und risikobasierter Ansatz verfolgt werden muss. Auf institutioneller Seite stammten die wichtigsten Beiträge vom Europäischen Ausschuss für Systemrisiken (ESRB), den ESA, der Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Europäischen Zentralbank (EZB) sowie den zuständigen Behörden der Mitgliedstaaten.

- Einholung und Nutzung von Expertenwissen

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

Bei der Ausarbeitung des Vorschlags stützte sich die Kommission auf qualitative und quantitative Nachweise aus anerkannten Quellen, einschließlich der beiden gemeinsamen fachlichen Gutachten der ESA. Ergänzt wurde dies durch vertrauliche Beiträge und öffentlich zugängliche Berichte von Aufsichtsbehörden, internationalen Normungsgremien und führenden Forschungsinstituten sowie durch quantitative und qualitative Beiträge ausgewählter Interessenträger des globalen Finanzsektors.

- Folgenabschätzung

Diesem Vorschlag liegt eine Folgenabschätzung[18] bei, die dem Ausschuss für Regulierungskontrolle (RSB) am 29. April 2020 vorgelegt und von diesem am 29. Mai 2020 genehmigt wurde. Der RSB empfahl Verbesserungen in einigen Bereichen, um: i) weitere Informationen darüber bereitzustellen, wie die Verhältnismäßigkeit gewährleistet würde; ii) deutlicher herauszustellen, inwieweit sich die bevorzugte Option vom gemeinsamen fachlichen Gutachten der ESA unterscheidet, und warum diese Option optimal ist; und iii) weiter deutlich zu machen, welche Wechselwirkung zwischen dem Vorschlag und den bestehenden EU-Rechtsvorschriften, einschließlich derzeit überarbeiteter Vorschriften, gegeben ist. Die Folgenabschätzung wurde angepasst, um diesen Punkten Rechnung zu tragen und auf die ausführlicheren Bemerkungen des Ausschusses für Regulierungskontrolle einzugehen.

Die Kommission hat eine Reihe politischer Optionen für die Entwicklung eines Rahmens für die digitale Betriebsstabilität geprüft:

- „Untätig bleiben“: Die Vorschriften über Betriebsstabilität würden weiterhin durch die aktuellen, voneinander abweichenden EU-Finanzdienstleistungsvorschriften, zum Teil durch die NIS-Richtlinie, sowie durch bestehende oder künftige nationale Regelungen festgelegt;
- Option 1: Stärkung der Kapitalpuffer: Es würden zusätzliche Kapitalpuffer eingeführt, um die Fähigkeit von Finanzunternehmen zu erhöhen, Verluste zu absorbieren, die aufgrund mangelnder digitaler Betriebsstabilität entstehen könnten;
- Option 2: Einführung eines Rechtsakts über die digitale Betriebsstabilität in Bezug auf Finanzdienstleistungen: Schaffung eines umfassenden Rahmens auf EU-Ebene mit kohärenten Vorschriften, die den Anforderungen an die digitale Betriebsstabilität aller regulierten Finanzunternehmen Rechnung tragen, und Schaffung eines Aufsichtsrahmens für kritische IKT-Drittanbieter;
- Option 3: ein Rechtsakt über die digitale Betriebsstabilität in Bezug auf Finanzdienstleistungen in Verbindung mit einer zentralisierten Aufsicht über kritische IKT-Drittanbieter; neben einem Rechtsakt über digitale Betriebsstabilität (Option 2) würde eine neue Behörde eingerichtet, die die Erbringung von Diensten durch IKT-Drittanbieter überwacht.

Die zweite Option wurde deswegen gewählt, weil damit die meisten der angestrebten Ziele auf eine wirksame, effiziente und mit anderen Politikbereichen der Union abgestimmte Weise erreicht werden. Auch die meisten Interessenträger ziehen diese Option vor.

[18] Arbeitsunterlage der Kommissionsdienststellen – Folgenabschätzung als Begleitunterlage zum Dokument Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014, SWD(2020) 198 vom 24.9.2020.

Die gewählte Option würde sowohl einmalige als auch wiederkehrende Kosten mit sich bringen.[19] Die einmaligen Kosten sind hauptsächlich auf Investitionen in IT-Systeme zurückzuführen und lassen sich aufgrund der unterschiedlichen Beschaffenheit komplexer IT-Landschaften von Unternehmen und insbesondere ihrer IT-Altsysteme nur schwer quantifizieren. Dennoch dürften sich diese Kosten für große Unternehmen angesichts der beträchtlichen IKT-Investitionen, die diese bereits getätigt haben, im Rahmen halten. Auch für kleinere Unternehmen dürften die Kosten begrenzt sein, da angesichts ihres geringeren Risikos verhältnismäßige Maßnahmen zur Anwendung kämen.

Die gewählte Option würde sich in wirtschaftlicher, sozialer und ökologischer Hinsicht positiv auf KMU auswirken, die in der Finanzdienstleistungsbranche tätig sind. Mit dem Vorschlag werden KMU Klarheit darüber erhalten, welche Vorschriften anwendbar sind, wodurch die Befolgungskosten sinken.

Die wesentlichen sozialen Auswirkungen der gewählten Option würden Verbraucher und Anleger betreffen. Eine höhere digitale Betriebsstabilität des Finanzsystems der EU würde die Anzahl und die Durchschnittskosten von Vorfällen senken. Außerdem käme das zunehmende Vertrauen in die Finanzdienstleistungsbranche der Gesellschaft insgesamt zugute.

Mit Blick auf die ökologischen Auswirkungen würde die gewählte Option die verstärkte Nutzung der neuesten Generation von IKT-Infrastrukturen und -Diensten fördern, die ökologisch nachhaltiger werden dürften.

- Effizienz der Rechtsetzung und Vereinfachung

Die Beseitigung sich überschneidender Anforderungen für die Meldung IKT-bezogener Vorfälle würde den Verwaltungsaufwand verringern und damit verbundene Kosten senken. Darüber hinaus werden harmonisierte Tests der digitalen Betriebsstabilität mit gegenseitiger Anerkennung im gesamten Binnenmarkt dafür sorgen, dass die Kosten insbesondere für grenzüberschreitend tätige Unternehmen, die andernfalls mehreren Tests in den Mitgliedstaaten unterzogen werden könnten, sinken.[20]

- Grundrechte

Die EU hat sich der Gewährleistung hoher Standards für den Schutz der Grundrechte verschrieben. Alle freiwilligen Vereinbarungen über den Informationsaustausch zwischen Finanzunternehmen, die mit dieser Verordnung gefördert werden, würden unter uneingeschränkter Einhaltung der Datenschutzvorschriften der Union, vor allem der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[21], in vertrauenswürdigen Umgebungen geschlossen, insbesondere wenn die Verarbeitung personenbezogener Daten für die Zwecke eines berechtigten Interesses erforderlich ist, das der für die Verarbeitung Verantwortliche verfolgt.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

---

19 Ebd., S. 89-94.

20 Ebd.

21 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).

Da die derzeitige Verordnung den ESA durch die ihnen übertragenen Befugnisse zur angemessenen Beaufsichtigung kritischer IKT-Drittanbieter eine größere Rolle zuerkennt, würde der Vorschlag – was die Auswirkungen auf den Haushalt betrifft – den Einsatz zusätzlicher Ressourcen, insbesondere zur Erfüllung des Überwachungsauftrags (z. B. Vor-Ort- und Online-Kontrollen und -Prüfungen), und den Einsatz von Fachpersonal im Bereich der IKT-Sicherheit mit sich bringen.

Der Umfang und die Aufteilung dieser Kosten hängen vom Ausmaß der neuen Aufsichtsbefugnisse und den (genauen) Aufgaben der ESA ab. Was die Bereitstellung neuer Personalressourcen angeht, werden die EBA, die ESMA und die EIOPA insgesamt 18 Vollzeitbeschäftigte (VZÄ) – 6 VZÄ pro Behörde – benötigen, wenn die verschiedenen Bestimmungen des Vorschlags in Kraft treten (schätzungsweise 15,71 Mio. EUR für den Zeitraum 2022-2027). Überdies entstehen den ESA zusätzliche IT-Kosten, Kosten für Kontrollen vor Ort und Übersetzungen (schätzungsweise 12 Mio. EUR für den Zeitraum 2022-2027) sowie sonstige Verwaltungsausgaben (schätzungsweise 2,48 Mio. EUR für den Zeitraum 2022-2027). Daher belaufen sich die geschätzten Gesamtkosten für den Zeitraum 2022-2027 auf rund 30,19 Mio. EUR.

Zudem ist darauf hinzuweisen, dass die für die direkte Aufsicht erforderliche Mitarbeiterzahl (z. B. neue Mitarbeiter und sonstige Ausgaben im Zusammenhang mit den neuen Aufgaben) im Laufe der Zeit davon abhängen wird, wie sich Zahl und Größe der zu überwachenden kritischen IKT-Drittanbieter entwickeln, die entsprechenden Ausgaben jedoch vollständig mit Gebühren dieser Marktteilnehmer finanziert werden. Daher sind keine Auswirkungen auf die Haushaltsmittel der EU (mit Ausnahme des zusätzlichen Personals) zu erwarten, da diese Kosten vollständig durch Gebühren finanziert werden.

Die finanziellen und budgetären Auswirkungen des Vorschlags werden im beigefügten Finanzbogen ausführlich erläutert.

5. WEITERE ANGABEN

- Durchführungspläne sowie Überwachungs-, Bewertungs- und Berichterstattungsmodalitäten

Der Vorschlag enthält einen allgemeinen Plan für die Überwachung und Bewertung der Auswirkungen auf die spezifischen Ziele, wonach die Kommission mindestens drei Jahre nach Inkrafttreten eine Überprüfung vornehmen und dem Europäischen Parlament und dem Rat über die wichtigsten Ergebnisse Bericht erstatten muss.

Die Überprüfung ist im Einklang mit den Leitlinien der Kommission für eine bessere Rechtsetzung durchzuführen.

- Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags

Der Vorschlag ist auf mehrere wichtige Politikbereiche ausgerichtet, bei denen es sich um wichtige miteinander verknüpfte Säulen handelt, die einvernehmlich in europäischen und internationalen Leitlinien und bewährten Verfahren zur Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen und der digitalen Betriebsstabilität des Finanzsektors enthalten sind.

Anwendungsbereich der Verordnung und verhältnismäßige Anwendung erforderlicher Maßnahmen (Artikel 2)

Um bei den im Finanzsektor für das IKT-Risikomanagement anwendbaren Anforderungen eine Kohärenz zu gewährleisten, werden mit der Verordnung eine Reihe von auf Unionsebene regulierten Finanzunternehmen abgedeckt, namentlich Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Zentralverwahrer, zentrale Gegenparteien, Handelsplätze, Transaktionsregister, Verwalter alternativer Investmentfonds und Verwaltungsgesellschaften, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, Einrichtungen der betrieblichen Altersversorgung (EbAV), Ratingagenturen, Abschlussprüfer und Prüfungsgesellschaften, Administratoren kritischer Referenzwerte und Crowdfunding-Dienstleister.

Eine solche Abdeckung erleichtert die einheitliche und kohärente Anwendung aller Komponenten des Risikomanagements in IKT-bezogenen Bereichen und sorgt gleichzeitig für gleiche Wettbewerbsbedingungen für Finanzunternehmen in Bezug auf ihre Regelungsverpflichtungen betreffend IKT-Risiken. Gleichzeitig wird in der Verordnung anerkannt, dass zwischen Finanzunternehmen in Bezug auf Größe, Unternehmensprofile oder das Ausmaß digitaler Risiken erhebliche Unterschiede bestehen. Da größere Finanzunternehmen über mehr Ressourcen verfügen, müssen nur Finanzunternehmen, die nicht als Kleinstunternehmen gelten, beispielsweise komplexe Governance-Regelungen und spezielle Verwaltungsfunktionen einführen und nach größeren Veränderungen an Netz- und Informationssysteminfrastrukturen eingehende Bewertungen sowie regelmäßige Risikoanalysen bei IKT-Altsystemen durchführen und die Prüfung von Plänen für Betriebskontinuität, Gegenmaßnahmen und Wiederherstellung ausweiten, um Szenarien für die Umstellung von ihrer primären IKT-Infrastruktur auf redundante Einrichtungen zu konzipieren. Darüber hinaus werden nur Finanzunternehmen, die für die Zwecke einer erweiterten Prüfung der digitalen Resilienz als bedeutend eingestuft wurden, bedrohungsorientierte Penetrationstests durchführen müssen.

Trotz dieser umfassenden Abdeckung ist dies nicht erschöpfend. Insbesondere werden mit dieser Verordnung weder Systembetreiber im Sinne von Artikel 2 Buchstabe p der Richtlinie 98/26/EG[22] über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen noch Systemteilnehmer erfasst, sofern diese Teilnehmer nicht selbst ein Finanzunternehmen sind, das auf Unionsebene reguliert ist und als solches eigenständig unter diese Verordnung fallen würde (d. h. Kreditinstitut, Wertpapierfirma, zentrale Gegenpartei (CCP)). Darüber hinaus fällt auch das Unionsregister für Emissionszertifikate, das gemäß der Richtlinie 2003/87/EG[23] unter Federführung der Europäischen Kommission betrieben wird, nicht in den Anwendungsbereich.

Mit solchen Ausschlüssen durch die Richtlinie wird der Notwendigkeit einer weiteren Prüfung rechtlicher und politischer Fragen Rechnung getragen, die die Betreiber und Teilnehmer von Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen betreffen, wobei die Auswirkungen der derzeit geltenden Rahmenregelungen für Zahlungssysteme[24], die

---

22 Richtlinie 98/26/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen (ABl. L 166 vom 11.6.1998, S. 45).

23 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).

24 Insbesondere Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme.

von Zentralbanken betrieben werden, gebührend berücksichtigt werden. Da diese Fragen Aspekte einschließen können, die sich von den unter diese Verordnung fallenden Sachverhalten unterscheiden, wird die Kommission die Notwendigkeit und die Auswirkungen einer weiteren Ausweitung des Anwendungsbereichs dieser Verordnung auf Einrichtungen und IKT-Infrastrukturen, die derzeit nicht in ihren Anwendungsbereich fallen, weiter prüfen.

Anforderungen an die Governance (Artikel 4)

Mit dieser Verordnung sollen die Geschäftsstrategien von Finanzunternehmen und das IKT-Risikomanagement besser aufeinander abgestimmt werden. Zu diesem Zweck wird das Leitungsorgan eine entscheidende und aktive Rolle bei der Steuerung des Rahmens für das IKT-Risikomanagement übernehmen und für die Einhaltung einer strikten Cyberhygiene sorgen müssen. Die volle Verantwortung des Leitungsorgans für die Steuerung des IKT-Risikos des Finanzunternehmens wird einen übergeordneten Grundsatz umfassen, der in eine Reihe spezifischer Anforderungen aufzuspalten ist, darunter die Zuweisung klarer Rollen und Zuständigkeiten für alle IKT-bezogenen Funktionen, ein kontinuierliches Engagement bei der Kontrolle der Überwachung des IKT-Risikomanagements sowie der gesamten Bandbreite der Genehmigungs- und Kontrollverfahren und der angemessenen Zuweisung von IKT-Investitionen und -Schulungen.

Anforderungen an das IKT-Risikomanagement (Artikel 5 bis 14)

Die digitale Betriebsstabilität beruht auf einer Reihe zentraler Grundsätze und Anforderungen für den IKT-Risikomanagementrahmen im Einklang mit dem gemeinsamen fachlichen Gutachten der ESA. Diese Anforderungen, die sich an einschlägigen internationalen, nationalen und branchenspezifischen Normen, Leitlinien und Empfehlungen orientieren, betreffen spezifische Funktionen des IKT-Risikomanagements (Identifizierung, Schutz und Prävention, Erkennung, Gegenmaßnahmen und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation). Um mit einer sich rasch ändernden Bedrohungslage Schritt zu halten, müssen Finanzunternehmen stabile IKT-Systeme und -Instrumente einrichten und aufrechterhalten, die die Auswirkungen von IKT-Risiken minimieren, kontinuierlich alle Ursachen von IKT-Risiken ermitteln, Schutz- und Präventionsmaßnahmen ergreifen, anormale Aktivitäten umgehend aufdecken, dedizierte und umfassende Strategien für die Fortführung des Geschäftsbetriebs sowie Notfall- und Wiederherstellungspläne als integralen Bestandteil der operativen Strategie für die Fortführung des Geschäftsbetriebs einrichten. Letztere sind für eine zügige Wiederherstellung nach IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, erforderlich, indem Schäden begrenzt werden und die sichere Fortführung des Geschäftsbetriebs Vorrang erhält. Mit der Verordnung selbst wird keine spezifische Standardisierung vorgeschrieben; vielmehr wird auf europäischen und international anerkannten technischen Normen oder bewährten Branchenverfahren aufgebaut, insofern sie den aufsichtsrechtlichen Anweisungen für die Verwendung und Übernahme solcher internationaler Normen in vollem Umfang entsprechen. Diese Verordnung erstreckt sich ebenfalls auf die Integrität, Sicherheit und Robustheit physischer Infrastrukturen und Einrichtungen, die die Nutzung von Technologien und einschlägigen IKT-bezogenen Prozessen und Personen als Teil des digitalen Fußabdrucks der Geschäftstätigkeit eines Finanzunternehmens unterstützen.

Meldung IKT-bezogener Vorfälle (Artikel 15 bis 20)

Die Harmonisierung und Straffung der Meldung IKT-bezogener Vorfälle wird erreicht, indem Finanzunternehmen zunächst generell verpflichtet werden, einen Managementprozess zur Überwachung und Protokollierung IKT-bezogener Vorfälle einzurichten und umzusetzen; im Anschluss sind diese Vorfälle auf Grundlage der in der Verordnung dargelegten und von den

ESA im Rahmen von Mandaten weiterentwickelten Kriterien zu klassifizieren, um Wesentlichkeitsschwellen festzulegen. Zweitens müssen den zuständigen Behörden nur IKT-bezogene Vorfälle gemeldet werden, die als schwerwiegend gelten. Die Meldung sollte über eine gemeinsame Vorlage und nach einem von den ESA entwickelten harmonisierten Verfahren erfolgen. Finanzunternehmen sollten Erst-, Zwischen- und Abschlussberichte vorlegen und ihre Nutzer und Kunden informieren, sofern der Vorfall Auswirkungen auf ihre finanziellen Interessen hat oder haben könnte. Die zuständigen Behörden sollten anderen Institutionen oder Behörden, d. h. den ESA, der EZB und den in der Richtlinie (EU) 2016/1148 benannten zentralen Anlaufstellen, sachdienliche Einzelheiten zu den Vorfällen mitteilen.

Um einen Dialog zwischen den Finanzunternehmen und den zuständigen Behörden einzuleiten, der dazu beitragen würde, die Auswirkungen möglichst gering zu halten und geeignete Abhilfemaßnahmen zu ermitteln, sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Rückmeldungen und Leitlinien der Aufsichtsbehörden ergänzt werden.

Schließlich sollte die Möglichkeit, IKT-bezogene Vorfälle zentralisiert auf Unionsebene zu melden, in einem gemeinsamen Bericht der ESA, der EZB und der ENISA weiter untersucht werden, indem bewertet wird, ob die Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen machbar ist.

Prüfung der digitalen Betriebsstabilität (Artikel 21 bis 24)

Die im Rahmen für das IKT-Risikomanagement enthaltenen Kapazitäten und Funktionen müssen regelmäßig auf die Abwehrbereitschaft und die Ermittlung von Schwachstellen, Mängeln oder Lücken sowie auf die umgehende Umsetzung von Korrekturmaßnahmen hin geprüft werden. Diese Verordnung ermöglicht eine verhältnismäßige Anwendung der Anforderungen an die Prüfung der digitalen Betriebsstabilität in Abhängigkeit von Größe sowie Geschäfts- und Risikoprofilen von Finanzunternehmen: Zwar sollten alle Unternehmen IKT-Instrumente und -Systeme testen, doch sollten nur diejenigen, die von den zuständigen Behörden (auf der Grundlage der in dieser Verordnung festgelegten und von den ESA weiterentwickelten Kriterien) als bedeutend und cyberreif eingestuft wurden, verpflichtet sein, erweiterte Tests auf der Grundlage bedrohungsorientierter Penetrationstests (TLPT) durchzuführen. Diese Verordnung enthält auch Anforderungen an Prüfer und die unionsweite Anerkennung von TLPT-Ergebnissen für Finanzunternehmen, die in mehreren Mitgliedstaaten operieren.

Risiko durch IKT-Drittanbieter (Artikel 25 bis 39)

Mit der Verordnung soll eine solide Überwachung des Risikos durch IKT-Drittanbieter sichergestellt werden. Dieses Ziel wird zunächst durch die Einhaltung grundsatzbasierter Regeln erreicht, die für die Überwachung des Risikos durch IKT-Drittanbieter durch Finanzunternehmen gelten. Zweitens werden mit dieser Verordnung wesentliche Bestandteile des Dienstes und die Beziehungen zu IKT-Drittanbietern harmonisiert. Diese Bestandteile decken Mindestaspekte ab, die für eine vollständige Überwachung des Risikos durch IKT-Drittanbieter durch das Finanzunternehmen während des Abschlusses, der Erfüllung, der Beendigung und der Nachvertragsphase ihrer Beziehung von entscheidender Bedeutung sind.

Die Verträge, mit denen diese Beziehung geregelt wird, müssen insbesondere eine vollständige Beschreibung der Dienste, Angaben zu den Orten, an denen Daten verarbeitet werden sollen, vollständige Leistungsbeschreibungen mit quantitativen und qualitativen Leistungszielen, einschlägige Bestimmungen über Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten sowie Garantien für den Zugang, die

Wiederherstellung und die Rückgabe bei Ausfall von IKT-Drittanbietern, Kündigungsfristen und Berichtspflichten der IKT-Drittanbieter, Zugangsrechte, Kontroll- und Prüfstrategien des Finanzunternehmens oder eines beauftragten Dritten sowie unmissverständliche Kündigungsrechte und spezielle Ausstiegsstrategien enthalten. Da sich einige dieser Vertragsbestandteile standardisieren lassen, fördert die Verordnung zudem die freiwillige Verwendung von Standardvertragsklauseln, die von der Kommission für die Nutzung von Cloud-Computing-Diensten entwickelt werden sollen.

Schließlich zielt die Verordnung darauf ab, die Konvergenz der Aufsichtskonzepte für das Risiko durch IKT-Drittanbieter im Finanzsektor zu fördern, indem kritische IKT-Drittanbieter einem Aufsichtsrahmen der Union unterworfen werden. Durch einen neuen harmonisierten Rechtsrahmen erhält die ESA, die als federführende Aufsichtsinstanz für jeden dieser kritischen IKT-Drittanbieter benannt wurde, Befugnisse, um sicherzustellen, dass Technologiedienstleister, die entscheidend zum Funktionieren des Finanzsektors beitragen, auf gesamteuropäischer Ebene angemessen überwacht werden. Der in dieser Verordnung vorgesehene Aufsichtsrahmen fußt auf der bestehenden institutionellen Architektur im Finanzdienstleistungsbereich, wobei der Gemeinsame Ausschuss der ESA im Einklang mit seinen Aufgaben im Bereich der Cybersicherheit die sektorübergreifende Koordinierung in Bezug auf alle Aspekte des IKT-Risikos sicherstellt und dabei vom zuständigen Unterausschuss (Aufsichtsforum) unterstützt wird, der vorbereitende Arbeiten für Einzelentscheidungen und gemeinsame Empfehlungen für kritische IKT-Drittanbieter durchführt.

Informationsaustausch (Artikel 40)

Um das Bewusstsein für IKT-Risiken zu schärfen, ihre Ausbreitung zu minimieren, die Abwehrkapazitäten von Finanzunternehmen und die Techniken zur Erkennung von Bedrohungen zu unterstützen, ermöglicht die Verordnung Finanzunternehmen, untereinander Vereinbarungen für den Austausch von Informationen und Erkenntnissen über Cyberbedrohungen zu treffen.

2020/0266 (COD)

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

(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 eines Gesetzgebungsaktes an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank[25],

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[26],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Informations- und Kommunikationstechnologien (IKT) unterstützen im digitalen Zeitalter komplexe Systeme, die für alltägliche gesellschaftliche Aktivitäten eingesetzt werden. Sie sorgen dafür, dass Schlüsselsektoren unserer Volkswirtschaften, einschließlich des Finanzwesens, am Laufen gehalten werden, und verbessern das Funktionieren des Binnenmarkts. Die zunehmende Digitalisierung und Vernetzung verstärken auch die IKT-Risiken, die die Gesellschaft insgesamt – und insbesondere das Finanzsystem – anfälliger für Cyberbedrohungen oder IKT-Störungen machen. Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale aller Tätigkeiten von Finanzunternehmen der Union sind, ist die digitale Resilienz noch nicht ausreichend in ihren operativen Rahmen verankert.

(2) Die Nutzung von IKT hat in den letzten Jahrzehnten einen zentralen Stellenwert im Finanzwesen erlangt und trägt heute entscheidend zur Ausführung typischer alltäglicher Aufgaben aller Finanzunternehmen bei. Auf Digitalisierung beruhen 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, Versicherungsübernahme, Schadenmanagement und Back-Office-Transaktionen. Das Finanzwesen ist nicht nur sektorweit weitgehend digital geworden,

[25] [*Verweis einfügen*] ABl. C, S.
[26] [*Verweis einfügen*] ABl. C, S.

sondern die Digitalisierung hat auch die Verflechtungen und Abhängigkeiten innerhalb des Finanzsektors sowie von Infrastrukturen Dritter und Drittanbietern verstärkt.

(3) Der Europäische Ausschuss für Systemrisiken (ESRB) hat in einem Bericht aus dem Jahr 2020 über systemische Cyberrisiken[27] bekräftigt, wie das bestehende hohe Maß an Verflechtungen zwischen Finanzunternehmen, Finanzmärkten und Finanzmarktinfrastrukturen und insbesondere die Interdependenzen ihrer IKT-Systeme eine Systemanfälligkeit herbeiführen könnten, da lokalisierte Cybervorfälle in einem der rund 22 000 Finanzunternehmen[28] der Union über geografische Grenzen hinweg rasch auf das gesamte Finanzsystem übergreifen könnten. Schwerwiegende IKT-Verstöße im Finanzsektor 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, was zu Liquiditätsengpässen und allgemein zu einem schwindenden Vertrauen in die Finanzmärkte führt.

(4) Nationale, europäische und internationale politische Entscheidungsträger, Regulierungsbehörden und Normungsgremien haben sich in den letzten Jahren mit IKT-Risiken befasst, um die Widerstandsfähigkeit 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 Gruppe der G7- und G20-Staaten bestrebt, den zuständigen Behörden und Marktteilnehmern in verschiedenen Rechtsordnungen Instrumente an die Hand zu geben, um die Widerstandsfähigkeit ihrer Finanzsysteme zu stärken.

(5) IKT-Risiken bleiben trotz gezielter politischer und legislativer Initiativen auf nationaler und europäischer Ebene eine Herausforderung für die Betriebsstabilität, Leistungsfähigkeit und Stabilität des Finanzsystems der Union. Mit der Reform nach der Finanzkrise von 2008 wurde in erster Linie die finanzielle Widerstandsfähigkeit 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, besitzen sie in der Regulierungsagenda in der Zeit nach der Krise weniger Gewicht und wurden nur in einigen Bereichen der Unionspolitik für Finanzdienstleistungen und Regulierung oder nur in wenigen Mitgliedstaaten weiterentwickelt.

(6) Im FinTech-Aktionsplan[29] der Kommission aus dem Jahr 2018 wurde hervorgehoben, wie überaus wichtig es ist, den Finanzsektor der Union auch aus operativer Sicht

---

27 ESRB-Bericht über systemische Cyberrisiken, Februar 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Laut der Folgenabschätzung für die Überprüfung der Europäischen Aufsichtsbehörden SWD(2017) 308 gibt es rund 5665 Kreditinstitute, 5934 Wertpapierfirmen, 2666 Versicherungsunternehmen, 1573 Einrichtungen der betrieblichen Altersversorgung (EbAV), 2500 Anlageverwaltungsgesellschaften, 350 Marktinfrastrukturen (wie CCP, Börsen, systemische Internalisierer, Transaktionsregister und multilaterale Handelssysteme (MTF)), 45 Ratingagenturen und 2500 zugelassene Zahlungsinstitute und E-Geld-Institute. Dies schließt rund 21 233 Unternehmen, jedoch keine Crowdfunding-Unternehmen, Abschlussprüfer und Prüfungsgesellschaften, Anbieter von Krypto-Dienstleistungen und Benchmark-Administratoren ein.

29 Mitteilung der Kommission an das Europäische Parlament, den Rat, die Europäische Zentralbank, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, *FinTech-*

stabiler zu machen, um seine technologische Sicherheit und sein reibungsloses Funktionieren sowie seine rasche Wiederherstellung nach IKT-Verstößen 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 gaben die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) (gemeinsam als „Europäische Aufsichtsbehörden“ oder „ESA“ bezeichnet) gemeinsam zwei fachliche Gutachten heraus, in denen ein kohärenter Ansatz für das IKT-Risiko im Finanzbereich gefordert und empfohlen wurde, die digitale Betriebsstabilität der Finanzdienstleistungsbranche durch eine sektorspezifische Initiative der Union auf verhältnismäßige Weise zu stärken.

(8) Der Finanzsektor der Union wird durch ein harmonisiertes einheitliches Regelwerk reguliert und unterliegt einem europäischen Finanzaufsichtssystem. Dennoch wurden Bestimmungen über die digitale Betriebsstabilität und IKT-Sicherheit noch nicht vollständig oder konsequent harmonisiert, obwohl die digitale Betriebsstabilität 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 diese Komponente abdecken, indem die Mandate von Finanzaufsichtsbehörden, die mit der Überwachung und dem Schutz der Finanzstabilität und der Marktintegrität betraut sind, erweitert werden.

(9) Rechtliche Unterschiede und ungleiche nationale Regulierungs- oder Aufsichtskonzepte in Bezug auf IKT-Risiken schaffen Hindernisse für den Binnenmarkt für Finanzdienstleistungen und erschweren grenzüberschreitend tätigen Finanzunternehmen die reibungslose Ausübung der Niederlassungsfreiheit und die Erbringung von Dienstleistungen. Ebenso kann der Wettbewerb zwischen denselben Arten von Finanzunternehmen, die in verschiedenen Mitgliedstaaten tätig sind, verzerrt sein. Insbesondere in Bereichen, in denen die Harmonisierung auf Unionsebene bislang sehr begrenzt – wie bei der Prüfung der digitalen Betriebsstabilität – oder gar nicht vorhanden ist, wie bei der Überwachung des Risikos durch IKT-Drittanbieter, könnten Unterschiede, die sich aus den auf nationaler Ebene geplanten Entwicklungen ergeben, weitere Hindernisse für das Funktionieren des Binnenmarkts schaffen, die sich nachteilig auf die Marktteilnehmer und die Finanzstabilität auswirken.

(10) Die unvollständige Art und Weise, in der einschlägige Bestimmungen über IKT-Risiken bisher auf Unionsebene angegangen wurden, fördert Lücken oder Überschneidungen in wichtigen Bereichen, wie der Meldung IKT-bezogener Vorfälle und der Prüfung der digitalen Betriebsstabilität, zu Tage und führt zu Unstimmigkeiten aufgrund sich abzeichnender unterschiedlicher nationaler Vorschriften oder einer kostenineffizienten Anwendung sich überschneidender Vorschriften. Dies ist besonders schädlich für intensive IKT-Nutzer wie den Finanzsektor, da technologische

---

Aktionsplan: Für einen wettbewerbsfähigeren und innovativeren europäischen Finanzsektor, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

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 von IKT-Risiken 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 Betriebsstabilität für alle Finanzunternehmen erforderlich. Die Kapazitäten und die allgemeine Resilienz, die Finanzunternehmen auf der Grundlage solcher Kernanforderungen entwickeln würden, um operativen Ausfällen standzuhalten, würden 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 AEUV in der Auslegung der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union stützen.

(12) Mit dieser Verordnung sollen vorrangig die Anforderungen mit Blick auf IKT-Risiken konsolidiert und verbessert werden, die bisher in den einzelnen Verordnungen und Richtlinien gesondert behandelt wurden. Diese Rechtsakte der Union 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 operativer Resilienz ausgerichtet. Bei der Weiterentwicklung der Anforderungen an das operationelle Risiko in den Rechtsakten der Union wurde häufig ein traditioneller quantitativer Ansatz zur Bewältigung von Risiken (d. h. die Festlegung einer Kapitalvorgabe zur Absicherung gegen IKT-Risiken) bevorzugt, anstatt gezielte qualitative Anforderungen zur Stärkung der Kapazitäten durch Vorgaben, die auf den Schutz, die Erkennung, Eindämmung, Wiederherstellung und die Sanierungskapazitäten bei IKT-bezogenen Vorfällen abzielen, oder durch die Festlegung von Kapazitäten für Meldungen und Prüfungen digitaler Technologie einzubetten. Mit diesen Richtlinien und Verordnungen sollten in erster Linie wesentliche Vorschriften über die Aufsicht, die Integrität oder das Verhalten des Marktes abgedeckt werden.

Durch diese Maßnahme, mit der die Vorschriften über IKT-Risiken konsolidiert und aktualisiert werden, würden alle Bestimmungen, die sich mit dem digitalen Risiko im Finanzsektor befassen, erstmals in einheitlicher Weise in einem einzigen Rechtsakt zusammengefasst. Somit sollte diese Initiative Lücken schließen oder Unstimmigkeiten in einigen dieser Rechtsakte beheben (auch in Bezug auf die darin verwendete Terminologie) und durch gezielte Vorschriften über die Kapazitäten für IKT-Risikomanagement, die Meldung und Tests sowie die Überwachung von Risiken durch Drittanbieter ausdrücklich auf IKT-Risiken Bezug nehmen.

(13) Finanzunternehmen sollten bei der Bewältigung von IKT-Risiken denselben Ansatz und dieselben grundsatzbasierten Regeln befolgen. Kohärenz trägt dazu bei, das Vertrauen in das Finanzsystem zu stärken und dessen Stabilität zu erhalten,

insbesondere in Zeiten der übermäßigen Nutzung von IKT-Systemen, -Plattformen und -Infrastrukturen, die erhöhte Risiken im digitalen Bereich 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) Die Anwendung einer Verordnung hilft, die Komplexität der Regulierung zu verringern, fördert die aufsichtliche Konvergenz, erhöht die Rechtssicherheit und trägt gleichzeitig dazu bei, die Befolgungskosten, insbesondere für grenzüberschreitend tätige Finanzunternehmen, zu begrenzen und Wettbewerbsverzerrungen zu verringern. Daher erscheint die Wahl einer Verordnung zur Schaffung eines gemeinsamen Rahmens für die digitale Betriebsstabilität von Finanzunternehmen am besten geeignet, eine einheitliche und kohärente Anwendung aller Komponenten des IKT-Risikomanagements in den Finanzsektoren der Union zu gewährleisten.

(15) Neben den Rechtsvorschriften über Finanzdienstleistungen stellt die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[30] den aktuellen allgemeinen Rahmen für die Cybersicherheit auf Unionsebene dar. Unter den sieben kritischen Sektoren gilt diese Richtlinie auch für drei Arten von Finanzunternehmen, namentlich für Kreditinstitute, Handelsplätze und zentrale Gegenparteien. Da in der Richtlinie (EU) 2016/1148 jedoch ein Mechanismus zur Identifizierung der Betreiber wesentlicher Dienste auf nationaler Ebene vorgesehen ist, werden in der Praxis nur bestimmte Kreditinstitute, Handelsplätze und zentrale Gegenparteien, die von den Mitgliedstaaten ermittelt wurden, in den Anwendungsbereich der Richtlinie aufgenommen und somit verpflichtet, die darin festgelegten Anforderungen an die IKT-Sicherheit und die Meldung von Vorfällen zu erfüllen.

(16) Da mit dieser Verordnung das Ausmaß der Harmonisierung in Bezug auf 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 in den aktuellen Rechtsvorschriften der Union für Finanzdienstleistungen, stellt dies auch im Vergleich zu den Anforderungen der Richtlinie (EU) 2016/1148 eine stärkere Harmonisierung dar. Folglich verkörpert diese Verordnung eine Lex specialis zur Richtlinie (EU) 2016/1148.

Es ist von entscheidender Bedeutung, dass eine enge Beziehung zwischen dem Finanzsektor und dem horizontalen Rahmen der Union für Cybersicherheit aufrechterhalten wird, zumal dies die Kohärenz mit den bereits von den Mitgliedstaaten angenommenen Strategien für Cybersicherheit gewährleisten und Finanzaufsichtsbehörden ermöglichen würde, auf Cybervorfälle aufmerksam gemacht zu werden, die andere unter die Richtlinie (EU) 2016/1148 fallende Sektoren betreffen.

(17) Um einen sektorübergreifenden Lernprozess zu ermöglichen und Erfahrungen anderer Sektoren beim Umgang mit Cyberbedrohungen wirksam zu nutzen, sollten Finanzunternehmen im Sinne der Richtlinie (EU) 2016/1148 Teil des „Ökosystems“ dieser Richtlinie bleiben (z. B. Kooperationsgruppe für Netz- und

[30] 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).

Informationssicherheit (NIS) und Reaktionsteam für Computersicherheitsverletzungen (CSIRT)).

Die ESA und zuständige nationale Behörden sollten in der Lage sein, sich an den strategischen politischen Diskussionen und der technischen Arbeit der NIS-Kooperationsgruppe zu beteiligen, Informationen austauschen und mit den in der Richtlinie (EU) 2016/1148 benannten zentralen Anlaufstellen weiter zusammenarbeiten. Die nach dieser Verordnung zuständigen Behörden sollten auch die gemäß Artikel 9 der Richtlinie (EU) 2016/1148 benannten nationalen CSIRT konsultieren und mit ihnen zusammenarbeiten.

(18) Außerdem ist es wichtig, für Kohärenz mit der Richtlinie über europäische kritische Infrastrukturen („EKI“) zu sorgen, die derzeit überarbeitet wird, um den Schutz und die Widerstandsfähigkeit kritischer Infrastrukturen gegenüber nicht cyberbedingten Bedrohungen mit möglichen Auswirkungen auf den Finanzsektor zu verbessern.[31]

(19) Anbieter von Cloud-Computing-Diensten sind eine Kategorie von Anbietern digitaler Dienste, die unter die Richtlinie (EU) 2016/1148 fallen. Als solche unterliegen sie einer nachträglichen Überwachung durch die gemäß dieser Richtlinie benannten nationalen Behörden, die sich auf die in diesem Rechtsakt festgelegten Anforderungen an die IKT-Sicherheit und die Meldung von Vorfällen beschränkt. Da der mit dieser Verordnung geschaffene Aufsichtsrahmen für alle kritischen IKT-Drittanbieter, einschließlich Anbietern von Cloud-Computing-Diensten, gilt, wenn diese Finanzunternehmen IKT-Dienste erbringen, sollte er als Ergänzung zu der Aufsicht gemäß der Richtlinie (EU) 2016/1148 betrachtet werden. Darüber hinaus sollte der mit dieser Verordnung geschaffene Aufsichtsrahmen für Anbieter von Cloud-Computing-Diensten gelten, wenn es keinen horizontalen sektorunabhängigen Rahmen der Union gibt, mit dem eine Behörde für die digitale Aufsicht eingerichtet wird.

(20) Um die vollständige Kontrolle über IKT-Risiken zu behalten, müssen Finanzunternehmen über umfassende Kapazitäten verfügen, die ein leistungsfähiges und wirksames IKT-Risikomanagement ermöglichen – neben spezifischen Mechanismen und Strategien für die Meldung IKT-bezogener Vorfälle, die Erprobung von IKT-Systemen, -Kontrollen und -Prozessen sowie für die Steuerung des Risikos durch IKT-Drittanbieter. Die Schwelle der digitalen Betriebsstabilität für das Finanzsystem sollte angehoben werden, wobei gleichzeitig eine verhältnismäßige Anwendung der Anforderungen an Finanzunternehmen, bei denen es sich um Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission handelt, möglich sein sollte.[32]

(21) Die Schwellenwerte und Taxonomien für die Meldung IKT-bezogener Vorfälle unterscheiden sich auf nationaler Ebene erheblich. Wenngleich sich durch einschlägige Arbeiten der Agentur der Europäischen Union für Cybersicherheit (ENISA)[33] und der NIS-Kooperationsgruppe für die Finanzunternehmen gemäß der

---

31 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

32 Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

33 ENISA Reference Incident Classification Taxonomy (universelle Taxonomie der ENISA zur Einstufung von Vorfällen), https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

Richtlinie (EU) 2016/1148 eine gemeinsame Grundlage schaffen lässt, bestehen noch immer unterschiedliche Ansätze in Bezug auf Schwellenwerte und Taxonomien bzw. können sich für die übrigen Finanzunternehmen ergeben. Dies beinhaltet eine Vielzahl von Anforderungen, die Finanzunternehmen einhalten müssen, insbesondere wenn sie in mehreren Rechtsordnungen der Union tätig sind und Teil eines Finanzkonzerns sind. Darüber hinaus können diese 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 von IKT-Risiken bei Großangriffen mit potenziell systemischen Folgen von entscheidender Bedeutung ist.

(22) Um den zuständigen Behörden die Erfüllung ihrer 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, müssen Vorschriften festgelegt werden, damit die Regelung für die Meldung IKT-bezogener Vorfälle um die Anforderungen ergänzt wird, die derzeit in den Rechtsvorschriften des Teilsektors Finanzen fehlen, und etwaige Überschneidungen und Doppelarbeit mit Blick auf eine Senkung der Kosten beseitigt werden. Daher ist es von wesentlicher Bedeutung, die Regelung für die Meldung IKT-bezogener Vorfälle zu harmonisieren, indem alle Finanzunternehmen verpflichtet werden, nur ihren zuständigen Behörden Bericht zu erstatten. Darüber hinaus sollten die ESA ermächtigt werden, Aspekte für die Meldung IKT-bezogener Vorfälle wie Taxonomie, Zeitrahmen, Datensätze, Vorlagen und anwendbare Schwellenwerte näher zu spezifizieren.

(23) In einigen Teilsektoren des Finanzsektors haben sich Anforderungen für die Prüfung der digitalen Betriebsstabilität innerhalb mehrerer und unkoordinierter nationaler Rahmen entwickelt, in denen dieselben Sachverhalte unterschiedlich behandelt werden. Dies führt zu doppelten Kosten für grenzüberschreitend tätige Finanzunternehmen und erschwert die gegenseitige Anerkennung von Ergebnissen. Folglich können unkoordinierte Tests den Binnenmarkt segmentieren.

(24) Darüber hinaus bleiben Schwachstellen, wann immer Tests nicht vorgeschrieben sind, unentdeckt, wodurch das Finanzunternehmen und letztlich die Stabilität und Integrität des Finanzsektors einem höheren Risiko unterlägen. Ohne ein Tätigwerden der Union wäre die Prüfung der digitalen Betriebsstabilität weiterhin lückenhaft, und es gäbe keine gegenseitige Anerkennung der Testergebnisse in verschiedenen Rechtsordnungen. Da es unwahrscheinlich ist, dass solche Systeme in anderen Teilsektoren des Finanzsektors in bedeutendem Umfang eingeführt würden, gingen auch die potenziellen Vorteile verloren, wie die Aufdeckung von Schwachstellen und Risiken, Tests von Verteidigungsfähigkeiten und Geschäftskontinuität sowie ein höheres Vertrauen von Kunden, Lieferanten und Geschäftspartnern. Um solche Überschneidungen, Divergenzen und Lücken zu beseitigen, müssen Vorschriften festgelegt werden, die auf koordinierte Tests durch Finanzunternehmen und zuständige Behörden abzielen, damit die gegenseitige Anerkennung erweiterter Tests für wichtige Finanzunternehmen erleichtert wird.

(25) Die Nutzung von IKT-Diensten durch Finanzunternehmen 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 haben sich in den letzten Jahren ständig verändert, was zu Kostensenkungen bei der Finanzintermediation geführt hat, die Expansion von Unternehmen und die Skalierbarkeit bei der Erbringung von Finanztätigkeiten ermöglicht und gleichzeitig ein breites Spektrum an IKT-Instrumenten für die Verwaltung komplexer interner Prozesse zur Verfügung hervorgebracht hat.

(26) Die umfangreiche Nutzung von IKT-Diensten 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 Prüfungsrechte, wenn diese in den Vereinbarungen verankert sind. Darüber hinaus fehlen in vielen dieser Verträge ausreichende Garantien, die eine vollständige Überwachung von Verfahren für die Unterauftragsvergabe ermöglichen, wodurch das Finanzunternehmen diese damit verbundenen Risiken nicht bewerten kann. Da IKT-Drittanbieter häufig standardisierte Dienstleistungen für verschiedene Arten von Kunden anbieten, wird den individuellen oder spezifischen Bedürfnissen der Akteure der Finanzbranche in solchen Verträgen unter Umständen nicht immer angemessen Rechnung getragen.

(27) Trotz einiger allgemeiner Vorschriften über die Auslagerung von Tätigkeiten in einigen Rechtsakten der Union im Bereich der Finanzdienstleistungen 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-Drittanbietern anwendbar sind, fehlen, werden externe Quellen für IKT-Risiken nicht umfassend behandelt. Daher müssen bestimmte Leitprinzipien festgelegt werden, die Finanzunternehmen als Richtschnur für die Steuerung des Risikos durch IKT-Drittanbieter dienen und mit einer Reihe grundlegender vertraglicher Rechte einhergehen, die sich auf mehrere Aspekte bei der Erfüllung und Beendigung von Verträgen beziehen, damit bestimmte Mindestgarantien verankert werden, die Finanzunternehmen bei der wirksamen Überwachung aller Risiken auf Ebene von IKT-Drittanbietern unterstützen.

(28) Die Homogenität und Konvergenz in Bezug auf die Risiken durch IKT-Drittanbieter und die Abhängigkeit von IKT-Drittanbietern ist mangelhaft. Obwohl einige Anstrengungen unternommen wurden, um den spezifischen Bereich der Auslagerung anzugehen, wie die Empfehlungen aus dem Jahr 2017 zur Auslagerung der Anbieter von Cloud-Diensten[34], wird das Problem systemischer Risiken, das entstehen könnte, weil der Finanzsektor einer begrenzten Anzahl kritischer IKT-Drittanbieter ausgesetzt ist, in den Rechtsvorschriften der Union kaum behandelt. Dieser Mangel auf Unionsebene wird noch dadurch verschärft, dass keine spezifischen Mandate und Instrumente bestehen, die es nationalen Aufsichtsbehörden ermöglichen, Abhängigkeiten von IKT-Drittanbietern ordnungsgemäß zu erfassen und Risiken, die sich aus der Konzentration solcher Abhängigkeiten von IKT-Drittanbietern ergeben, angemessen zu überwachen.

(29) Unter Berücksichtigung der potenziellen Systemrisiken, die mit der verstärkten Auslagerung und der Konzentration der Abhängigkeiten von IKT-Drittanbietern

[34] Empfehlungen zur Auslagerung an Cloud-Anbieter (EBA/REC/2017/03), inzwischen aufgehoben durch die EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02).

verbunden sind, und in Anbetracht unzureichender nationaler Regelungen, die es Finanzaufsichtsbehörden ermöglichen, die Folgen der bei kritischen IKT-Drittanbietern auftretenden IKT-Risiken zu quantifizieren, zu qualifizieren und zu beheben, muss ein geeigneter Aufsichtsrahmen der Union geschaffen werden, der eine kontinuierliche Überwachung der Tätigkeiten von IKT-Drittanbietern, die für Finanzunternehmen systemrelevant sind, ermöglicht.

(30) Da IKT-Bedrohungen komplexer und technisch ausgereifter werden, hängen gute Erkennungs- und Präventionsmaßnahmen in hohem Maße von einem regelmäßigen Informationsaustausch zwischen Finanzunternehmen über Bedrohungen und Anfälligkeiten ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen, wodurch Finanzunternehmen Bedrohungen bekämpfen können, bevor sie in reale Vorfälle münden, und in der Lage sind, die Auswirkungen IKT-bezogener Vorfälle besser einzudämmen und effizienter zu reagieren. 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.

(31) Darüber hinaus führen Unsicherheiten 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. Umfang und Qualität des Informationsaustauschs sind 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 Finanzsektors zugeschnitten sind.

(32) Daher sollten Finanzunternehmen ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren. Dementsprechend 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, Bedrohungen vorzubeugen und gemeinsam darauf zu reagieren, indem die Ausbreitung von IKT-Risiken rasch eingedämmt und potenzielle Ansteckungseffekte über alle Finanzkanäle hinweg verhindert werden. Diese Regelungen sollten unter uneingeschränkter Einhaltung des anwendbaren Wettbewerbsrechts der Union[35] sowie in einer Weise eingerichtet werden, die die uneingeschränkte Einhaltung der Datenschutzvorschriften der Union und hauptsächlich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[36] gewährleistet – insbesondere im Zusammenhang mit der Verarbeitung personenbezogener Daten, die zur Wahrung der

[35] Mitteilung der Kommission – Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit, 2011/C 11/01.

[36] 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).

berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung erforderlich ist.

(33) Ungeachtet des in dieser Verordnung vorgesehenen breiten Geltungsbereichs sollten bei der Anwendung der Vorschriften für die digitale Betriebsstabilität wesentliche Unterschiede zwischen Finanzunternehmen in Bezug auf Größe, Unternehmensprofile oder digitale Risiken berücksichtigt werden. Finanzunternehmen sollten bei der Zuordnung von Ressourcen und Kapazitäten zur Umsetzung des Rahmens für das IKT-Risikomanagement ihren IKT-Bedarf sorgfältig auf ihre Größe und ihr Profil abstimmen, während die zuständigen Behörden den Ansatz einer solchen Verteilung weiterhin bewerten und überprüfen sollten.

(34) 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 zu treffen. Solche Unternehmen sind besser gerüstet, um insbesondere spezielle Verwaltungsfunktionen für die Überwachung von Vereinbarungen mit IKT-Drittanbietern oder für den Umgang mit dem Krisenmanagement einzurichten, ihr IKT-Risikomanagement nach dem Modell der drei Verteidigungslinien zu strukturieren oder ein HR-Dokument zu verabschieden, in dem Richtlinien für die Zugangsrechte umfassend erläutert werden.

Ebenso sollten nur solche Finanzunternehmen aufgefordert werden, nach größeren Veränderungen der Netz- und Informationssysteminfrastrukturen und -prozesse eingehende Bewertungen durchzuführen, regelmäßig Risikoanalysen von IKT-Altsystemen vorzunehmen oder die Prüfung der Pläne für die Fortführung des Geschäftsbetriebs, Reaktion und Wiederherstellung auszuweiten, um Szenarien für die Umstellung von primärer IKT-Infrastruktur auf redundante Systeme zu erfassen.

(35) Da darüber hinaus nur die Finanzunternehmen, die für die Zwecke der erweiterten Prüfung der digitalen Resilienz als bedeutend eingestuft wurden, zu bedrohungsorientierten Penetrationstests verpflichtet werden sollten, sollten die Verwaltungsverfahren und finanziellen Kosten, die mit der Durchführung solcher Tests verbunden sind, einem kleinen Prozentsatz der Finanzunternehmen übertragen werden. Schließlich sollten zur Verringerung der Regulierungslast nur Finanzunternehmen, die keine Kleinstunternehmen sind, aufgefordert werden, den zuständigen Behörden regelmäßig alle Kosten und Verluste, die durch IKT-Unterbrechungen verursacht werden, sowie die Ergebnisse von Prüfungen nach erheblichen IKT-Störungen zu melden.

(36) Um die vollständige Abstimmung und allgemeine Kohärenz zwischen den Geschäftsstrategien der Finanzunternehmen einerseits und der Durchführung des IKT-Risikomanagements andererseits zu gewährleisten, sollte das Leitungsorgan verpflichtet sein, bei der Steuerung und Anpassung des IKT-Risikomanagementrahmens und der Gesamtstrategie für die digitale Resilienz eine zentrale und aktive Rolle zu bewahren. Der vom Leitungsorgan 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 Strategien 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 die Steuerung der IKT-Risiken 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.

(37) Darüber hinaus geht die uneingeschränkte Rechenschaftspflicht des Leitungsorgans mit der Sicherstellung eines bestimmten Umfangs von IKT-Investitionen und eines Gesamthaushalts einher, damit das Finanzunternehmen in der Lage ist, die Mindestanforderungen an die digitale Betriebsstabilität umzusetzen.

(38) Aufbauend auf einschlägigen internationalen, nationalen und branchenspezifischen Standards, Leitlinien, Empfehlungen oder Konzepten für die Steuerung von Cyberrisiken[37] werden mit dieser Verordnung eine Reihe von Funktionen gefördert, die die allgemeine Strukturierung des IKT-Risikomanagements erleichtern. Solange die wichtigsten von Finanzunternehmen eingerichteten Kapazitäten auf die Ziele abgestimmt sind, die in den Funktionen (Ermittlung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation) in dieser Verordnung vorgesehen sind, steht es Finanzunternehmen frei, IKT-Risikomanagementmodelle zu verwenden, die anders gegliedert oder kategorisiert sind.

(39) Um mit einer sich rasch ändernden Bedrohungslage Schritt zu halten, sollten Finanzunternehmen auf dem neuesten Stand befindliche IKT-Systeme unterhalten, die zuverlässig sind und über ausreichende Kapazitäten verfügen, um nicht nur die Verarbeitung der Daten, wie sie für die Erbringung ihrer Dienste erforderlich ist, sondern auch die technologische Resilienz zu gewährleisten, damit Finanzunternehmen in angemessener Weise auf zusätzliche Verarbeitungserfordernisse reagieren können, die durch angespannte Marktbedingungen oder andere ungünstige Umstände entstehen können. Obwohl in dieser Verordnung keine Standardisierung spezifischer IKT-Systeme, -Instrumente oder -Technologien vorgesehen ist, stützt sie sich auf die angemessene Anwendung europäischer und international anerkannter technischer Normen (z. B. ISO) oder bewährter Branchenverfahren durch die Finanzunternehmen, insofern diese Anwendung den spezifischen Aufsichtsanweisungen für die Verwendung und Übernahme internationaler Normen in vollem Umfang entspricht.

(40) Effiziente Pläne für die Geschäftskontinuität und 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 Vorrang erhalten. Obwohl Systeme für die Datensicherung unverzüglich mit der Verarbeitung beginnen sollten, darf die Integrität und Sicherheit

---

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (Leitfaden zur Widerstandsfähigkeit gegenüber Cyberangriffen für Finanzmarktinfrastrukturen), https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector* (Grundzüge der Cybersicherheit für den Finanzsektor der G-7-Staaten), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework (NIST-Rahmen für Cybersicherheit), https://www.nist.gov/cyberframework; FSB *CIRR toolkit* (Toolkit des FSB für den Umgang mit Cybervorfällen), https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

der Netz- und Informationssysteme oder die Vertraulichkeit von Daten durch einen solchen unverzüglichen Beginn in keiner Weise gefährdet werden.

(41) Mit dieser Verordnung wird Finanzunternehmen zwar ermöglicht, die zeitlichen Vorgaben bis zur Wiederherstellung flexibel und so festzulegen, dass Art und der Kritikalität der jeweiligen Funktion und etwaige spezifische geschäftliche Erfordernisse in vollem Umfang berücksichtigt werden, doch sollte bei der Festlegung dieser Vorgaben auch eine Bewertung der potenziellen Gesamtauswirkungen auf die Markteffizienz vorgeschrieben sein.

(42) Die weitreichenden Folgen von Cyberangriffen werden verstärkt, wenn sie sich im Finanzsektor und damit in einem Bereich ereignen, in dem die Gefahr viel größer ist, dass böswillige Verbreiter direkt an der Quelle finanzielle Gewinne erzielen. Um solche Risiken zu mindern und zu verhindern, dass IKT-Systeme ihre Integrität einbüßen oder nicht verfügbar werden und vertrauliche Daten eingesehen oder physische IKT-Infrastrukturen beschädigt werden, sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen erheblich verbessert werden.

Die Meldung IKT-bezogener Vorfälle sollte für alle Finanzunternehmen harmonisiert werden, indem sie verpflichtet werden, nur ihren zuständigen Behörden Bericht zu erstatten. Obwohl alle Finanzunternehmen dieser Meldepflicht unterlägen, sollten nicht alle in gleicher Weise betroffen sein, da einschlägige Wesentlichkeitsschwellen und Zeitrahmen so austariert werden sollten, dass nur schwerwiegende IKT-bezogene Vorfälle erfasst werden. Eine direkte Meldung würde Finanzaufsichtsbehörden den Zugang zu Informationen über IKT-bezogene Vorfälle ermöglichen. Dennoch sollten Finanzaufsichtsbehörden diese Informationen an Nicht-Finanzbehörden (für Netzwerk- und Informationssicherheit zuständige Behörden, nationale Datenschutzbehörden und Strafverfolgungsbehörden bei Vorfällen strafrechtlicher Art) weiterleiten. Die Informationen über IKT-bezogene Vorfälle sollten wechselseitig gelenkt werden: Die Finanzaufsichtsbehörden sollten dem Finanzunternehmen alle erforderlichen Rückmeldungen oder Orientierungshilfen geben, während die ESA anonymisierte Daten über Bedrohungen und Schwachstellen im Zusammenhang mit einem Ereignis austauschen sollten, um eine umfassende kollektive Verteidigung zu unterstützen.

(43) Weitere Überlegungen über die mögliche Zentralisierung von Berichten über IKT-bezogene Vorfälle sollten in Betracht gezogen werden, indem eine einheitliche zentrale EU-Plattform entweder direkt die entsprechenden Meldungen entgegennimmt und die zuständigen nationalen Behörden automatisch benachrichtigt oder lediglich die von den zuständigen nationalen Behörden übermittelten Meldungen zentralisiert und eine Koordinierungsfunktion wahrnimmt. Die ESA sollten verpflichtet sein, in Absprache mit der EZB und der ENISA bis zu einem bestimmten Tag einen gemeinsamen Bericht über die Machbarkeit der Einrichtung einer solchen zentralen EU-Plattform auszuarbeiten.

(44) Um eine robuste digitale Betriebsstabilität zu erreichen und internationale Standards zu übernehmen (z. B. die „G7 Fundamental Elements for Threat-Led Penetration Testing“ (Grundzüge bedrohungsorientierter Penetrationstests der G7-Staaten)), sollten Finanzunternehmen ihre IKT-Systeme und -Mitarbeiter regelmäßig auf die Effizienz ihrer Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung hin überprüfen, um potenzielle IKT-Schwachstellen aufzudecken und zu beseitigen. Um den Unterschieden Rechnung zu tragen, die zwischen und in

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 Anfälligkeit, Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests oder End-to-End-Tests) bis hin zu erweiterten Prüfungen (z. B. TLPT für Finanzunternehmen, die aus IKT-Perspektive ausgereift genug sind) reichen. Folglich sollte die Prüfung der digitalen Betriebsstabilität für große Finanzunternehmen (wie große Kreditinstitute, Börsen, Zentralverwahrer, zentrale Gegenparteien usw.) ausgedehnter sein. Gleichzeitig sollte die Prüfung der digitalen Betriebsstabilität für einige Teilsektoren, die eine zentrale und systemrelevante Rolle spielen (z. B. Zahlungen, Banken, Clearing und Abrechnung), mehr Relevanz und für andere Teilsektoren (z. B. Vermögensverwalter, Ratingagenturen usw.) weniger Relevanz besitzen. Grenzübergreifend tätige Finanzunternehmen, die ihre Niederlassungs- oder Dienstleistungsfreiheit in der Union ausüben, sollten in ihrem Herkunftsmitgliedstaat eine einheitliche Reihe von Anforderungen für erweiterte Prüfungen (z. B. TLPT) erfüllen, und diese Tests sollten sich auf die IKT-Infrastrukturen in allen Rechtsordnungen erstrecken, in denen die grenzüberschreitende Gruppe innerhalb der Union tätig ist, sodass grenzüberschreitend tätigen Gruppen nur in einer Rechtsordnung Testkosten entstehen.

(45) Um eine solide Überwachung des Risikos durch IKT-Drittanbieter zu gewährleisten, sind eine Reihe grundsatzbasierter Regeln festzulegen, um Finanzunternehmen bei der Überwachung der Risiken anzuleiten, die im Zusammenhang mit an IKT-Drittanbieter ausgelagerten Funktionen und ganz allgemein im Zusammenhang mit Abhängigkeiten von IKT-Drittanbietern entstehen.

(46) Ein Finanzunternehmen sollte jederzeit die volle Verantwortung für die Einhaltung der Verpflichtungen aus dieser Verordnung tragen. Es sollte eine verhältnismäßige Überwachung der Risiken, die auf Ebene des IKT-Drittanbieters entstehen, organisiert werden, indem Umfang, Komplexität und Bedeutung IKT-bezogener Abhängigkeiten, die Kritikalität oder Bedeutung der Dienste, Prozesse oder Funktionen, die den vertraglichen Vereinbarungen unterliegen, letztlich je nach Sachlage anhand einer sorgfältigen Bewertung potenzieller Auswirkungen auf die Kontinuität und Qualität von Finanzdienstleistungen auf Einzel- und Gruppenebene gebührend berücksichtigt werden.

(47) Die Durchführung einer solchen Überwachung sollte nach einem strategischen Ansatz für das Risiko durch IKT-Drittanbieter erfolgen, der durch die Annahme einer eigenen Strategie durch das Leitungsorgan des Finanzunternehmens formalisiert wird, und zwar auf Grundlage einer kontinuierlichen Überprüfung aller Abhängigkeiten von IKT-Drittanbietern. Um die Aufsichtsbehörden für Abhängigkeiten von IKT-Drittanbietern zu sensibilisieren und den durch diese Verordnung geschaffenen Aufsichtsrahmen weiter zu unterstützen, sollten Finanzaufsichtsbehörden regelmäßig wesentliche Informationen aus den Registern erhalten und auf Ad-hoc-Basis Auszüge anfordern können.

(48) Dem förmlichen Abschluss vertraglicher Vereinbarungen sollte eine gründliche Analyse vor Vertragsabschluss zugrunde liegen und diesem vorausgehen, während die Kündigung von Verträgen zumindest durch eine Reihe von Umständen ausgelöst werden sollte, die Unzulänglichkeiten bei dem IKT-Drittanbieter erkennen lassen.

(49) Um den systemischen Auswirkungen des Konzentrationsrisikos von IKT-Drittanbietern entgegenzuwirken, sollte eine ausgewogene Lösung durch einen flexiblen und schrittweisen Ansatz gefördert werden, da starre Obergrenzen oder strenge Beschränkungen die Geschäftstätigkeit und die Vertragsfreiheit behindern können. Finanzunternehmen sollten vertragliche Vereinbarungen gründlich prüfen, um die Wahrscheinlichkeit eines solchen Risikos zu ermitteln, unter anderem durch fundierte Analysen von Vereinbarungen über weiteres Outsourcing, insbesondere wenn diese mit IKT-Drittanbietern geschlossen werden, die in einem Drittland niedergelassen sind. Zum gegenwärtigen Zeitpunkt wird es im Hinblick auf ein ausgewogenes Verhältnis zwischen dem Sachzwang, die Vertragsfreiheit zu wahren und Finanzstabilität zu gewährleisten, nicht als angemessen erachtet, strenge Obergrenzen und Beschränkungen für Geschäftsbeziehungen zu IKT-Drittanbietern vorzusehen. Die mit der Aufsicht über jeden kritischen IKT-Drittanbieter beauftragte ESA (im Folgenden „federführende Aufsichtsinstanz“) sollte bei der Wahrnehmung ihrer Aufsichtsaufgaben besonders darauf achten, das Ausmaß wechselseitiger Abhängigkeiten voll zu erfassen und spezifische Fälle zu ermitteln, in deren Rahmen eine hohe Konzentration kritischer IKT-Drittanbieter in der Union die Stabilität und Integrität des Finanzsystems der Union belasten dürfte, und einen Dialog mit kritischen IKT-Drittanbietern einrichten, bei denen dieses Risiko festgestellt wird.[38]

(50) Um die Fähigkeit des IKT-Drittanbieters, sichere Dienstleistungen für das Finanzunternehmen ohne nachteilige Auswirkungen auf dessen Resilienz zu erbringen, regelmäßig überwachen und überprüfen zu können, sollten wesentliche Vertragsbestandteile während der gesamten Ausführung von Verträgen mit IKT-Drittanbietern harmonisiert werden. Diese Elemente decken nur vertragliche Mindestaspekte ab, die für eine umfassende Überwachung durch das Finanzunternehmen unter dem Gesichtspunkt, seine digitale Resilienz auf Basis der Stabilität und Sicherheit des IKT-Dienstes zu gewährleisten, von entscheidender Bedeutung sind.

(51) Um eine wirksame Überwachung durch das Finanzunternehmen zu ermöglichen, sollte in den vertraglichen Vereinbarungen insbesondere eine Spezifikation vollständiger Beschreibungen von Funktionen und Dienstleistungen sowie von Orten vorgesehen sein, an denen solche Funktionen bereitgestellt und Daten verarbeitet werden; ebenso müssen vollständige Leistungsbeschreibungen mit quantitativen und qualitativen Leistungszielen innerhalb vereinbarter Serviceniveaus enthalten sein. In gleicher Weise sollten Bestimmungen über Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten sowie Garantien für den Zugang, die Wiederherstellung und die Rückgabe bei Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit des IKT-Drittanbieters ebenfalls als wesentliche Aspekte für die Fähigkeit eines Finanzunternehmens betrachtet werden, das durch Drittanbieter bedingte Risiko zu überwachen.

(52) Damit Finanzunternehmen die volle Kontrolle über alle Entwicklungen behalten, die ihre IKT-Sicherheit beeinträchtigen könnten, sollten bei Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittanbieters auswirken könnten, kritische oder wichtige Funktionen wirksam wahrzunehmen, darunter auch die Unterstützung durch

[38] Falls das Risiko eines Missbrauchs durch einen IKT-Drittanbieter, der als marktbeherrschend angesehen wird, besteht, sollten Finanzunternehmen außerdem die Möglichkeit haben, bei der Europäischen Kommission oder bei den nationalen Wettbewerbsbehörden entweder eine formelle oder eine informelle Beschwerde einzureichen.

diesen Anbieter bei IKT-bezogenen Vorfällen ohne zusätzliche Kosten oder zu vorab festgelegten Kosten, Kündigungsfristen und Meldepflichten des IKT-Drittanbieters festgelegt werden.

(53) Zugangs-, Inspektions- und Prüfrechte des Finanzunternehmens oder eines beauftragten Dritten sind wesentliche Instrumente für die laufende Überwachung der Leistung des IKT-Drittanbieters durch die Finanzunternehmen, die mit der uneingeschränkten Zusammenarbeit des Drittanbieters bei den Prüfungen einhergeht. In gleicher Weise sollte die zuständige Behörde des Finanzunternehmens auf der Grundlage von Mitteilungen über die Rechte verfügen, den IKT-Drittanbieter unter Wahrung der Vertraulichkeit zu inspizieren und zu prüfen.

(54) Vertragliche Vereinbarungen sollten klare Kündigungsrechte und entsprechende Mindestfristen sowie spezielle Ausstiegsstrategien vorsehen, die insbesondere verbindliche Übergangszeiträume ermöglichen, in denen die IKT-Drittanbieter weiterhin die einschlägigen Funktionen bereitstellen sollten, um das Risiko von Störungen auf Ebene des Finanzunternehmens zu verringern oder es Letzterem zu ermöglichen, effektiv zu anderen IKT-Drittanbietern zu wechseln oder alternativ auf die Nutzung von Lösungen vor Ort zurückzugreifen, die der Komplexität des bereitgestellten Dienstes entsprechen.

(55) Darüber hinaus kann die freiwillige Verwendung von Standardvertragsklauseln, die von der Kommission für Cloud-Computing-Dienste entwickelt wurden, Finanzunternehmen und ihren IKT-Drittanbietern eine zusätzliche Rückversicherung bieten, indem sie die Rechtssicherheit bei der Nutzung von Cloud-Computing-Diensten durch den Finanzsektor in voller Übereinstimmung mit den Anforderungen und Erwartungen in der Verordnung über Finanzdienstleistungen erhöht. Diese Arbeiten bauen 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.

(56) Um die Konvergenz und Effizienz von Aufsichtskonzepten für das Risiko durch IKT-Drittanbieter für den Finanzsektor zu fördern, die digitale Betriebsstabilität von Finanzunternehmen zu stärken, die für die Bereitstellung operativer Funktionen auf kritische IKT-Drittanbieter angewiesen sind, und damit dazu beizutragen, die Stabilität des Finanzsystems der Union und die Integrität des Binnenmarkts für Finanzdienstleistungen zu bewahren, sollten kritische IKT-Drittanbieter einem Aufsichtsrahmen der Union unterliegen.

(57) Da nur kritische IKT-Drittanbieter eine besondere Behandlung rechtfertigen, sollte für die Zwecke der Anwendung des Aufsichtsrahmens der Union ein Benennungsverfahren eingeführt werden, um dem Ausmaß und der Art der Abhängigkeit des Finanzsektors von solchen IKT-Drittanbietern Rechnung zu tragen, was sich in einer Reihe quantitativer und qualitativer Kriterien niederschlägt, mit denen die Kritikalitätsparameter als Grundlage für die Einbeziehung in die Aufsicht festgelegt würden. Kritische IKT-Drittanbieter, die aufgrund der Anwendung der oben genannten Kriterien nicht automatisch benannt werden, sollten die Möglichkeit haben, sich freiwillig für den Aufsichtsrahmen zu entscheiden, während IKT-Drittanbieter, die bereits Aufsichtsrahmen unterliegen, die auf Ebene des Eurosystems

zur Unterstützung der in Artikel 127 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union genannten Aufgaben festgelegt wurden, ausgenommen werden sollten.

(58) Das Erfordernis der Registrierung von Drittanbietern, die als kritisch eingestuft wurden, in der Union ist keiner Lokalisierung der Daten gleichzusetzen, da diese Verordnung keine weiteren Anforderungen für die Speicherung oder Verarbeitung von Daten in der Union enthält.

(59) Dieser Rahmen sollte nicht die Zuständigkeit der Mitgliedstaaten berühren, eigene Überwachungen in Bezug auf IKT-Drittanbieter durchzuführen, die im Rahmen dieser Verordnung nicht kritisch sind, aber auf nationaler Ebene als wichtig angesehen werden könnten.

(60) Um die aktuelle 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 und dabei durch einen neuen Unterausschuss (Aufsichtsforum) unterstützt werden, der sowohl Einzelentscheidungen, die sich an kritische IKT-Drittanbieter richten, als auch gemeinsame Empfehlungen, insbesondere zum Benchmarking der Überwachungsprogramme kritischer IKT-Drittanbieter und zur Ermittlung bewährter Verfahren zur Bewältigung von Problemen im Zusammenhang mit IKT-Konzentrationsrisiken, ausarbeitet.

(61) Um sicherzustellen, dass IKT-Drittanbieter, die entscheidend zum Funktionieren des Finanzsektors beitragen, auf Unionsebene angemessen beaufsichtigt werden, sollte eine der ESA als federführende Aufsichtsinstanz für jeden kritischen IKT-Drittanbieter benannt werden.

(62) Federführende Aufsichtsinstanzen sollten über die erforderlichen Befugnisse verfügen, um bei kritischen IKT-Drittanbietern Untersuchungen, Prüfungen am Standort und außerhalb des Standorts durchzuführen, Zugang zu allen einschlägigen Räumlichkeiten und Standorten und vollständige und aktuelle Informationen zu erhalten, damit sie Art, Ausmaß und Auswirkungen des Risikos durch IKT-Drittanbieter, das für die Finanzunternehmen und letztlich für das Finanzsystem der Union besteht, wahrheitsgetreu erfassen können.

Die Übertragung der federführenden Aufsicht auf die ESA ist eine Voraussetzung dafür, die systemische Dimension des IKT-Risikos im Finanzwesen zu erfassen und zu berücksichtigen. Der unionsweite Fußabdruck kritischer IKT-Drittanbieter und die damit verbundenen potenziellen Probleme durch das IKT-Konzentrationsrisiko erfordern einen kollektiven Ansatz auf Unionsebene. Die Wahrnehmung mehrfacher Prüfungs- und Zugangsrechte, die von zahlreichen zuständigen Behörden separat mit geringer oder keiner Koordinierung erfolgte, würde keinen vollständigen Überblick über das Risiko durch IKT-Drittanbieter verschaffen und gleichzeitig unnötige Redundanzen, Belastungen und Komplexitäten auf Ebene kritischer IKT-Drittanbieter mit sich bringen, die mit solch zahlreichen Anfragen konfrontiert sind.

(63) Darüber hinaus sollten federführende Aufsichtsinstanzen in der Lage sein, Empfehlungen zu IKT-Risiken und geeigneten Abhilfemaßnahmen abzugeben, einschließlich der Ablehnung bestimmter vertraglicher Vereinbarungen, die letztlich die Stabilität des Finanzunternehmens oder des Finanzsystems beeinträchtigen. Die zuständigen nationalen Behörden sollten im Rahmen ihrer Aufgabe im

Zusammenhang mit der Beaufsichtigung von Finanzunternehmen gebührend berücksichtigen, ob die von den federführenden Aufsichtsinstanzen ausgesprochenen wesentlichen Empfehlungen eingehalten werden.

(64) Der Aufsichtsrahmen ersetzt nicht die Steuerung des Risikos, das die Nutzung von IKT-Drittanbietern mit sich bringt, durch Finanzunternehmen und tritt weder in irgendeiner Form noch für irgendeinen Aspekt an deren Stelle; dies schließt auch die Verpflichtung zur laufenden Überwachung der mit kritischen IKT-Drittanbietern geschlossenen vertraglichen Vereinbarungen ein und lässt die volle Verantwortung der Finanzunternehmen für die Einhaltung und Erfüllung aller Anforderungen dieser Verordnung und der einschlägigen Rechtsvorschriften über Finanzdienstleistungen unberührt. Um Doppelarbeit und Überschneidungen zu vermeiden, sollten die zuständigen Behörden davon absehen, im Alleingang Maßnahmen zur Überwachung der Risiken durch kritische IKT-Drittanbieter zu ergreifen. Etwaige Maßnahmen sollten zuvor im Rahmen des Aufsichtsrahmens koordiniert und vereinbart werden.

(65) Um auf internationaler Ebene die Konvergenz in Bezug auf bewährte Verfahren zu fördern, die für die Überprüfung der Steuerung digital bedingter Risiken durch IKT-Drittanbieter zu nutzen sind, sollten die ESA aufgefordert werden, Kooperationsvereinbarungen mit den zuständigen Aufsichtsbehörden und Regulierungsbehörden in Drittländern zu schließen, um die Entwicklung bewährter Verfahren zur Bewältigung des Risikos durch IKT-Drittanbieter zu erleichtern.

(66) Um das technische Fachwissen zuständiger Behörden im Bereich der Steuerung von operationellen und IKT-Risiken zu nutzen, sollten federführende Aufsichtsinstanzen auf nationale Aufsichtserfahrung zurückgreifen und für jeden einzelnen kritischen IKT-Drittanbieter spezielle Untersuchungsteams einrichten und multidisziplinäre Teams zusammenlegen, um sowohl die Vorbereitung als auch die tatsächliche Wahrnehmung von Aufsichtstätigkeiten zu unterstützen, einschließlich Vor-Ort-Prüfungen kritischer IKT-Drittanbieter sowie der erforderlichen Folgemaßnahmen.

(67) Zuständige Behörden sollten über alle erforderlichen Aufsichts-, Untersuchungs- und Sanktionsbefugnisse verfügen, um die Anwendung dieser Verordnung sicherzustellen. Verwaltungssanktionen sollten grundsätzlich veröffentlicht werden. Da Finanzunternehmen und kritische IKT-Drittanbieter in unterschiedlichen Mitgliedstaaten ansässig sein und der Aufsicht unterschiedlicher sektoraler Behörden unterliegen können, ist 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[39] übertragenen besonderen Aufgaben und die Abstimmung mit den ESA durch gegenseitigen Informationsaustausch und die Erbringung von Amtshilfe in Aufsichtsbelangen zu gewährleisten.

(68) Um die Benennungskriterien für kritische IKT-Drittanbieter weiter zu quantifizieren und zu präzisieren und Aufsichtsgebühren zu harmonisieren, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte in Bezug auf Folgendes zu erlassen: die weitere Präzisierung der systemischen Auswirkungen, die ein Ausfall eines Dienstes eines IKT-Drittanbieters auf die von ihm bedienten Finanzunternehmen haben könnte; die Zahl global systemrelevanter Institute (G-SRI) oder anderer

[39] 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).

systemrelevanter Institute (A-SRI), die auf den jeweiligen IKT-Drittanbieter angewiesen sind; die Zahl der IKT-Drittanbieter, die auf einem bestimmten Markt tätig sind; die Kosten für die Migration zu einem anderen IKT-Drittanbieter; die Zahl der Mitgliedstaaten, in denen der betreffende IKT-Drittanbieter Dienste erbringt und in denen Finanzunternehmen, die den jeweiligen IKT-Drittanbieter nutzen, operieren; den Betrag der Aufsichtsgebühren und die damit verbundene Zahlungsweise.

Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt wurden.[40] 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, während deren Sachverständige systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission besitzen, die mit der Ausarbeitung der delegierten Rechtsakte befasst sind.

(69) Da diese Verordnung in Verbindung mit der Richtlinie (EU) 20xx/xx des Europäischen Parlaments und des Rates[41] 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, sollten diese Verordnungen mit Blick auf die volle Übereinstimmung geändert werden, damit klargestellt ist, dass die einschlägigen Bestimmungen über IKT-Risiken in dieser Verordnung verankert sind.

Die konsequente Harmonisierung der in dieser Verordnung festgelegten Anforderungen sollte mit technischen Standards gewährleistet werden. Als Einrichtungen mit hochspezialisierten Fachkräften sollten die ESA beauftragt werden, Entwürfe technischer Regulierungsstandards auszuarbeiten, die keine politischen Entscheidungen erfordern, und der Kommission vorzulegen. In den Bereichen IKT-Risikomanagement, Berichterstattung, Prüfung und Kernanforderungen für eine solide Überwachung des Risikos durch IKT-Drittanbieter sollten technische Regulierungsstandards entwickelt werden.

(70) Besonders wichtig ist, dass die Kommission bei ihren vorbereitenden Arbeiten angemessene Konsultationen, auch auf Sachverständigenebene, durchführt. Die Kommission und die ESA sollten sicherstellen, dass diese Standards und Anforderungen von allen Finanzunternehmen auf eine Weise angewandt werden können, die der Art, dem Umfang und der Komplexität dieser Unternehmen und ihrer Tätigkeiten angemessen ist.

(71) Um die Vergleichbarkeit der Berichte über schwerwiegende IKT-bezogene Vorfälle zu erleichtern und für Transparenz in Bezug auf vertragliche Vereinbarungen über die Nutzung von IKT-Diensten von Drittanbietern zu sorgen, sollten die ESA beauftragt werden, Entwürfe technischer Durchführungsstandards zu erarbeiten, mit denen standardisierte Vorlagen, Formulare und Verfahren für Finanzunternehmen zur Meldung schwerwiegender IKT-Vorfälle sowie standardisierte Vorlagen für das Register der Informationen festgelegt werden. Bei der Ausarbeitung dieser Standards

---

40 ABl. L 123 vom 12.5.2016, S. 1.

41 [*Bitte vollständigen Verweis einfügen*]

sollten die ESA die Größe und Komplexität der Finanzunternehmen sowie die Art und das Ausmaß des mit ihren Tätigkeiten verbundenen Risikos 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. Da weitere Anforderungen bereits durch delegierte Rechtsakte und Durchführungsrechtsakte auf der Grundlage technischer Regulierungs- und Durchführungsstandards in den Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 bzw. (EU) Nr. 909/2014 festgelegt wurden, ist es angezeigt, die ESA entweder einzeln oder gemeinsam über den Gemeinsamen Ausschuss zu beauftragen, der Kommission technische Regulierungs- und Durchführungsstandards für den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten zur Übernahme und Aktualisierung bestehender IKT-Risikomanagementvorschriften vorzulegen.

(72) In diesem Rahmen werden bestehende delegierte Rechtsakte und Durchführungsrechtsakte, die in verschiedenen Bereichen der Rechtsvorschriften über Finanzdienstleistungen erlassen wurden, später geändert. Der Geltungsbereich der Artikel über operationelle Risiken, auf deren Basis durch Befugnisübertragungen in diesen Rechtsakten der Erlass von delegierten Rechtsakten und Durchführungsrechtsakten ermöglicht wurde, sollte geändert werden, damit alle Bestimmungen über die digitale Betriebsstabilität, die heute Teil dieser Verordnungen sind, in diese Verordnung übernommen werden können.

(73) Da die Ziele dieser Verordnung, namentlich die Erreichung eines hohen Niveaus digitaler Betriebsstabilität in allen Finanzunternehmen, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden können, weil sie die Harmonisierung einer Vielzahl unterschiedlicher Vorschriften erfordern, die derzeit entweder in bestimmten Rechtsakten der Union oder in den Rechtssystemen der einzelnen Mitgliedstaaten bestehen, sondern sich wegen ihres Umfangs und ihrer Wirkungen besser auf Unionsebene verwirklichen lassen, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten 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 —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

(1) In dieser Verordnung werden wie folgt die folgenden einheitlichen Anforderungen für die Sicherheit von Netz- und Informationssystemen festgelegt, die die Geschäftsprozesse von Finanzunternehmen unterstützen, die zur Erreichung eines hohen gemeinsamen Niveaus digitaler Betriebsstabilität erforderlich sind:

a) auf Finanzunternehmen anwendbare Anforderungen in Bezug auf:

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

– Meldung schwerwiegender IKT-bezogener Vorfälle an die zuständigen Behörden;

– Prüfung der digitalen Betriebsstabilität;

– Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen;

– Maßnahmen für die wirtschaftliche Steuerung des Risikos durch IKT-Drittanbieter;

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

c) den Aufsichtsrahmen für kritische IKT-Drittanbieter 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 5 der Richtlinie (EU) 2016/1148 als Betreiber wesentlicher Dienste ermittelt wurden, gilt diese Verordnung für die Zwecke von Artikel 1 Absatz 7 der genannten Richtlinie als sektorspezifischer Rechtsakt der Union.

Artikel 2

Persönlicher Geltungsbereich

(1) Diese Verordnung gilt für folgende Unternehmen:

a) Kreditinstitute,

b) Zahlungsinstitute,

c) E-Geld-Institute,

d) Wertpapierfirmen,

e) Anbieter von Krypto-Dienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Token und Emittenten signifikanter an Vermögenswerten geknüpfter Token,

f) Zentralverwahrer,

g) zentrale Gegenparteien,

h) Handelsplätze,

i) Transaktionsregister,

j) Verwalter alternativer Investmentfonds,

k) Verwaltungsgesellschaften,

l) Datenbereitstellungsdienste,

m) Versicherungs- und Rückversicherungsunternehmen,

n) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

o) Einrichtungen der betrieblichen Altersversorgung,

p) Ratingagenturen,

q) Abschlussprüfer und Prüfungsgesellschaften,

r) Administratoren kritischer Benchmarks,

s) Crowdfunding-Dienstleister,

t) Verbriefungsregister,

u) IKT-Drittanbieter.

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

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „digitale Betriebsstabilität“ die Fähigkeit eines Finanzunternehmens, seine operative Integrität aus technologischer Sicht aufzubauen, zu gewährleisten und zu überprüfen, indem es durch Nutzung der Dienste von IKT-Drittanbietern entweder direkt oder indirekt das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netz- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität unterstützen;

2. „Netz- und Informationssystem“ Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. „Sicherheit von Netz- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 2 der Richtlinie (EU) 2016/1148;

4. „IKT-Risiko“ jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netz- und Informationssystemen – einschließlich Störungen, Kapazitätsüberschreitungen, Ausfällen, Unterbrechungen, Beeinträchtigungen, Missbräuchen, Verlusten oder sonstiger böswilliger oder nicht böswilliger Ereignisse, die bei Eintritt die Sicherheit der Netz- und Informationssysteme, jeglicher technologiegestützter Instrumente oder Prozesse, des Betriebs und laufender Prozesse oder der Erbringung von Diensten beeinträchtigen können – und folglich die Integrität oder Verfügbarkeit von Daten, Software-Programmen oder sonstigen Komponenten von IKT-Diensten und -infrastrukturen zunichte macht oder einen Verstoß gegen den Datenschutz, Beschädigungen der physischen IKT-Infrastruktur oder sonstige nachteilige Folgen mit sich bringt;

5. „Informationsbestand“ eine Sammlung materieller oder immaterieller Informationen, die geschützt werden sollten;

6. „IKT-bezogener Vorfall“ ein unvorhergesehenes in den Netz- und Informationssystemen festgestelltes Ereignis, das von böswilligen Handlungen herrühren kann und die Sicherheit von Netz- und Informationssystemen und der von diesen Systemen verarbeiteten, gespeicherten oder übertragenen Informationen beeinträchtigt oder nachteilige Auswirkungen auf die Verfügbarkeit, Vertraulichkeit,

Kontinuität oder Authentizität der vom Finanzunternehmen erbrachten Finanzdienstleistungen hat;

7. „schwerwiegender IKT-bezogener Vorfall“ einen IKT-Vorfall mit potenziell umfassenden nachteiligen Auswirkungen auf die Netz- und Informationssysteme, die kritische Funktionen des Finanzunternehmens unterstützen;

8. „Cyberbedrohung“ eine „Cyberbedrohung“ im Sinne der Definition in Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[42];

9. „Cyberangriff“ einen böswilligen IKT-bezogenen Vorfall, in dessen Rahmen ein Angriffsvektor versucht, 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;

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

11. „gestaffeltes Sicherheitskonzept“ eine IKT-bezogene Strategie, bei der Personen, Prozesse und Technologien einbezogen werden, um eine Vielzahl von Barrieren über mehrere Ebenen und Dimensionen des Unternehmens hinweg zu errichten;

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

13. „bedrohungsorientierte Penetrationstests“ einen Rahmen, der Taktik, Techniken und Verfahren realer Angriffsvektoren, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-)Test der kritischen Live-Produktionssysteme des Unternehmens ermöglicht;

14. „Risiko durch IKT-Drittanbieter“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Diensten entstehen kann, die von IKT-Drittanbietern oder weiteren Unterauftragnehmern erbracht werden;

15. „IKT-Drittanbieter“ ein Unternehmen, das digitale Dienste und Datendienste erbringt, einschließlich Anbietern von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren, jedoch unter Ausschluss von Anbietern von Hardwarekomponenten und nach Unionsrecht zugelassene Unternehmen, die

[42] 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).

elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates[43] erbringen;

16. „IKT-Dienste“ digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern erbracht werden, einschließlich Diensten für die Bereitstellung, Eingabe, Speicherung und Verarbeitung von Daten und Berichterstattungsdiensten, Datenüberwachung sowie datenbasierter Dienste und Diensten für Entscheidungsunterstützung;

17. „kritische oder wichtige Funktion“ eine Funktion, deren unterbrochene, eingeschränkte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach anwendbaren Finanzdienstleistungsvorschriften oder seine finanzielle Leistungsfähigkeit oder die Solidität oder Kontinuität seiner Dienstleistungen und Tätigkeiten erheblich beeinträchtigen würde;

18. „kritischer IKT-Drittanbieter“ einen IKT-Drittanbieter, der gemäß Artikel 29 benannt wurde und dem in den Artikeln 30 bis 37 genannten Aufsichtsrahmen unterliegt;

19. „IKT-Drittanbieter mit Sitz in einem Drittland“ einen IKT-Drittanbieter, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die in der Union weder ein Unternehmen noch eine Niederlassung besitzt und mit einem Finanzunternehmen eine vertragliche Vereinbarung über die Erbringung von IKT-Diensten geschlossen hat;

20. „IKT-Unterauftragnehmer mit Sitz in einem Drittland“ einen IKT-Unterauftragnehmer, der eine juristische Person mit Sitz in einem Drittland ist, in der Union weder ein Unternehmen noch eine Niederlassung besitzt und mit einem IKT-Drittanbieter oder einem IKT-Drittanbieter mit Sitz in einem Drittland eine vertragliche Vereinbarung geschlossen hat;

21. „IKT-Konzentrationsrisiko“ die Exposition gegenüber einzelnen oder mehreren verbundenen kritischen IKT-Drittanbietern, die zu einer gewissen Abhängigkeit von solchen Anbietern führt, sodass die Nichtverfügbarkeit, der Ausfall oder sonstige Defizite Letzterer die Fähigkeit eines Finanzunternehmens und letztlich des Finanzsystems der Union insgesamt gefährden könnte, kritische Funktionen zu erfüllen, oder andere Formen nachteiliger Auswirkungen, einschließlich großer Verluste, herbeiführen;

22. „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, 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 des Europäischen Parlaments und des Rates[44] sowie von Artikel 3 Absatz 1 Buchstabe u der Verordnung (EU) 20xx/xx des Europäischen Parlaments und des

---

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

[44] 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).

Rates[45] [MiCA] oder die entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit einschlägigen Unions- oder nationalen Rechtsvorschriften Schlüsselfunktionen wahrnehmen;

23. „Kreditinstitut“ ein Kreditinstitut oder im Sinne des Artikels 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates[46];

24. „Wertpapierfirma“ eine Wertpapierfirma im Sinne des Artikels 4 Absatz 1 Nummer 1 der Richtlinie 2014/65/EU;

25. „Zahlungsinstitut“ ein Zahlungsinstitut im Sinne des Artikels 1 Absatz 1 Buchstabe d der Richtlinie (EU) 2015/2366;

26. „E-Geld-Institut“ ein E-Geld-Institut im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates[47];

27. „zentrale Gegenpartei“ eine zentrale Gegenpartei im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012;

28. „Transaktionsregister“ ein Transaktionsregister im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) Nr. 648/2012;

29. „Zentralverwahrer“ ein Zentralverwahrer im Sinne des Artikels 2 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 909/2014;

30. „Handelsplatz“ einen Handelsplatz im Sinne des Artikels 4 Absatz 1 Nummer 24 der Richtlinie 2014/65/EU;

31. „Verwalter alternativer Investmentfonds“ einen Verwalter alternativer Investmentfonds im Sinne des Artikels 4 Absatz 1 Buchstabe b der Richtlinie 2011/61/EU;

32. „Verwaltungsgesellschaft“ eine Verwaltungsgesellschaft im Sinne des Artikels 2 Absatz 1 Buchstabe b der Richtlinie 2009/65/EG;

33. „Datenbereitstellungsdienst“ einen Datenbereitstellungsdienst im Sinne des Artikels 4 Absatz 1 Nummer 63 der Richtlinie 2014/65/EU;

34. „Versicherungsunternehmen“ ein Versicherungsunternehmen im Sinne des Artikels 13 Nummer 1 der Richtlinie 2009/138/EG;

35. „Rückversicherungsunternehmen“ ein Rückversicherungsunternehmen im Sinne des Artikels 13 Nummer 4 der Richtlinie 2009/138/EG;

36. „Versicherungsvermittler“ einen Versicherungsvermittler im Sinne des Artikels 2 Nummer 3 der Richtlinie (EU) 2016/97;

37. „Versicherungsvermittler in Nebentätigkeit“ einen Versicherungsvermittler in Nebentätigkeit im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2016/97;

---

45 [*bitte vollständigen Titel und Amtsblattangaben eingeben*]

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

47 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).

38. „Rückversicherungsvermittler“ einen Rückversicherungsvermittler im Sinne des Artikels 2 Nummer 5 der Richtlinie (EU) 2016/97;

39. „Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung im Sinne des Artikels 1 Nummer 6 der Richtlinie (EU) 2016/2341;

40. „Ratingagentur“ eine Ratingagentur im Sinne des Artikels 3 Absatz 1 Buchstabe a der Verordnung (EG) Nr. 1060/2009;

41. „Abschlussprüfer“ einen Abschlussprüfer im Sinne des Artikels 2 Nummer 2 der Richtlinie 2006/43/EG;

42. „Prüfungsgesellschaft“ eine Prüfungsgesellschaft im Sinne des Artikels 2 Nummer 3 der Richtlinie 2006/43/EG;

43. „Anbieter von Krypto-Dienstleistungen“ einen Anbieter von Krypto-Dienstleistungen im Sinne des Artikels 3 Absatz 1 Buchstabe n der Verordnung (EU) 202x/ xx [*Amt für Veröffentlichungen: Verweis auf die MiCA-Verordnung einfügen*];

44. „Emittent von Kryptowerten“ einen Emittenten von Kryptowerten im Sinne des Artikels 3 Absatz 1 Buchstabe h der [*ABl.: Verweis auf die MiCA-Verordnung einfügen*];

45. „Emittent von an Vermögenswerte geknüpften Tokens“ einen Emittenten von an Vermögenswerte geknüpften Tokens im Sinne des Artikels 3 Absatz 1 Buchstabe i der [*ABl.: Verweis auf die MiCA-Verordnung einfügen*];

46. „Emittent signifikanter an Vermögenswerte geknüpfter Tokens“ einen Emittenten signifikanter an Vermögenswerte geknüpfter Tokens im Sinne des Artikels 3 Absatz 1 Buchstabe j der [*ABl.*: *Verweis auf die MiCA-Verordnung einfügen*];

47. „Administrator kritischer Referenzwerte“ einen Administrator kritischer Referenzwerte im Sinne des Artikels x Buchstabe x der Verordnung Nr. xx/202x [*ABl.: Verweis auf die Referenzwerte-Verordnung einfügen*];

48. „Crowdfunding-Dienstleister“ einen Crowdfunding-Dienstleister im Sinne des Artikels x Buchstabe x der Verordnung (EU) 202x/xx [*Amt für Veröffentlichungen: Verweis auf die Crowdfunding-Verordnung einfügen*];

49. „Verbriefungsregister“ ein Verbriefungsregister im Sinne des Artikels 2 Nummer 23 der Verordnung (EU) 2017/2402;

50. „Kleinstunternehmen“ ein Finanzunternehmen im Sinne des Artikels 2 Absatz 3 des Anhangs der Empfehlung 2003/361/EG.

KAPITEL II

IKT-RISIKOMANAGEMENT

ABSCHNITT I

Artikel 4

Steuerung und Organisation

(1) Finanzunternehmen verfügen über interne Governance- und Kontrollrahmen, die eine wirksame und umsichtige Steuerung aller IKT-Risiken gewährleisten.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt und überwacht alle Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 5 Absatz 1 und ist für die Umsetzung rechenschaftspflichtig:

Für die Zwecke von Unterabsatz 1 gilt Folgendes:

a) das Leitungsorgan trägt die Endverantwortung für die Steuerung der IKT-Risiken des Finanzunternehmens;

b) das Leitungsorgan legt klare Aufgaben und Zuständigkeiten für alle IKT-bezogenen Funktionen fest;

c) das Leitungsorgan ermittelt die angemessene Toleranzschwelle für das IKT-Risiko des Finanzunternehmens gemäß Artikel 5 Absatz 9 Buchstabe b;

d) das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der in Artikel 10 in den Absätzen 1 und 3 genannten IKT-Strategie für die Fortführung des Geschäftsbetriebs sowie des IKT-Plans für die Wiederherstellung im Notfall;

e) das Leitungsorgan genehmigt und überprüft regelmäßig die IKT-Prüfpläne, IKT-Prüfungen und daran vorgenommene wesentliche Änderungen;

f) das Leitungsorgan weist angemessene Haushaltsmittel zu und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale Betriebsstabilität in Bezug auf die verschiedensten Ressourcen gerecht zu werden, einschließlich Schulungen zu IKT-Risiken und -Kompetenzen für alle einschlägigen Mitarbeiter;

g) das Leitungsorgan genehmigt und überprüft regelmäßig die Richtlinien des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Diensten, die von IKT-Drittanbietern erbracht werden;

h) das Leitungsorgan ist ordnungsgemäß über die mit IKT-Drittanbietern zur Nutzung von IKT-Diensten getroffenen Vereinbarungen, über relevante geplante wesentliche Änderungen in Bezug auf IKT-Drittanbieter sowie über die potenziellen Auswirkungen solcher Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, unterrichtet und erhält eine Übersicht über die Risikoanalyse zur Bewertung der Auswirkungen dieser Änderungen;

i) das Leitungsorgan ist ordnungsgemäß über IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen informiert.

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

(4) Die Mitglieder des Leitungsorgans absolvieren regelmäßig Fachschulungen, um ausreichende Kenntnisse und Fähigkeiten zu erwerben und auf dem neuesten Stand zu halten, damit sie IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.

ABSCHNITT II

Artikel 5

IKT-Risikomanagementrahmen

(1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der es ihnen ermöglicht, IKT-Risiken rasch, effizient und umfassend anzugehen und ein hohes Maß an digitaler Betriebsstabilität zu gewährleisten, das ihren geschäftlichen Bedürfnissen, ihrer Größe und ihrer Komplexität entspricht.

(2) Der in Absatz 1 genannte IKT-Risikomanagementrahmen umfasst Strategien, Strategien, Verfahren, IKT-Protokolle und -Instrumente, die erforderlich sind, um alle relevanten physischen Komponenten und Infrastrukturen, einschließlich Computer-Hardware und Server, sowie alle relevanten Räumlichkeiten, Rechenzentren und ausgewiesenen sensiblen Bereiche ordnungsgemäß und wirksam zu schützen, damit sichergestellt ist, dass alle diese physischen Elemente angemessen vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder unbefugter Nutzung, geschützt sind.

(3) Finanzunternehmen minimieren die Auswirkungen von IKT-Risiken, indem sie auf geeignete Strategien, Richtlinien, Verfahren, Protokolle und Instrumente zurückgreifen, die im IKT-Risikomanagementrahmen festgelegt sind. Ebenso stellen sie vollständige und aktuelle Informationen über IKT-Risiken bereit, die von den zuständigen Behörden verlangt werden.

(4) Als Teil des IKT-Risikomanagementrahmens gemäß Absatz 1 wenden Finanzunternehmen, die keine Kleinstunternehmen sind, ein System für die Steuerung der Informationssicherheit an, das auf anerkannten internationalen Standards beruht und im Einklang mit aufsichtsrechtlichen Leitlinien steht, und überprüfen dieses regelmäßig.

(5) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, sorgen für eine angemessene Trennung von IKT-Verwaltungsfunktionen, -Kontrollfunktionen und internen Prüffunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.

(6) Der in Absatz 1 genannte IKT-Risikomanagementrahmen wird mindestens einmal jährlich sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach

aufsichtsrechtlichen Anweisungen oder Schlussfolgerungen, die sich aus einschlägigen Prüfungen oder Auditverfahren für die digitale Betriebsstabilität ergeben, dokumentiert und überprüft. Der Rahmen wird auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert.

(7) Der in Absatz 1 genannte IKT-Risikomanagementrahmen wird regelmäßig von IKT-Prüfern geprüft, die über ausreichende Kenntnisse, Fähigkeiten und Fachkenntnisse im Bereich der IKT-Risiken verfügen. Häufigkeit und Schwerpunkt von IKT-Prüfungen sind den IKT-Risiken des Finanzunternehmens angemessen.

(8) Überdies wird ein förmliches Follow-up-Verfahren mit Regeln für die zeitnahe Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Prüfung festgelegt, bei dem die Schlussfolgerungen aus der Überprüfung berücksichtigt werden, wobei Art, Umfang und Komplexität von Dienstleistungen und Tätigkeiten der Finanzunternehmen gebührend berücksichtigt werden.

(9) Der in Absatz 1 genannte IKT-Risikomanagementrahmen umfasst eine Strategie für digitale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt er die Methoden für die Kontrolle von IKT-Risiken und die Erreichung spezifischer IKT-Ziele 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 Belastungstoleranz mit Blick auf IKT-Störungen untersucht wird;

c) klare Ziele für die Informationssicherheit festgelegt werden;

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

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

f) die Zahl gemeldeter schwerwiegender IKT-Vorfälle und die Wirksamkeit von Präventivmaßnahmen dargelegt wird;

g) auf Unternehmensebene eine ganzheitliche Strategie bei Nutzung mehrerer IKT-Anbieter festgelegt wird, mit der wesentliche Abhängigkeiten von IKT-Drittanbietern aufgezeigt und die Gründe für die Nutzung verschiedener Drittanbieter erläutert werden;

h) Tests zur Prüfung der digitalen Betriebsstabilität durchgeführt werden;

i) bei IKT-bezogenen Vorfällen eine Kommunikationsstrategie umrissen wird.

(10) Finanzunternehmen können die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement nach Genehmigung durch die zuständigen Behörden an gruppeninterne oder externe Unternehmen delegieren.

Artikel 6

IKT-Systeme, -Protokolle und -Instrumente

(1) Finanzunternehmen verwenden und pflegen auf dem neuesten Stand befindliche IKT-Systeme, -Protokolle und -Instrumente, die die folgenden Bedingungen erfüllen:

a) die Systeme und Instrumente sind der Art, der Vielfalt, der Komplexität und dem Umfang von Vorgängen, die die Ausübung ihrer Tätigkeiten unterstützen, angemessen;

b) sie sind zuverlässig;

c) sie verfügen über ausreichende Kapazitäten, um die Daten, die für die fristgerechte Ausführung von Tätigkeiten und die fristgerechte Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Spitzen bei Aufträgen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können;

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

(2) Wenn Finanzunternehmen international anerkannte technische Standards und branchenführende Praktiken in den Bereichen Informationssicherheit und interne IKT-Kontrollen anwenden, greifen sie auf diese Standards und Praktiken im Einklang mit einschlägigen aufsichtsrechtlichen Empfehlungen zu ihrem Status zurück.

Artikel 7

Identifizierung

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 5 Absatz 1 identifizieren, klassifizieren und dokumentieren Finanzunternehmen angemessen alle IKT-bezogenen Unternehmensfunktionen, die Informationsressourcen, die diese Funktionen unterstützen, sowie die Konfigurationen und Vernetzungen des IKT-Systems mit internen und externen IKT-Systemen. Ebenso überprüfen Finanzunternehmen erforderlichenfalls, mindestens jedoch einmal jährlich, ob die Klassifizierung der Informationsressourcen und jeglicher einschlägigen Unterlagen angemessen ist.

(2) Finanzunternehmen ermitteln kontinuierlich alle Quellen für IKT-Risiken, insbesondere das Risiko gegenüber und von anderen Finanzunternehmen, und bewerten Cyberbedrohungen und IKT-Anfälligkeiten, die für ihre IKT-bezogenen Geschäftsfunktionen und Informationsressourcen 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 Netz- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, die sich auf ihre Funktionen, unterstützende Prozesse oder Informationsressourcen auswirken, eine Risikobewertung durch.

(4) Darüber hinaus identifizieren Finanzunternehmen alle Konten von IKT-Systemen, einschließlich der Konten an externen Standorten, der Netzressourcen und der Hardware, und erfassen als kritisch betrachtete physische Ausrüstungen. Ebenso

erfassen sie die Konfiguration von IKT-Ressourcen sowie die Verbindungen und Interdependenzen zwischen den verschiedenen IKT-Ressourcen.

(5) Finanzunternehmen identifizieren und dokumentieren alle Prozesse, die sich auf IKT-Drittanbieter stützen, und ermitteln Vernetzungen mit IKT-Drittanbietern.

(6) Für die Zwecke der Absätze 1, 4 und 5 führen Finanzunternehmen einschlägige Verzeichnisse und aktualisieren diese regelmäßig.

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

Artikel 8

Schutz und Prävention

(1) Um einen angemessenen Schutz der IKT-Systeme zu gewährleisten und Gegenmaßnahmen zu planen, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Funktionsweise der IKT-Systeme und -Instrumente und minimieren die Auswirkungen einschlägiger Risiken durch den Einsatz geeigneter IKT-Sicherheitsinstrumente, -Strategien und -Verfahren.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsstrategien, -Richtlinien, -Verfahren, -Protokolle und -Instrumente, die insbesondere darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen zu gewährleisten und hohe Standards in Bezug auf Sicherheit, Vertraulichkeit und Integrität 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 moderne IKT-Technologien und -Prozesse zurück, die

a) die Sicherheit der Mittel zur Informationsübermittlung gewährleisten;

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

c) das Durchsickern von Informationen verhindern;

d) sicherstellen, dass Daten vor schlechter Verwaltung oder verarbeitungsbezogenen Risiken, einschließlich der unangemessenen Aufbewahrung von Aufzeichnungen, geschützt werden.

(4) Als Teil des IKT-Risikomanagementrahmens nach Artikel 5 Absatz 1 gilt für Finanzunternehmen Folgendes:

a) sie erarbeiten und dokumentieren eine Strategie für Informationssicherheit, in der Regeln zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer IKT-Ressourcen, Daten und Informationsressourcen sowie derjenigen ihrer Kunden festgeschrieben sind;

b) sie richten gemäß einem risikobasierten Ansatz ein robustes Netz- und Infrastrukturmanagement unter Verwendung geeigneter Techniken, Methoden und Protokolle ein, darunter auch die Umsetzung automatisierter Mechanismen

zur Isolierung betroffener Informationsressourcen im Falle von Cyberangriffen;

c) sie implementieren Strategien, die den physischen und virtuellen Zugang zu Ressourcen und Daten des IKT-Systems auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist, und legen zu diesem Zweck eine Reihe von Strategien, Verfahren und Kontrollen fest, die auf Zugriffsrechte und deren ordnungsgemäße Verwaltung abzielen;

d) sie implementieren Strategien und Protokolle für leistungsfähige Authentifizierungsmechanismen, die auf einschlägigen Normen und speziellen Kontrollsystemen basieren, um den Zugang zu kryptografischen Schlüsseln zu verhindern, wobei Daten auf Basis von Ergebnissen zulässiger Prozesse für Datenklassifizierung und Risikobewertung verschlüsselt werden;

e) sie implementieren Strategien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, einschließlich Änderungen an Software, Hardware, Firmware-Komponenten sowie System- oder Sicherheitsänderungen, die auf einem Konzept für die Risikobewertung beruhen und integraler Bestandteil des gesamten Änderungsmanagementprozesses des Finanzunternehmens sind, damit alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden;

f) sie besitzen angemessene und umfassende Strategien für Patches und Aktualisierungen.

Finanzunternehmen konzipieren die Infrastruktur für die Netzwerkanbindung mit Blick auf die Zwecke unter Buchstabe b so, dass sie sofort getrennt werden kann, und sorgen für ihre Abschottung und Segmentierung, damit eine Ansteckung, insbesondere bei miteinander verbundenen Finanzprozessen, minimiert und verhindert wird.

Für die Zwecke von Buchstabe e wird das Verfahren für das IKT-Änderungsmanagement von entsprechenden Berichtslinien genehmigt und geht mit spezifischen Protokollen für Änderungen im Notfall einher.

Artikel 9

Erkennung

(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 15, darunter auch Probleme bei der Leistung von IKT-Netzen und IKT-bezogene Vorfälle, umgehend zu erkennen und alle potenziellen einzelnen Schwachstellen zu ermitteln.

Alle in Unterabsatz 1 aufgeführten Erkennungsmechanismen werden gemäß Artikel 22 regelmäßig getestet.

(2) Die in Absatz 1 genannten Erkennungsmechanismen ermöglichen mehrere Kontrollebenen und die Festlegung von Alarmschwellen und -kriterien, um die Erkennung IKT-bezogener Vorfälle und Abläufe für Gegenmaßnahmen bei IKT-bezogenen Vorfällen einzuleiten, und richten automatische Warnmechanismen für Mitarbeiter ein, die für Gegenmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind.

(3) Finanzunternehmen stellen unter gebührender Berücksichtigung ihrer Größe, ihres Geschäftsfelds und ihrer Risikoprofile ausreichende Ressourcen und Kapazitäten

bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

(4) Die in Artikel 2 Absatz 1 Buchstabe l genannten Finanzunternehmen verfügen darüber hinaus über Systeme, mit denen wirksam Handelsauskünfte auf Vollständigkeit geprüft, Lücken und offensichtliche Fehler erkannt und bei derlei fehlerhaften Auskünften eine Neuübermittlung angefordert werden können.

Artikel 10

Gegenmaßnahmen und Wiederherstellung

(1) Als Teil des in Artikel 5 Absatz 1 genannten IKT-Risikomanagementrahmens und auf Grundlage der Identifizierungsanforderungen nach Artikel 7 legen Finanzunternehmen eine spezielle und umfassende IKT-Strategie zur Fortführung des Geschäftsbetriebs als integralen Bestandteil der operativen Strategie zur Fortführung des Geschäftsbetriebs des Finanzunternehmens fest.

(2) Finanzunternehmen implementieren die in Absatz 1 genannte IKT-Strategie für die Fortführung des Geschäftsbetriebs mittels spezieller, geeigneter und dokumentierter Regelungen, Pläne, Verfahren und Mechanismen, die darauf abzielen

a) alle IKT-bezogenen Vorfälle aufzuzeichnen;

b) die Kontinuität der kritischen Funktionen des Finanzunternehmens sicherzustellen;

c) auf alle IKT-bezogenen Vorfälle, darunter insbesondere – jedoch nicht ausschließlich – Cyberangriffe, rasch, angemessen und wirksam zu reagieren und diesen so entgegenzuwirken, dass Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Wiederherstellungsmaßnahmen Vorrang erhalten;

d) unverzüglich spezielle Pläne zu aktivieren, die Eindämmungsmaßnahmen, -prozesse und -technologien für alle Arten IKT-bezogener Vorfälle ermöglichen, und weitere Schäden zu vermeiden sowie maßgeschneiderte Verfahren für Gegenmaßnahmen und Wiederherstellung gemäß Artikel 11 zu aktivieren;

e) vorläufige Auswirkungen, Schäden und Verluste einzuschätzen;

f) Kommunikations- und Krisenmanagementmaßnahmen festzulegen, damit allen einschlägigen internen Mitarbeitern und externen Interessenträgern gemäß Artikel 13 aktualisierte Informationen übermittelt und gemäß Artikel 17 den zuständigen Behörden gemeldet werden.

(3) Finanzunternehmen implementieren als Teil des in Artikel 5 Absatz 1 genannten IKT-Risikomanagementrahmens einen damit verbundenen IKT-Plan für die Wiederherstellung im Notfall, der einer unabhängigen Prüfung zu unterziehen ist, sofern es sich bei dem Finanzunternehmen nicht um ein Kleinstunternehmen handelt.

(4) Finanzunternehmen erstellen, pflegen und überprüfen regelmäßig angemessene IKT-Pläne zur Fortführung des Geschäftsbetriebs, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittanbieter vergeben werden.

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

a) sie überprüfen mindestens einmal jährlich und nach wesentlichen Änderungen an den IKT-Systemen die IKT-Strategie für die Fortführung des Geschäftsbetriebs sowie den IKT-Plan für die Wiederherstellung im Notfall;

b) sie überprüfen die gemäß Artikel 13 erstellten Krisenkommunikationspläne.

Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, nehmen für die Zwecke unter Buchstabe a Szenarien für Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme auf, die für die Erfüllung der Verpflichtungen nach Artikel 11 erforderlich sind.

Finanzunternehmen überprüfen ihre IKT-Strategie zur Fortführung des Geschäftsbetriebs und ihren IKT-Plan für die Wiederherstellung im Notfall regelmäßig und berücksichtigen dabei die Ergebnisse von Prüfungen, die gemäß Unterabsatz 1 durchgeführt wurden, sowie die Empfehlungen, die sich aus Prüfungen oder aufsichtlichen Überprüfungen ergeben.

(6) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, legen eine Krisenmanagementfunktion fest, die bei Aktivierung ihrer IKT-Strategie zur Fortführung des Geschäftsbetriebs oder ihres IKT-Plans für die Wiederherstellung im Notfall klare Verfahren für die Abwicklung interner und externer Krisenkommunikation gemäß Artikel 13 festschreibt.

(7) Finanzunternehmen legen Aufzeichnungen über Tätigkeiten vor und während Störungen vor, wenn ihre IKT-Strategie zur Fortführung des Geschäftsbetriebs oder ihr IKT-Plan für die Wiederherstellung im Notfall aktiviert sind. Diese Aufzeichnungen müssen ohne Weiteres verfügbar sein.

(8) Die in Artikel 2 Absatz 1 Buchstabe f genannten Finanzunternehmen übermitteln den zuständigen Behörden Kopien der Ergebnisse der IKT-Tests zur Fortführung des Geschäftsbetriebs oder ähnlicher Vorgänge, die während des Überprüfungszeitraums durchgeführt wurden.

(9) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, melden den zuständigen Behörden alle Kosten und Verluste, die durch IKT-Störungen und IKT-bezogene Vorfälle verursacht werden.

Artikel 11

Strategien für Datensicherung und Wiederherstellungsverfahren

(1) Um die Wiederherstellung von IKT-Systemen mit minimaler Ausfallzeit und begrenzter Störung als Teil ihres IKT-Risikomanagementrahmens sicherzustellen, entwickeln Finanzunternehmen:

a) eine Strategie für die Datensicherung, in der der Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf Basis der Kritikalität der Informationen oder der Sensibilität der Daten festgelegt werden;

b) Wiederherstellungsverfahren.

(2) Datensicherungssysteme beginnen ohne ungebührliche Verzögerung mit der Verarbeitung, sofern hierdurch nicht die Sicherheit der Netz- und Informationssysteme oder die Integrität oder Vertraulichkeit von Daten gefährdet wird.

(3) Bei der Wiederherstellung gesicherter Daten mithilfe eigener Systeme verwenden Finanzunternehmen IKT-Systeme mit einer nicht mit der Hauptumgebung zusammenhängenden Betriebsumgebung, die nicht unmittelbar mit der Hauptumgebung vernetzt und sicher vor unbefugtem Zugriff oder Manipulationen im IKT-Bereich geschützt ist.

Bei Finanzunternehmen im Sinne von Artikel 2 Absatz 1 Buchstabe g ermöglichen die Wiederherstellungspläne, alle zum Zeitpunkt der Unterbrechung laufenden Transaktionen wiederherzustellen, damit die zentrale Gegenpartei weiterhin sicher arbeiten und die Abwicklung zum vorgesehenen Zeitpunkt abschließen kann.

(4) Finanzunternehmen unterhalten redundante IKT-Kapazitäten mit Ressourcen und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind.

(5) Die in Artikel 2 Absatz 1 Buchstabe f genannten Finanzunternehmen sorgen dafür oder gewährleisten, dass ihre IKT-Drittanbieter mindestens einen sekundären Bearbeitungsstandort unterhalten, dessen Ressourcen, Kapazitäten, Funktionen und Personalressourcen ausreichend und angemessen sind, um den Geschäftsbedarf zu decken.

Der sekundäre Bearbeitungsstandort:

a) befindet sich in geografischer Entfernung vom primären Bearbeitungsstandort, 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, mit dem primären Standort identischer Dienstleistungen gewährleisten oder ein Leistungsniveau bereitstellen, das sicherstellt, dass das Finanzunternehmen seine kritischen Vorgänge im Rahmen der Wiederherstellungsziele durchführt;

c) ist für das Personal des Finanzunternehmens unmittelbar zugänglich, damit die Kontinuität kritischer Dienstleistungen gewährleistet werden kann, wenn der primäre Bearbeitungsstandort nicht mehr zur Verfügung steht.

(6) Bei der Festlegung der Zeitvorgaben für die Wiederherstellung und die Wiederherstellungspunkte jeder Funktion berücksichtigen Finanzunternehmen die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarten Leistungsniveaus in Extremszenarien erreicht werden.

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

Artikel 12

Lernprozesse und Weiterentwicklung

(1) Finanzunternehmen verfügen über Kapazitäten und Personal, die auf ihre Größe sowie ihre Geschäfts- und Risikoprofile zugeschnitten sind, um Informationen über Anfälligkeiten und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere

Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf ihre digitale Betriebsstabilität zu untersuchen.

(2) Finanzunternehmen richten nachträgliche Prüfungen IKT-bezogener Vorfälle ein, die nach erheblichen Störungen der IKT ihrer Haupttätigkeiten durchgeführt werden, untersuchen die Ursachen für Störungen und ermitteln erforderliche Verbesserungen an IKT-Vorgängen oder im Rahmen der in Artikel 10 genannten IKT-Strategie zur Fortführung des Geschäftsbetriebs.

Bei der Umsetzung von Änderungen teilen Finanzunternehmen, die keine Kleinstunternehmen sind, diese Änderungen den zuständigen Behörden mit.

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 kriminaltechnischer Analysen;

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

d) die Wirksamkeit interner und externer Kommunikation.

(3) Erkenntnisse aus der gemäß den Artikeln 23 und 24 durchgeführten Prüfung der digitalen Betriebsstabilität und aus realen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, werden neben Herausforderungen, die sich bei der Aktivierung von Plänen für die Fortführung des Geschäftsbetriebs oder die Wiederherstellung 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 fließen in angemessene Überprüfungen relevanter Komponenten des IKT-Risikomanagementrahmens gemäß Artikel 5 Absatz 1 ein.

(4) Finanzunternehmen überwachen die Wirksamkeit der Umsetzung ihrer Strategie für die digitale Resilienz gemäß Artikel 5 Absatz 9. 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 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 für digitale Betriebsstabilität, die im Rahmen ihrer Programme für die Mitarbeiterschulung obligatorisch sind. Diese gelten für alle Beschäftigten und die Geschäftsleitung.

Finanzunternehmen 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 Betriebsstabilität zu verstehen. Überdies halten sie sich über die neuesten Prozesse

für das IKT-Risikomanagement auf dem Laufenden, um gegenwärtige oder neue Formen von Cyberangriffen wirksam abzuwehren.

Artikel 13
Kommunikation

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 5 Absatz 1 verfügen Finanzunternehmen über Kommunikationspläne, die je nach Sachlage eine verantwortungsbewusste Offenlegung IKT-bezogener Vorfälle oder erheblicher Anfälligkeiten gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit ermöglichen.

(2) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 5 Absatz 1 setzen Finanzunternehmen Kommunikationsstrategien für Mitarbeiter und externe Interessenträger um. Bei Kommunikationsstrategien für Mitarbeiter wird berücksichtigt, dass zwischen Personal, das am IKT-Risikomanagement, insbesondere im Bereich der Gegenmaßnahmen und der Wiederherstellung, beteiligt ist, und zu informierendem Personal unterschieden werden muss.

(3) Mindestens eine Person im Unternehmen ist mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt und nimmt zu diesem Zweck die Rolle des öffentlichen Sprechers und Mediensprechers wahr.

Artikel 14
Weitere Harmonisierung von Instrumenten, Methoden, Prozessen und Strategien für IKT-Risikomanagement

Die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) arbeiten in Absprache mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) Entwürfe technischer Regulierungsstandards für die folgenden Zwecke aus:

a) Festlegung weiterer Elemente, die in die in Artikel 8 Absatz 2 genannten Strategien, Verfahren, Protokolle und Instrumente für IKT-Sicherheit aufzunehmen sind, um die Sicherheit von Netzen zu gewährleisten, angemessene Schutzvorrichtungen gegen Eindringen und Missbrauch von Daten zu ermöglichen, die Authentizität und Integrität der Daten, einschließlich kryptografischer Techniken, zu wahren und eine präzise und rasche Datenübermittlung ohne wesentliche Störungen zu gewährleisten;

b) Vorgaben dazu, wie die in Artikel 8 Absatz 2 genannten Strategien, Verfahren und Instrumente für IKT-Sicherheit vorweg Sicherheitskontrollen in Systeme integrieren (eingebaute Sicherheit), Anpassungen an die sich wandelnde Bedrohungslage ermöglichen und den Einsatz gestaffelter Sicherheitskonzepte vorsehen;

c) nähere Spezifizierung geeigneter Techniken, Methoden und Protokolle gemäß Artikel 8 Absatz 4 Buchstabe b;

d) Entwicklung weiterer Komponenten der Kontrollen von Zugangsverwaltungsrechten gemäß Artikel 8 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 geeignete Indikatoren – auch für Netznutzungsmuster, Zeiten, IT-Aktivität und unbekannte Geräte – spezifiziert werden;

e) Weiterentwicklung der in Artikel 9 Absatz 1 genannten Elemente, die eine unverzügliche Erkennung anomaler Tätigkeiten ermöglichen, und der in Artikel 9 Absatz 2 genannten Kriterien, die Verfahren für die Erkennung IKT-bezogener Vorfälle und die damit verbundenen Gegenmaßnahmen auslösen;

f) nähere Spezifizierung der in Artikel 10 Absatz 1 genannten Komponenten des IKT-Plans für die Fortführung des Geschäftsbetriebs;

g) nähere Präzisierung der Prüfung von IKT-Plänen für die Fortführung des Geschäftsbetriebs gemäß Artikel 10 Absatz 5, damit Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese ganz fehlt, und die potenziellen Auswirkungen der Insolvenz oder sonstiger Unzulänglichkeiten einschlägiger IKT-Drittanbieter sowie gegebenenfalls die politischen Risiken in den Rechtsordnungen der jeweiligen Anbieter gebührend berücksichtigt werden;

h) nähere Präzisierung der Komponenten des in Artikel 10 Absatz 3 genannten IKT-Plans für die Wiederherstellung im Notfall.

Die EBA, die ESMA und die EIOPA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum [ABl.: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*].

Der Kommission wird die Befugnis übertragen, die technischen Regulierungsstandards nach Unterabsatz 1 gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 zu erlassen.

KAPITEL III

IKT-BEZOGENE VORFÄLLE

BEWÄLTIGUNG, KLASSIFIZIERUNG UND BERICHTERSTATTUNG

Artikel 15

Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle

(1) Finanzunternehmen legen eine Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle fest und wenden diese an, um IKT-bezogene Vorfälle zu erkennen, zu bewältigen und zu melden, und richten Frühwarnindikatoren als Warnmeldungen ein.

(2) Zudem legen Finanzunternehmen angemessene Vorgehensweisen fest, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten, damit Ursachen ermittelt und beseitigt werden, um das Auftreten solcher Vorfälle zu verhindern.

(3) Über die in Absatz 1 genannte Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle:

a) werden Verfahren zur Ermittlung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend

ihrer Priorität und der Schwere und Kritikalität der betroffenen Dienste gemäß den in Artikel 16 Absatz 1 genannten Kriterien eingerichtet;

b) werden Funktionen und Zuständigkeiten zugewiesen, die für verschiedene Arten von IKT-bezogenen Vorfällen und -Szenarien aktiviert werden müssen;

c) werden gemäß Artikel 13 Pläne für die Kommunikation mit Personal, externen Interessenträgern und Medien sowie für die Benachrichtigung von Kunden, interne Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzunternehmen ausgearbeitet, je nach Sachlage;

d) wird sichergestellt, dass schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene und dem Leitungsorgan gemeldet werden, wobei die Folgen und Gegenmaßnahmen und zusätzliche Kontrollen erläutert werden, die infolge IKT-bezogener Vorfälle einzuführen sind;

e) werden Verfahren für Gegenmaßnahmen bei IKT-bezogenen Vorfällen eingerichtet, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste rechtzeitig verfügbar und sicher sind.

Artikel 16

Klassifizierung IKT-bezogener Vorfälle

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

a) Zahl der Nutzer oder anderer Akteure im Finanzbereich, die von der durch den IKT-bezogenen Vorfall verursachten Störung betroffen sind, und ob der IKT-bezogene Vorfall einen Rufschaden 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 Datenverluste, z. B. Verlust der Datenintegrität, Preisgabe oder Nichtverfügbarkeit von Daten;

e) Schwere der Auswirkungen des IKT-bezogenen Vorfalls auf die IKT-Systeme des Finanzunternehmens;

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

g) wirtschaftliche Auswirkungen des IKT-bezogenen Vorfalls auf absoluter und relativer Basis.

(2) Die ESA erarbeiten über den Gemeinsamen Ausschuss der ESA (im Folgenden „Gemeinsamer Ausschuss“) und nach Abstimmung mit der Europäischen Zentralbank (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, die der Meldepflicht nach Artikel 17 Absatz 1 unterliegen;

b) die Kriterien, die von zuständigen Behörden anzuwenden sind, um die Relevanz schwerwiegender IKT-bezogener Vorfälle für die Hoheitsbereiche anderer Mitgliedstaaten zu bewerten, sowie die Einzelheiten in Berichten über IKT-bezogene Vorfälle, die anderen zuständigen Behörden gemäß Artikel 17 Nummer 5 und 6 übermittelt werden müssen.

(3) Bei der Ausarbeitung der in Absatz 2 genannten gemeinsamen Entwürfe technischer Regulierungsstandards berücksichtigen die ESA internationale Normen sowie von der ENISA entwickelte und veröffentlichte Spezifikationen, gegebenenfalls auch Spezifikationen für andere Wirtschaftszweige.

Die ESA legen der Kommission diese allgemeinen Entwürfe für technische Regulierungsstandards bis zum [*Amt für Veröffentlichungen*: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*] vor.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 2 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 17

Meldung schwerwiegender IKT-bezogener Vorfälle

(1) Finanzunternehmen melden der jeweils zuständigen Behörde gemäß Artikel 41 innerhalb der in Absatz 3 festgelegten Fristen schwerwiegende IKT-bezogene Vorfälle.

Für die Zwecke von Unterabsatz 1 erstellen Finanzunternehmen nach Erfassung und Analyse aller relevanten Informationen unter Verwendung der in Artikel 18 genannten Vorlage einen Bericht über den Vorfall und übermitteln ihn der zuständigen Behörde.

Der Bericht enthält alle Informationen, die die zuständige Behörde benötigt, um die Signifikanz des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten.

(2) Wenn ein schwerwiegender IKT-bezogener Vorfall Auswirkungen auf die finanziellen Interessen von Dienstnutzern und Kunden hat oder haben könnte, unterrichten Finanzunternehmen ihre Dienstnutzer und Kunden unverzüglich über den schwerwiegenden IKT-bezogenen Vorfall und so bald wie möglich über alle Maßnahmen, die ergriffen wurden, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern.

(3) Finanzunternehmen legen der in Artikel 41 genannten zuständigen Behörde Folgendes vor:

a) eine erste Meldung, die unverzüglich, spätestens jedoch am Ende des Geschäftstags oder – bei einem schwerwiegenden IKT-bezogenen Vorfall, der später als 2 Stunden vor dem Ende des Geschäftstages eintrat – spätestens 4 Stunden nach Beginn des folgenden Geschäftstags zu erfolgen hat; bei Nichtverfügbarkeit von Meldekanälen erfolgt die Meldung, sobald diese Kanäle verfügbar sind;

b) spätestens 1 Woche nach der ursprünglichen Meldung gemäß Buchstabe a einen Zwischenbericht, gegebenenfalls gefolgt von aktualisierten Meldungen,

wann immer eine entsprechende Statusaktualisierung vorliegt, sowie auf ausdrücklichen Antrag der zuständigen Behörde;

c) einen Abschlussbericht, wenn die Ursachenanalyse abgeschlossen ist – unabhängig davon, ob bereits Abmilderungsmaßnahmen getroffen wurden oder nicht – und sich die tatsächlichen Auswirkungen beziffern lassen und Schätzungen ersetzen, jedoch nicht später als einen Monat nach Übermittlung des ersten Berichts.

(4) Finanzunternehmen dürfen die Meldepflichten nach diesem Artikel erst dann an einen Drittanbieter delegieren, wenn die in Artikel 41 genannte zuständige Behörde dies genehmigt hat.

(5) Nach Eingang des in Absatz 1 genannten Berichts übermittelt die zuständige Behörde unverzüglich Einzelheiten zu dem Vorfall an:

a) die EBA, die ESMA oder die EIOPA, je nach Sachlage;

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

c) die in Artikel 8 der Richtlinie (EU) 2016/1148 benannte zentrale Anlaufstelle.

(6) Die EBA, die ESMA oder die EIOPA und die EZB bewerten die Relevanz des schwerwiegenden IKT-bezogenen Vorfalls für andere einschlägige Behörden und benachrichtigen diese so bald wie möglich entsprechend. Die EZB unterrichtet die Mitglieder des Europäischen Systems der Zentralbanken über die für das Zahlungssystem relevanten Aspekte. Auf Grundlage dieser Unterrichtung treffen die zuständigen Behörden gegebenenfalls alle für die unmittelbare Stabilität des Finanzsystems notwendigen Schutzvorkehrungen.

Artikel 18

Harmonisierung von Inhalt und Vorlagen von Meldungen

(1) Die ESA erarbeiten über den Gemeinsamen Ausschuss und nach Abstimmung mit der ENISA und der EZB:

a) gemeinsame Entwürfe technischer Regulierungsstandards, um:

1) den Inhalt von Berichten über schwerwiegende IKT-bezogene Vorfälle festzulegen;

2) die Bedingungen, unter denen Finanzunternehmen nach vorheriger Genehmigung durch die zuständige Behörde die in diesem Kapitel festgelegten Meldepflichten an einen Drittanbieter delegieren können, zu präzisieren;

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

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 xx 202x [*Amt für Veröffentlichungen: Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*].

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. 1095/2010 und (EU) Nr. 1094/2010 zu ergänzen.

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

Artikel 19

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 Bericht werden Möglichkeiten sondiert, um den Meldefluss zu IKT-bezogenen Vorfällen zu erleichtern, verbundene Kosten zu senken und thematische Analysen mit Blick auf eine stärkere aufsichtliche Konvergenz zu unterstützen.

(2) Der Bericht gemäß Absatz 1 umfasst mindestens die folgenden Aspekte:

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

b) Vorteile, Grenzen und mögliche Risiken;

c) Elemente des Betriebsmanagements;

d) Voraussetzungen für die Mitgliedschaft;

e) Modalitäten für den Zugang von Finanzunternehmen und zuständigen nationalen Behörden zur EU-Plattform;

f) eine vorläufige Bewertung der finanziellen Kosten, die durch die Einrichtung der operativen Plattform zur Unterstützung der 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 xx 202x [*ABl.: Datum 3 Jahre nach Tag des Inkrafttretens einfügen*].

Artikel 20

Stellungnahmen von Aufsichtsbehörden

(1) Nach Eingang eines Berichts gemäß Artikel 17 Absatz 1 bestätigt die zuständige Behörde den Eingang der Meldung und übermittelt dem Finanzunternehmen schnellstmöglich alle erforderlichen Stellungnahmen oder Leitlinien, um insbesondere Abhilfemaßnahmen auf Ebene des Unternehmens oder Möglichkeiten zur Minimierung nachteiliger Auswirkungen über Sektoren hinweg zu erörtern.

(2) Die ESA berichten jährlich über den Gemeinsamen Ausschuss in anonymisierter und aggregierter Form über die Meldungen zuständiger Behörden zu schwerwiegenden IKT-bezogenen Vorfällen; aus solchen Berichten gehen mindestens die Zahl schwerwiegender IKT-bezogener Vorfälle, ihre Art, die Auswirkungen auf die

Geschäftstätigkeit von Finanzunternehmen oder Kunden sowie die Kosten und ergriffene Abhilfemaßnahmen hervor.

Die ESA sprechen Warnungen aus und erstellen hochwertige Statistiken, um Einschätzungen zu Bedrohungen und Anfälligkeiten im IKT-Bereich mit entsprechenden Zahlen zu unterlegen.

KAPITEL IV

PRÜFUNG DER DIGITALEN BETRIEBSSTABILITÄT

Artikel 21

Allgemeine Anforderungen für Prüfungen der digitalen Betriebsstabilität

(1) Um die Abwehrbereitschaft gegenüber IKT-bezogenen Vorfällen zu bewerten, Schwachstellen, Mängel oder Lücken in Bezug auf die digitale Betriebsstabilität zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erarbeiten, pflegen und überprüfen Finanzunternehmen unter gebührender Berücksichtigung ihrer Größe, ihrer Geschäfts- und Risikoprofile ein solides und umfassendes Programm zur Prüfung der digitalen Betriebsstabilität als integraler Bestandteil des in Artikel 5 genannten IKT-Risikomanagementrahmens.

(2) Das Programm zur Prüfung der digitalen Betriebsstabilität umfasst eine Reihe von Bewertungen, Prüfungen, Methoden, Verfahren und Instrumenten, die gemäß den Bestimmungen der Artikel 22 und 23 anzuwenden sind.

(3) Bei der Durchführung des in Absatz 1 genannten Programms zur Prüfung der digitalen Betriebsstabilität wenden Finanzunternehmen einen risikobasierten Ansatz an und berücksichtigen die sich verändernden Szenarien für IKT-Risiken, etwaige spezifische Risiken, denen das Finanzunternehmen ausgesetzt ist oder ausgesetzt sein könnte, die Kritikalität von Informationsressourcen und erbrachten Dienstleistungen sowie alle sonstigen Faktoren, die das Finanzunternehmen für angemessen hält.

(4) Finanzunternehmen stellen sicher, dass Prüfungen von unabhängigen, internen oder externen Parteien durchgeführt werden.

(5) Finanzunternehmen legen Verfahren und Strategien zur Priorisierung, Klassifizierung und Behebung aller während der Prüfungen erkannten Probleme fest und legen interne Validierungsmethoden fest, um sicherzustellen, dass alle ermittelten Schwachstellen, Mängel oder Lücken umfassend angegangen werden.

(6) Finanzunternehmen prüfen alle kritischen IKT-Systeme und -Anwendungen mindestens einmal jährlich.

Artikel 22

Prüfung von IKT-Instrumenten und -Systemen

(1) Das in Artikel 21 genannte Programm für die Prüfung der digitalen Betriebsstabilität beinhaltet die Durchführung eines vollständigen Spektrums geeigneter Tests, darunter Bewertungen und Überprüfungen der Anfälligkeit, Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Überprüfungen der physischen Sicherheit, Fragebögen und

Scansoftwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests oder Penetrationstests.

(2) Finanzunternehmen im Sinne von Artikel 2 Absatz 1 Buchstaben f und g führen Bewertungen der Anfälligkeit durch, bevor neue oder bestehende Dienste, die kritische Funktionen, Anwendungen und Infrastrukturkomponenten des Finanzunternehmens unterstützen, eingerichtet oder erneut eingerichtet werden.

Artikel 23

Erweiterte Prüfungen von IKT-Instrumenten, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests

(1) Gemäß Absatz 4 ermittelte Finanzunternehmen führen mindestens alle 3 Jahre anhand bedrohungsorientierter Penetrationstests erweiterte Prüfungen durch.

(2) Prüfungen anhand bedrohungsorientierter Penetrationstests schließen mindestens die kritischen Funktionen und Dienstleistungen eines Finanzunternehmens ein und werden an Live-Produktionssystemen durchgeführt, die solche Funktionen unterstützen. Der genaue Umfang bedrohungsorientierter Penetrationstests, die auf Basis der Bewertung kritischer Funktionen und Dienste durchgeführt werden, wird von Finanzunternehmen festgelegt und von den zuständigen Behörden genehmigt.

Für die Zwecke von Unterabsatz 1 ermitteln Finanzunternehmen alle relevanten zugrunde liegenden IKT-Prozesse, -Systeme und -Technologien zur Unterstützung kritischer Funktionen und Dienste, einschließlich Funktionen und Dienstleistungen, die an IKT-Drittanbieter ausgelagert oder per Vertrag vergeben werden.

Sind IKT-Drittanbieter in das Spektrum der bedrohungsorientierten Penetrationstests einbezogen, ergreift das Finanzunternehmen alle erforderlichen Maßnahmen, um die Einbindung dieser Anbieter sicherzustellen.

Finanzunternehmen wenden wirksame Risikomanagementkontrollen an, um die Gefahr von potenziellen Auswirkungen auf Daten, Schäden an Vermögenswerten und Unterbrechungen kritischer Dienstleistungen oder Vorgänge im Finanzunternehmen selbst, in anderen Finanzunternehmen oder im Finanzsektor zu verringern.

Nach Abschluss der Prüfung und der Ausarbeitung von Berichten und Plänen mit Abhilfemaßnahmen legen das Finanzunternehmen und die externen Prüfer der zuständigen Behörde die Unterlagen vor, aus denen hervorgeht, dass die bedrohungsorientierten Penetrationstests anforderungsgemäß durchgeführt wurden. Die zuständigen Behörden validieren die Unterlagen und stellen eine Bescheinigung aus.

(3) Finanzunternehmen beauftragen Prüfer gemäß Artikel 24 mit dem Ziel, bedrohungsorientierte Penetrationstests durchzuführen.

Die zuständigen Behörden ermitteln Finanzunternehmen, die bedrohungsorientierte Penetrationstests durchzuführen haben, nach Kriterien, die der Größe, dem Umfang, der Tätigkeit und dem Gesamtrisikoprofil des Finanzunternehmens angemessen sind, und stützen sich dabei auf die Bewertung von:

a) wirkungsbezogenen Faktoren, darunter insbesondere die Kritikalität der vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten;

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

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

(4) Die EBA, die ESMA und die EIOPA arbeiten in Abstimmung mit der EZB und unter Berücksichtigung einschlägiger Unionsrahmen, die für intelligenzgestützte Penetrationstests gelten, Entwürfe technischer Regulierungsstandards aus, in denen Folgendes präzisiert wird:

a) die für die Zwecke der Anwendung von Absatz 6 dieses Artikels herangezogenen Kriterien;

b) Anforderungen hinsichtlich:

a) des Umfangs der in Absatz 2 dieses Artikels genannten bedrohungsorientierten Penetrationstests;

b) der Prüfmethodik und des Prüfkonzepts für jede einzelne Phase des Prüfverfahrens;

c) der Ergebnisse, des Abschlusses und der Korrekturphasen der Prüfungen;

c) der Art der aufsichtlichen Zusammenarbeit, die für die Umsetzung bedrohungsorientierter Penetrationstests 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.

Die ESA legen der Kommission diese Entwürfe für technische Regulierungsstandards bis zum [*ABl.*: *bitte Datum 2 Monate vor dem Tag des Inkrafttretens einfügen*] vor.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme technischer Regulierungsstandards nach Unterabsatz 2 gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1095/2010 und (EU) Nr. 1094/2010 zu ergänzen.

Artikel 24

Anforderungen an Prüfer

(1) Finanzunternehmen ziehen für bedrohungsorientierte Penetrationstests nur Prüfer heran, die:

a) von höchster Eignung und Ansehen sind;

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

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

d) im Falle externer Prüfer eine unabhängige Gewähr oder einen Bestätigungsvermerk in Bezug auf die zuverlässige Steuerung von Risiken vorlegen, die mit der Durchführung bedrohungsorientierter Penetrationstests

verbunden sind, darunter auch der angemessene Schutz vertraulicher Informationen des Finanzunternehmens und die Beseitigung der geschäftlichen Risiken des Finanzunternehmens;

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

(2) Finanzunternehmen stellen sicher, dass in Vereinbarungen, die mit externen Prüfern geschlossen werden, eine zuverlässige Verwaltung der Ergebnisse bedrohungsorientierter Penetrationstests vorgesehen ist und ihre Verarbeitung, einschließlich Generierung, Entwurf, Speicherung, Aggregation, Berichterstattung, Weitergabe oder Vernichtung, keine Risiken für das Finanzunternehmen mit sich bringt.

KAPITEL V

STEUERUNG DES RISIKOS DURCH IKT-DRITTANBIETER

ABSCHNITT I

GRUNDSÄTZE FÜR EINE ZUVERLÄSSIGE STEUERUNG DES RISIKOS DURCH IKT-DRITTANBIETER

Artikel 25

Allgemeine Grundsätze

Finanzunternehmen steuern das Risiko durch IKT-Drittanbieter als integralen Bestandteil des IKT-Risikos innerhalb ihres IKT-Risikomanagementrahmens und im Einklang mit den folgenden Grundsätzen:

(1) Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Diensten für die Ausübung ihrer Geschäftstätigkeit getroffen haben, haften jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen in dieser Verordnung und den anwendbaren Rechtsvorschriften über Finanzdienstleistungen.

(2) Bei der Steuerung des Risikos durch IKT-Drittanbieter tragen Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung, wobei Folgendes zu berücksichtigen ist:

a) Ausmaß, Komplexität und Relevanz IKT-bezogener Abhängigkeiten,

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

(3) Finanzinstitute verabschieden im Rahmen ihres IKT-Risikomanagementrahmens eine Strategie für das Risiko durch IKT-Drittanbieter und überprüfen diese regelmäßig, wobei die in Artikel 5 Absatz 9 Buchstabe g genannte Strategie bei Nutzung mehrerer Anbieter Berücksichtigung findet. Diese Strategie umfasst eine

Politik für die Nutzung von IKT-Diensten, die von IKT-Drittanbietern erbracht werden, und gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis. Das Leitungsorgan überprüft regelmäßig Risiken, die im Zusammenhang mit der Auslagerung kritischer oder wichtiger Funktionen ermittelt werden.

(4) 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 IKT-Diensten durch IKT-Drittanbieter bezieht.

Die vertraglichen Vereinbarungen gemäß Unterabsatz 1 werden angemessen dokumentiert, wobei zwischen Vereinbarungen, die kritische oder wichtige Funktionen abdecken, und solchen Unterschieden wird, bei denen dies nicht der Fall ist.

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

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

Finanzunternehmen unterrichten die zuständige Behörde zeitnah über die geplante Vergabe von Aufträgen für kritische oder wichtige Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig wurde.

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

a) beurteilen, ob sich die vertragliche Vereinbarung auf eine kritische oder wichtige 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 solche vertraglichen Vereinbarungen dazu beitragen können, das IKT-Konzentrationsrisiko zu erhöhen;

d) bei potenziellen IKT-Drittanbietern alle gebotene Sorgfalt walten lassen und während der gesamten Auswahl- und Bewertungsprozesse sicherstellen, dass der IKT-Drittanbieter geeignet ist;

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

(6) Finanzunternehmen dürfen nur vertragliche Vereinbarungen mit IKT-Drittanbietern schließen, die hohe, angemessene und aktuelle Standards für Informationssicherheit einhalten.

(7) Bei der Ausübung der Zugangs-, Inspektions- und Prüfrechte in Bezug auf den IKT-Drittanbieter bestimmen Finanzunternehmen nach einem risikobasierten Ansatz

vorab die Häufigkeit von Prüfungen und Inspektionen und die zu prüfenden Bereiche, indem allgemein anerkannte Prüfungsgrundsätze im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Prüfungsgrundsätze eingehalten werden.

Bei vertraglichen Vereinbarungen, die ein hohes Maß an technologischer Komplexität mit sich bringen, überprüft das Finanzunternehmen, ob interne Prüfer, Prüferpools oder externe Prüfer über die Fähigkeiten und Kenntnisse verfügen, die für die wirksame Durchführung einschlägiger Prüfungen und Bewertungen erforderlich sind.

(8) Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Diensten zumindest unter folgenden Umständen gekündigt werden:

a) Verstoß des IKT-Drittanbieters gegen geltende Gesetze, Verordnungen oder Vertragsbedingungen;

b) Umstände, die im Laufe der Überwachung des Risikos durch IKT-Drittanbieter festgestellt wurden und die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen beeinträchtigen können, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittanbieters auswirken;

c) nachweisliche Schwächen des IKT-Drittanbieters mit Blick auf sein allgemeines IKT-Risikomanagement und insbesondere die Art und Weise, in der er die Sicherheit und Integrität vertraulicher, personenbezogener oder anderweitig sensibler Daten oder nicht personenbezogener Informationen gewährleistet;

d) Umstände, unter denen die zuständige Behörde das Finanzunternehmen infolge der jeweiligen vertraglichen Vereinbarung nicht mehr wirksam beaufsichtigen kann.

(9) Finanzunternehmen richten Ausstiegsstrategien ein, um Risiken Rechnung zu tragen, die auf Ebene des IKT-Drittanbieters entstehen können, darunter insbesondere ein möglicher Ausfall des IKT-Drittanbieters, eine Verschlechterung der Qualität der bereitgestellten Funktionen, Unterbrechungen der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Dienstleistungen oder ein erhebliches Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der Funktion.

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

a) Störung ihrer Geschäftstätigkeit,

b) Einschränkung der Einhaltung aufsichtsrechtlicher Anforderungen,

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

Ausstiegsstrategien müssen umfassend, dokumentiert und gegebenenfalls ausreichend erprobt sein.

Finanzunternehmen ermitteln alternative Lösungen und entwickeln Übergangspläne, die es ihnen ermöglichen, die vertraglich vereinbarten Funktionen und relevanten Daten vom IKT-Drittanbieter zu entfernen und sie sicher und vollständig an

alternative Anbieter weiterzuleiten oder wieder in die eigenen Systeme zu überführen.

Finanzunternehmen ergreifen geeignete Notfallmaßnahmen, um unter allen in Unterabsatz 1 genannten Umständen die Fortführung des Geschäftsbetriebs zu gewährleisten.

(10) Die ESA arbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Durchführungsstandards aus, um die Standardvorlagen für die Zwecke des in Absatz 4 genannten Informationsregisters festzulegen.

Die ESA legen der Kommission diese Entwürfe für technische Durchführungsstandards bis zum [*ABl.*: *Datum 1 Jahr nach Inkrafttreten dieser Verordnung einfügen*] vor.

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

(11) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe für Regulierungsstandards:

a) um den detaillierten Inhalt der Politik, die in Absatz 3 in Bezug auf die vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten, die von IKT-Drittanbietern erbracht werden, genannt wird, unter Bezugnahme auf die Hauptphasen des Lebenszyklus der jeweiligen Vereinbarungen über die Nutzung von IKT-Diensten weiter zu präzisieren;

b) um die Arten von Informationen näher zu spezifizieren, die in das in Absatz 4 genannte Informationsregister aufzunehmen sind.

Die ESA legen der Kommission diese Entwürfe für technische Regulierungsstandards bis zum [*Amt für Veröffentlichungen*: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*] vor.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme technischer Regulierungsstandards nach Unterabsatz 2 gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1095/2010 und (EU) Nr. 1094/2010 zu ergänzen.

Artikel 26

Vorläufige Bewertung des IKT-Konzentrationsrisikos und weiterer Vereinbarungen über weiteres Outsourcing

(1) Bei der Ermittlung und Bewertung des IKT-Konzentrationsrisikos gemäß Artikel 25 Absatz 5 Buchstabe c berücksichtigen Finanzunternehmen, ob der Abschluss einer vertraglichen Vereinbarung in Bezug auf die IKT-Dienste Folgendes herbeiführen würde:

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

b) mehrfache vertragliche Vereinbarungen über die Erbringung von IKT-Diensten mit demselben IKT-Drittanbieter oder mit eng verbundenen IKT-Drittanbietern.

Finanzunternehmen wägen Nutzen und Kosten alternativer Lösungen ab, z. B. die Nutzung verschiedener IKT-Drittanbieter, 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-Diensten die Möglichkeit vorgesehen, dass ein IKT-Drittanbieter eine kritische oder wichtige Funktion an andere IKT-Drittanbieter ausgelagert, wägen Finanzunternehmen die Vorteile und Risiken ab, die im Zusammenhang mit einer solchen möglichen Untervergabe entstehen können, insbesondere sofern der IKT-Unterauftragnehmer in einem Drittland niedergelassen ist.

Wenn vertragliche Vereinbarungen über die Nutzung von IKT-Diensten mit einem in einem Drittland niedergelassenen IKT-Drittanbieter geschlossen werden, berücksichtigen die Finanzunternehmen mindestens die folgenden Faktoren:

a) die Einhaltung des Datenschutzes;

b) die wirksame Durchsetzung des Rechts;

c) Bestimmungen des Insolvenzrechts, die im Falle der Insolvenz des IKT-Drittanbieters anwendbar wären;

d) etwaige Einschränkungen, die sich im Zusammenhang mit der Wiederherstellung der Daten des Finanzunternehmens im Notfall ergeben können.

Finanzunternehmen bewerten, 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 27

Wesentliche Vertragsbestimmungen

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

(2) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten umfassen mindestens Folgendes:

a) eine klare und vollständige Beschreibung aller Funktionen und Dienstleistungen, die der IKT-Drittanbieter zu erbringen hat, wobei anzugeben ist, ob die Vergabe von Unteraufträgen für kritische oder wichtige Funktionen oder wesentlicher Teile davon zulässig ist, und – wenn ja – welche Bedingungen für diese Unterauftragsvergabe gelten;

b) die Standorte, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und Dienstleistungen zu erbringen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittanbieter, das

Finanzunternehmen zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt;

c) Bestimmungen über Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten und über die Gewährleistung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Falle einer Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit des IKT-Drittanbieters verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;

d) vollständige Leistungsbeschreibungen, einschließlich Aktualisierungen und Überarbeitungen, sowie präzise quantitative und qualitative Leistungsziele innerhalb der vereinbarten Leistungsniveaus, um eine wirksame Überwachung durch das Finanzunternehmen zu ermöglichen und unverzüglich geeignete Korrekturmaßnahmen zu ermöglichen, wenn vereinbarte Leistungsniveaus nicht erreicht werden;

e) Kündigungsfristen und Berichtspflichten des IKT-Drittanbieters gegenüber dem Finanzunternehmen, einschließlich der Meldung von Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittanbieters auswirken könnten, kritische oder wichtige Funktionen gemäß vereinbarten Leistungsniveaus wirksam bereitzustellen;

f) die Verpflichtung des IKT-Drittanbieters, im Falle eines IKT-Vorfalls ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;

g) Anforderungen an den IKT-Drittanbieter, Notfallpläne zu implementieren und zu erproben und über Maßnahmen, Instrumente und Strategien für IKT-Sicherheit zu verfügen, die eine sichere Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen angemessen gewährleisten;

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

   i) Zugangs-, Inspektions- und Prüfrechte des Finanzunternehmens oder eines beauftragten Dritten sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen, deren tatsächliche Ausübung nicht durch andere vertragliche Vereinbarungen oder Durchführungsmaßnahmen behindert oder eingeschränkt wird;

   ii) das Recht, alternative Sicherheitsniveaus zu vereinbaren, wenn die Rechte anderer Kunden beeinträchtigt werden;

   iii) die Verpflichtung zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen, die vom Finanzunternehmen durchgeführt werden, sowie Einzelheiten zu Umfang, Modalitäten und Häufigkeit dezentraler Prüfungen;

i) die Verpflichtung des IKT-Drittanbieters, uneingeschränkt mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden, einschließlich der von diesen beauftragten Personen, zusammenzuarbeiten;

j) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Vertragsbeendigung entsprechend den Erwartungen der zuständigen Behörden;

k) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums:

a) in dem der IKT-Drittanbieter weiterhin die entsprechenden Funktionen oder Dienste bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern;

b) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT-Drittanbieter zu wechseln oder auf Lösungen vor Ort umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.

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

(4) Die ESA arbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards aus, um die Aspekte zu präzisieren, die ein Finanzunternehmen bei der Untervergabe kritischer oder wichtiger Funktionen bestimmen und bewerten muss, um die Bestimmungen von Absatz 2 Buchstabe a ordnungsgemäß umzusetzen.

Die ESA legen der Kommission diese Entwürfe für technische Regulierungsstandards bis zum [*ABl.*: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*] vor.

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

ABSCHNITT II

AUFSICHTSRAHMEN FÜR KRITISCHE IKT-DRITTANBIETER

Artikel 28

Benennung kritischer IKT-Drittanbieter

(1) Die ESA nehmen über den Gemeinsamen Ausschuss und auf Empfehlung des gemäß Artikel 29 Absatz 1 eingerichteten Aufsichtsforums folgende Aufgaben wahr:

a) Benennung der IKT-Drittanbieter, die für Finanzunternehmen von entscheidender Bedeutung sind, unter Berücksichtigung der in Absatz 2 genannten Kriterien;

b) Ernennung der EBA, der ESMA oder der EIOPA zur federführenden Aufsichtsinstanz für jeden kritischen IKT-Drittanbieter, je nachdem, ob der Gesamtwert der Vermögenswerte von Finanzunternehmen, die die Dienste dieses kritischen IKT-Drittanbieters nutzen und die unter eine der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 bzw. (EU) Nr. 1095/2010 fallen, mehr als die Hälfte des Gesamtwerts der Aktiva aller Finanzunternehmen darstellt, die die Dienste des kritischen IKT-Drittanbieters

nutzen – so wie die konsolidierten oder einzelnen Bilanzen (sofern keine Konsolidierung erfolgt) dieser Finanzunternehmen belegen.

(2) Die Ernennung nach Absatz 1 Buchstabe a basiert auf den folgenden Kriterien:

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

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

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

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

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

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

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

ii) der Schwierigkeiten bei der teilweisen oder vollständigen Migration der einschlägigen Daten und Arbeitslasten vom jeweiligen Drittanbieter zu einem anderen IKT-Drittanbieter, 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;

e) der Zahl der Mitgliedstaaten, in denen der betreffende IKT-Drittanbieter Dienstleistungen erbringt;

f) der Zahl der Mitgliedstaaten, in denen Finanzunternehmen tätig sind, die den betreffenden IKT-Drittanbieter in Anspruch nehmen.

(3) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zu erlassen, um die in Absatz 2 genannten Kriterien zu ergänzen.

(4) Der Ernennungsmechanismus nach Absatz 1 Buchstabe a darf erst angewendet werden, wenn die Kommission einen delegierten Rechtsakt gemäß Absatz 3 erlassen hat.

(5) Der Ernennungsmechanismus nach Absatz 1 Buchstabe a gilt nicht für IKT-Drittanbieter, die Aufsichtsrahmen unterliegen, die zur Unterstützung der in Artikel 127 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union genannten Aufgaben eingerichtet wurden.

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

(7) Die zuständigen Behörden übermitteln dem gemäß Artikel 29 eingerichteten Aufsichtsforum für die Zwecke von Absatz 1 Buchstabe a die in Artikel 25 Absatz 4 genannten Berichte auf jährlicher und aggregierter Basis. Das Aufsichtsforum bewertet die Abhängigkeiten von Finanzunternehmen gegenüber IKT-Drittanbietern auf der Grundlage der von den zuständigen Behörden übermittelten Informationen.

(8) IKT-Drittanbieter, die nicht in der in Absatz 6 genannten Liste aufgeführt sind, können beantragen, in diese Liste aufgenommen zu werden.

Für die Zwecke von Unterabsatz 1 reicht der IKT-Drittanbieter bei der EBA, der ESMA oder der EIOPA einen begründeten Antrag ein, die über den Gemeinsamen Ausschuss entscheiden, ob dieser IKT-Drittanbieter in diese Liste gemäß Absatz 1 Buchstabe a aufgenommen werden soll.

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

(9) Finanzunternehmen dürfen keinen IKT-Drittanbieter mit Sitz in einem Drittland in Anspruch nehmen, der gemäß Absatz 1 Buchstabe a als kritisch eingestuft würde, wenn er in der Union niedergelassen wäre.

Artikel 29

Struktur des Aufsichtsrahmens

(1) Der Gemeinsame Ausschuss richtet gemäß Artikel 57 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 das Aufsichtsforum als Unterausschuss ein, der die Arbeit des Gemeinsamen Ausschusses und der in Artikel 28 Absatz 1 Buchstabe b genannten federführenden Aufsichtsinstanz im Bereich des Risikos durch IKT-Drittanbieter in allen Finanzsektoren unterstützt. Das Aufsichtsforum erarbeitet die Entwürfe gemeinsamer Positionen und gemeinsamer Maßnahmen des Gemeinsamen Ausschusses in diesem Bereich.

(2) Das Aufsichtsforum erörtert regelmäßig einschlägige Entwicklungen in Bezug auf IKT-Risiken und -Anfälligkeiten und fördert einen kohärenten Ansatz bei der Überwachung des Risikos durch IKT-Drittanbieter auf Unionsebene.

(3) Das Aufsichtsforum führt jährlich eine gemeinsame Bewertung der Ergebnisse und Erkenntnisse von Aufsichtstätigkeiten durch, die für alle kritischen IKT-Drittanbieter durchgeführt wurden, und fördert Koordinierungsmaßnahmen, um die digitale Betriebsstabilität von Finanzunternehmen zu erhöhen, bewährte Verfahren zur

Eindämmung des IKT-Konzentrationsrisikos zu fördern und Möglichkeiten zur Abschwächung sektorübergreifender Risikotransfers auszuloten.

(4) Das Aufsichtsforum legt umfassende Benchmarks kritischer IKT-Drittanbieter 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.

(5) Das Aufsichtsforum setzt sich aus den Vorsitzenden der ESA und einem hochrangigen Vertreter des Personals der betreffenden zuständigen Behörde jedes Mitgliedstaats zusammen. Die Exekutivdirektoren jeder ESA und ein Vertreter der Europäischen Kommission, des ESRB, der EZB und der ENISA nehmen als Beobachter am Aufsichtsforum teil.

(6) Gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 geben die ESA Leitlinien für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden für die Zwecke dieses Abschnitts heraus, in denen die detaillierten Verfahren und Bedingungen für die Ausführung von Aufgaben zwischen zuständigen Behörden und den ESA sowie die Einzelheiten zum Austausch von Informationen enthalten sind, die zuständige Behörden benötigen, um die Weiterbehandlung von Empfehlungen zu gewährleisten, die von federführenden Aufsichtsinstanzen gemäß Artikel 31 Absatz 1 Buchstabe d an kritische IKT-Drittanbieter gerichtet werden.

(6) Die in diesem Abschnitt dargelegten Anforderungen gelten unbeschadet der Anwendung der Richtlinie (EU) 2016/1148 und anderer Aufsichtsvorschriften der Union, die für Anbieter von Cloud-Computing-Diensten gelten.

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

Artikel 30

Aufgaben der federführenden Aufsichtsinstanz

(1) Die federführende Aufsichtsinstanz bewertet, ob jeder kritische IKT-Drittanbieter über umfassende, robuste und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen zur Steuerung der IKT-Risiken verfügt, die er für Finanzunternehmen mit sich bringen kann.

(2) Die in Absatz 1 genannte Bewertung umfasst:

a) IKT-Anforderungen, um insbesondere die Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste zu gewährleisten, die der kritische IKT-Drittanbieter für Finanzunternehmen erbringt, sowie die Fähigkeit, jederzeit hohe Standards in Bezug auf Sicherheit, Vertraulichkeit und Integrität 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-Pläne für die Fortführung des Geschäftsbetriebs und die Wiederherstellung im Notfall;

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 IKT-bezogener Vorfälle an die Finanzunternehmen sowie die Bewältigung und Lösung dieser Vorfälle, darunter insbesondere Cyberangriffe;

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

g) die Prüfung von IKT-Systemen, Infrastrukturen und Kontrollen;

h) IKT-Prüfungen;

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

(3) Die federführende Aufsichtsinstanz verabschiedet auf der Grundlage der in Absatz 1 genannten Bewertung einen klaren, detaillierten und durchdachten individuellen Aufsichtsplan für jeden kritischen IKT-Drittanbieter. Dieser Plan wird dem kritischen IKT-Drittanbieter jedes Jahr übermittelt.

(4) Sobald die in Absatz 3 genannten jährlichen Aufsichtspläne festgelegt und den kritischen IKT-Drittanbietern übermittelt wurden, dürfen zuständige Behörden Maßnahmen in Bezug auf kritische IKT-Drittanbieter nur im Einvernehmen mit der federführenden Aufsichtsinstanz ergreifen.

Artikel 31

Befugnisse der federführenden Aufsichtsinstanz

(1) Die federführende Aufsichtsinstanz hat zur Wahrnehmung der in diesem Abschnitt dargelegten Aufgaben folgende Befugnisse:

a) alle einschlägigen Informationen und Unterlagen gemäß Artikel 32 anzufordern;

b) allgemeine Untersuchungen und Inspektionen gemäß den Artikeln 33 und 34 durchzuführen;

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

d) Empfehlungen zu den in Artikel 30 Absatz 2 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 Instanz für die Gewährleistung der IKT-Sicherheit von Diensten, die Finanzunternehmen erbracht werden, für relevant hält;

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

iii) jede geplante Unterauftragsvergabe, einschließlich weiteren Outsourcings, wenn die federführende Aufsichtsinstanz der Auffassung ist, dass eine weitere Unterauftragsvergabe Risiken für die Erbringung von Dienstleistungen durch das Finanzunternehmen oder Risiken für die Finanzstabilität mit sich bringen kann, sobald eine Prüfung gemäß den Artikeln 32 und 33 von Vereinbarungen über die Auftragsweitervergabe erfolgt ist, einschließlich Vereinbarungen über weiteres Outsourcing, die die kritischen IKT-Drittanbieter mit anderen IKT-Drittanbietern oder mit IKT-Unterauftragnehmern mit Sitz in einem Drittland zu schließen beabsichtigen;

iv) von einer weiteren Vereinbarung über die Auftragsweitervergabe abzusehen, wenn die folgenden kumulativen Bedingungen erfüllt sind:

– bei dem ausgewählten Unterauftragnehmer handelt es sich um einen IKT-Drittanbieter oder einen IKT-Unterauftragnehmer mit Sitz in einem Drittland;

– die Vergabe von Unteraufträgen betrifft eine kritische oder wichtige Funktion des Finanzunternehmens.

(2) Die federführende Aufsichtsinstanz konsultiert das Aufsichtsforum, bevor sie die in Absatz 1 genannten Befugnisse ausübt.

(3) Kritische IKT-Drittanbieter arbeiten nach Treu und Glauben mit der federführenden Aufsichtsinstanz zusammen und unterstützen die federführende Aufsichtsinstanz bei der Erfüllung ihrer Aufgaben.

(4) Die federführende Aufsichtsinstanz kann ein Zwangsgeld verhängen, um den kritischen IKT-Drittanbieter zur Einhaltung von Absatz 1 Buchstaben a, b und c zu zwingen.

(5) Das in Absatz 4 genannte Zwangsgeld wird täglich bis zur Einhaltung der Vorschriften und für höchstens sechs Monate nach der Mitteilung an den kritischen IKT-Drittanbieter verhängt.

(6) Die Höhe des Zwangsgelds, berechnet ab dem in der Entscheidung über die Verhängung des Zwangsgelds genannten Zeitpunkt, beträgt 1 % des durchschnittlichen globalen Tagesumsatzes, den der kritische IKT-Drittanbieter im vorangegangenen Geschäftsjahr erzielt hat.

(7) Zwangsgelder sind administrativer Art und vollstreckbar. Die Zwangsvollstreckung erfolgt nach den Vorschriften des Zivilprozessrechts des Mitgliedstaats, in dessen Hoheitsgebiet Prüfungen 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.

(8) Die ESA veröffentlichen sämtliche verhängten Zwangsgelder, sofern dies die Stabilität der Finanzmärkte nicht ernsthaft gefährdet oder den Beteiligten daraus kein unverhältnismäßiger Schaden erwächst.

(9) Die federführende Aufsichtsinstanz gibt den Vertretern des dem Verfahren unterliegenden kritischen IKT-Drittanbieters vor Verhängung eines Zwangsgeldes nach Absatz 4 Gelegenheit, zu den Feststellungen gehört zu werden, und stützt ihre Entscheidungen ausschließlich auf Feststellungen, zu denen sich der kritische IKT-Drittanbieter, der Gegenstand des Verfahrens ist, äußern konnte. Die Verteidigungsrechte der Personen, die dem Verfahren unterworfen sind, werden während des Verfahrens in vollem Umfang gewahrt. Diese Personen haben vorbehaltlich des berechtigten Interesses anderer Personen an der Wahrung ihrer Geschäftsgeheimnisse Recht auf Einsicht in die Akten. Vom Recht auf Akteneinsicht ausgenommen sind vertrauliche Informationen sowie interne vorbereitende Unterlagen der federführenden Aufsichtsinstanz.

Artikel 32

Informationsersuchen

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

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

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

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert die Art der geforderten Informationen;

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

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

(3) Fordert die federführende Aufsichtsinstanz nach 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 die Art der geforderten Informationen;

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

e) sie nennt die Zwangsgelder, die nach Artikel 31 Absatz 4 verhängt werden, wenn die geforderten Informationen unvollständig sind;

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) Vertreter kritischer IKT-Drittanbieter stellen die angeforderten Informationen zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können die Auskünfte im Namen ihrer Mandanten erteilen. Kritische IKT-Drittanbieter bleiben in vollem Umfang dafür verantwortlich, dass die erteilten Auskünfte vollständig, sachlich richtig und nicht irreführend sind.

(5) Die federführende Aufsichtsinstanz übermittelt den zuständigen Behörden der Finanzunternehmen, die die Dienste kritischer IKT-Drittanbieter in Anspruch nehmen, unverzüglich eine Kopie der Entscheidung, Informationen bereitzustellen.

Artikel 33
Allgemeine Untersuchungen

(1) Die federführende Aufsichtsinstanz kann zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung mit Unterstützung des in Artikel 34 Absatz 1 genannten Untersuchungsteams die erforderlichen Untersuchungen von IKT-Drittanbietern durchführen:

(2) Die federführende Aufsichtsinstanz 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 Verfahren und sonstigen Materialien anzufertigen oder zu verlangen;

c) Vertreter des IKT-Drittanbieters 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 Aufsichtsinstanz zu Untersuchungen gemäß Absatz 1 bevollmächtigte Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Vollmacht aus, in der Gegenstand und Zweck der Untersuchung angegeben werden.

In der Vollmacht sind auch die in Artikel 31 Absatz 4 vorgesehenen Zwangsgelder für den Fall anzugeben, dass die angeforderten Aufzeichnungen, Daten, Verfahren oder sonstigen Materialien oder die Antworten auf Fragen, die den Vertretern des IKT-Drittanbieters gestellt werden, nicht vorgelegt werden oder unvollständig sind.

(4) Die Vertreter der IKT-Drittanbieter sind verpflichtet, sich den Untersuchungen auf der Grundlage einer Entscheidung der federführenden Aufsichtsinstanz zu unterziehen. In dem Beschluss wird Folgendes angegeben: Gegenstand und Zweck

der Untersuchung, die nach Artikel 31 Absatz 4 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.

(5) Die federführenden Aufsichtsinstanzen unterrichten zuständige Behörden rechtzeitig vor der Untersuchung über die Finanzunternehmen, die diesen IKT-Drittanbieter in Anspruch nehmen, sowie über die Untersuchung und die Identität der bevollmächtigten Personen.

Artikel 34
Vor-Ort-Prüfungen

(1) Die federführende Aufsichtsinstanz kann zur Wahrnehmung ihrer Aufgaben nach dieser Verordnung mit Unterstützung der in Artikel 35 Absatz 1 genannten Untersuchungsteams alle erforderlichen Vor-Ort-Prüfungen in Geschäftsräumen, auf Grundstücken oder in Gebäuden von IKT-Drittanbietern, wie Hauptverwaltungen, Betriebszentren, sekundären Räumlichkeiten, einleiten und durchführen und Offline-Prüfungen durchführen.

(2) Die Bediensteten und sonstigen Personen, die von der federführenden Aufsichtsinstanz zur Durchführung einer Vor-Ort-Prüfung ermächtigt wurden, können diese Geschäftsräume, Grundstücke oder Gebäude betreten und sind befugt, Geschäftsräume, Bücher oder Aufzeichnungen für die Dauer der Prüfung und in dem für die Prüfung erforderlichen Umfang zu versiegeln.

Sie üben ihre Befugnisse unter Vorlage einer schriftlichen Vollmacht aus, in der Gegenstand und Zweck der Prüfung sowie die in Artikel 31 Absatz 4 vorgesehenen Zwangsgelder angegeben sind, wenn sich die Vertreter der betreffenden IKT-Drittanbieter nicht der Prüfung unterziehen.

(3) Die federführenden Aufsichtsinstanzen unterrichten die zuständigen Behörden der Finanzunternehmen, die diesen IKT-Drittanbieter nutzen, rechtzeitig vor der Prüfung.

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

(5) Die federführenden Aufsichtsinstanzen unterrichten die kritischen IKT-Drittanbieter vor jedem geplanten Vor-Ort-Besuch mit angemessenem Vorlauf, es sei denn, eine solche Unterrichtung ist aufgrund einer Not- oder Krisensituation nicht möglich oder würden Umstände herbeiführen, unter denen die Prüfung oder das Audit nicht mehr wirksam wären.

(6) Der kritische IKT-Drittanbieter unterzieht sich den durch Beschluss der federführenden Aufsichtsinstanz angeordneten Vor-Ort-Prüfungen. In dem Beschluss wird Folgendes angegeben: Gegenstand, Zweck und Datum des Beginns der Prüfung, die nach Artikel 31 Absatz 4 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.

(7) Gelangen die Bediensteten und sonstige von der federführenden Aufsichtsinstanz bevollmächtigte Personen zu dem Schluss, dass ein kritischer IKT-Drittanbieter sich

einer gemäß diesem Artikel angeordneten Prüfung widersetzt, unterrichtet die federführende Aufsichtsinstanz den kritischen IKT-Drittanbieter über die Folgen einer solchen Wiederbesetzung, einschließlich der Möglichkeit für zuständige Behörden der betreffenden Finanzunternehmen, die mit diesem kritischen IKT-Drittanbieter geschlossenen vertraglichen Vereinbarungen zu kündigen.

Artikel 35

Laufende Aufsicht

(1) Bei der Durchführung allgemeiner Untersuchungen oder Vor-Ort-Prüfungen werden die federführenden Aufsichtsinstanzen von einem gemeinsamen Untersuchungsteam unterstützt, das für jeden kritischen IKT-Drittanbieter eingerichtet wird.

(2) Das in Absatz 1 genannte gemeinsame Untersuchungsteam umfasst höchstens zehn Mitglieder und setzt sich aus Mitarbeitern der federführenden Aufsichtsinstanz und der jeweils zuständigen Behörden zusammen, die die Finanzunternehmen beaufsichtigen, denen der kritische IKT-Drittanbieter Dienstleistungen erbringt, und beteiligt sich an der Vorbereitung und Durchführung der Aufsichtstätigkeiten. Alle Mitglieder des gemeinsamen Untersuchungsteams müssen über Fachwissen in den Bereichen IKT und operationelle Risiken verfügen. Das gemeinsame Untersuchungsteam arbeitet unter der Koordinierung eines benannten ESA-Mitarbeiters („Koordinator der federführenden Aufsichtsinstanz“).

(3) Die ESA arbeiten über den Gemeinsamen Ausschuss gemeinsame Entwürfe technischer Regulierungsstandards aus, um die Ernennung der Mitglieder des gemeinsamen Untersuchungsteams von den jeweils zuständigen Behörden sowie die Aufgaben und Arbeitsvereinbarungen des Untersuchungsteams zu präzisieren. Die ESA legen der Kommission diese Entwürfe für technische Regulierungsstandards bis zum [*ABl.*: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*] vor.

Der Kommission wird die Befugnis übertragen, die technischen Regulierungsstandards nach Unterabsatz 1 gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 zu erlassen.

(4) Innerhalb von 3 Monaten nach Abschluss einer Untersuchung oder Vor-Ort-Prüfung verabschiedet die federführende Aufsichtsinstanz nach Konsultation des Aufsichtsforums Empfehlungen, die die federführende Aufsichtsinstanz gemäß den in Artikel 31 genannten Befugnissen an den kritischen IKT-Drittanbieter richten muss.

(5) Die in Absatz 4 genannten Empfehlungen werden dem kritischen IKT-Drittanbieter und den zuständigen Behörden der Finanzunternehmen, für die er Dienstleistungen erbringt, unverzüglich übermittelt.

Federführende Aufsichtsinstanzen können zur Erfüllung der Aufsichtstätigkeiten alle einschlägigen Zertifizierungen Dritter und interne oder externe IKT-Prüfberichte Dritter berücksichtigen, die von dem kritischen IKT-Drittanbieter zur Verfügung gestellt werden.

Artikel 36

Harmonisierung der Voraussetzungen für die Durchführung der Aufsicht

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

a) die Informationen, die von einem kritischen IKT-Drittanbieter in dem Antrag auf freiwillige Einbindung gemäß Artikel 28 Absatz 8 bereitzustellen sind;

b) Inhalt und Format von Berichten, die für die Zwecke des Artikels 31 Absatz 1 Buchstabe c angefordert werden können;

c) die Darstellung der Informationen, einschließlich Struktur, Formaten und Methoden, die ein kritischer IKT-Drittanbieter gemäß Artikel 31 Absatz 1 vorlegen, offenlegen oder melden muss;

d) die Einzelheiten der von den zuständigen Behörden vorgenommenen Bewertung von Maßnahmen, die von kritischen IKT-Drittanbietern auf der Grundlage der Empfehlungen der federführenden Aufsichtsinstanzen gemäß Artikel 37 Absatz 2 ergriffen wurden.

(2) Die ESA legen der Kommission diese Entwürfe für technische Regulierungsstandards bis zum 1. Januar 20xx [*ABl.*: *Datum 1 Jahr nach dem Datum des Inkrafttretens einfügen*] vor.

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

Artikel 37

Folgemaßnahmen zuständiger Behörden

(1) Kritische IKT-Drittanbieter teilen der federführenden Aufsichtsinstanz innerhalb von 30 Kalendertagen nach Eingang der Empfehlungen, die von der federführenden Aufsichtsinstanz gemäß Artikel 31 Absatz 1 Buchstabe d verabschiedet werden, mit, ob sie beabsichtigen, diesen Empfehlungen Folge zu leisten. Die federführende Aufsichtsinstanz übermittelt diese Information unverzüglich den zuständigen Behörden.

(2) Die zuständigen Behörden überwachen, ob Finanzunternehmen den Risiken Rechnung tragen, die in den Empfehlungen der federführenden Aufsichtsinstanz an kritische IKT-Drittanbieter gemäß Artikel 31 Absatz 1 Buchstabe d ermittelt wurden.

(3) Gemäß Artikel 44 können zuständige Behörden von Finanzunternehmen verlangen, die Nutzung oder den Einsatz eines Dienstes, der von einem kritischen IKT-Drittanbieter bereitgestellt wird, vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind, die in den an den kritischen IKT-Drittanbieter gerichteten Empfehlungen ermittelt worden. Behörden können von Finanzunternehmen erforderlichenfalls verlangen, die einschlägigen vertraglichen Vereinbarungen, die mit kritischen IKT-Drittanbietern geschlossen wurden, ganz oder teilweise zu kündigen.

(4) Bei den in Absatz 3 genannten Entscheidungen berücksichtigen zuständige Behörden die Art und das Ausmaß des Risikos, das vom kritischen IKT-Drittanbieter 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-Drittanbieters zutage gefördert wurden;

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

d) ob der Verstoß vorsätzlich oder fahrlässig begangen wurde.

(5) Die zuständigen Behörden unterrichten die federführenden Aufsichtsinstanzen regelmäßig über die Herangehensweisen und Maßnahmen, die sie bei ihren Aufsichtsaufgaben in Bezug auf Finanzunternehmen gewählt haben, sowie über die von Letzteren ergriffenen vertraglichen Maßnahmen, wenn kritische IKT-Drittanbieter Empfehlungen, die von den federführenden Aufsichtsinstanzen ausgesprochen wurden, weder teilweise noch vollständig befolgt haben.

Artikel 38
Aufsichtsgebühren

(1) Die ESA erheben von kritischen IKT-Drittanbietern Gebühren, die die notwendigen Ausgaben der ESA für die Durchführung von Aufsichtsaufgaben gemäß dieser Verordnung vollständig decken, einschließlich der Erstattung aller Kosten, die durch die Arbeit zuständiger Behörden, die sich an den Aufsichtstätigkeiten gemäß Artikel 35 beteiligen, entstehen können.

Die Höhe einer Gebühr, die einem kritischen IKT-Drittanbieter in Rechnung gestellt wird, deckt alle Verwaltungskosten ab und steht in einem angemessenen Verhältnis zu dessen Umsatz.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung durch Festlegung der Höhe der Gebühren und der Art und Weise ihrer Entrichtung zu erlassen.

Artikel 39
Internationale Zusammenarbeit

(1) Die EBA, die ESMA und die EIOPA können im Einklang mit Artikel 33 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 bzw. (EU) Nr. 1095/2010 Verwaltungsvereinbarungen mit Regulierungs- und Aufsichtsbehörden von Drittländern schließen, um die internationale Zusammenarbeit in Bezug auf das Risiko durch IKT-Drittanbieter in verschiedenen Finanzbranchen zu fördern, insbesondere durch die Entwicklung bewährter Verfahren für die Überprüfung von IKT-Risikomanagementverfahren und -kontrollen, Abmilderungsmaßnahmen und Gegenmaßnahmen 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 Risikos durch IKT-Drittanbieter und den Auswirkungen auf die Finanzstabilität, die Marktintegrität, den Anlegerschutz oder das Funktionieren des Binnenmarkts liegt.

KAPITEL VI

VEREINBARUNGEN ÜBER DEN AUSTAUSCH VON INFORMATIONEN

Artikel 40

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 Betriebsstabilität von Finanzunternehmen zu stärken, insbesondere indem für Cyberbedrohungen sensibilisiert, die Verbreitung von Cyberbedrohungen eingeschränkt oder verhindert wird und die Verteidigungskapazitäten von Finanzunternehmen, Techniken zur Erkennung von Bedrohungen, Abmilderungsstrategien oder Phasen mit Gegenmaßnahmen 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[48] und Leitlinien für die Wettbewerbspolitik vollumfänglich befolgt werden.[49]

(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 öffentlicher Behörden und der Eigenschaft, in der diese in die Vereinbarungen über den Austausch von Informationen eingebunden werden können, 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 oder, je nach Sachlage, endet und diese Beendigung in Kraft ist.

KAPITEL VII

ZUSTÄNDIGE BEHÖRDEN

---

48 Gemäß der 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).

49 Mitteilung der Kommission – Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit, 2011/C 11/01.

Artikel 41

Zuständige Behörden

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

a) bei Kreditinstituten durch die gemäß Artikel 4 der Richtlinie 2013/36/EU benannte zuständige Behörde, unbeschadet der besonderen Aufgaben, die der EZB durch die Verordnung (EU) Nr. 1024/2013 übertragen wurden;

b) bei Zahlungsdienstleistern durch die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde;

c) bei E-Geld-Instituten durch die gemäß Artikel 37 der Richtlinie 2009/110/EG benannte zuständige Behörde;

d) bei Wertpapierfirmen durch die gemäß Artikel 4 der Richtlinie (EU) 2019/2034 benannte zuständige Behörde;

e) bei Anbietern von Kryptodienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Tokens und Emittenten signifikanter an Vermögenswerte geknüpfter Tokens durch die gemäß Artikel 3 Absatz 1 Buchstabe ee erster Gedankenstrich der [*Verordnung (EU) 20xx MiCA-Verordnung*] benannte zuständige Behörde;

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

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

h) bei Handelsplätzen und Datenbereitstellungsdiensten durch die gemäß Artikel 67 der Richtlinie 2014/65/EU benannte zuständige Behörde;

i) bei Transaktionsregistern durch die gemäß Artikel 55 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

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

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

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

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

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

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

p) bei Abschlussprüfern und Prüfungsgesellschaften durch die gemäß Artikel 3 Absatz 2 und Artikel 32 der Richtlinie 2006/43/EG benannte zuständige Behörde;

q) bei Administratoren kritischer Referenzwerte durch die gemäß den Artikeln 40 und 41 der *Verordnung xx/202x* benannte zuständige Behörde;

r) bei Crowdfunding-Dienstleistern durch die gemäß *Artikel x der Verordnung xx/202x* benannte zuständige Behörde;

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

Artikel 42

Zusammenarbeit mit den durch die Richtlinie (EU) 2016/1148 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 11 der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe zu ermöglichen, können die ESA und die zuständigen Behörden verlangen, zur Arbeit der Kooperationsgruppe eingeladen zu werden.

(2) Zuständige Behörden können sich gegebenenfalls an die zentrale Anlaufstelle und die nationalen Computer-Notfallteams, die in Artikel 8 bzw. 9 der Richtlinie (EU) 2016/1148 genannt werden, wenden.

Artikel 43

Sektorübergreifende Simulationsübungen, Kommunikation und Zusammenarbeit im Finanzbereich

(1) Die ESA können über den Gemeinsamen Ausschuss und in Zusammenarbeit mit den zuständigen Behörden, der EZB und dem ESRB Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um das Lagebewusstsein 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 EU-Ebene 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 EBA, die ESMA oder die EIOPA und die EZB arbeiten eng zusammen und tauschen Informationen aus, um ihren Aufgaben gemäß den Artikeln 42 bis 48 nachzukommen. Dabei stimmen sie ihre Aufsichtstätigkeit eng untereinander ab, um Verstöße gegen diese Verordnung festzustellen und 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 44

Verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen

(1) Zuständige 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 Befugnisse, um:

a) auf Unterlagen oder Daten jeglicher Form zuzugreifen, die nach Ansicht der zuständigen Behörde für die Ausführung ihrer Aufgaben von Belang sind, und Kopien von ihnen zu erhalten oder anzufertigen;

b) Prüfungen oder Ermittlungen vor Ort durchzuführen;

c) bei Verstößen gegen die Anforderungen dieser Verordnung Korrektur- und Abhilfemaßnahmen zu verlangen.

(3) Unbeschadet des Rechts der Mitgliedstaaten, strafrechtliche Sanktionen gemäß Artikel 46 zu verhängen, legen die Mitgliedstaaten geeignete 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 zuständigen Behörden die Befugnis, bei Verstößen gegen diese Verordnung mindestens die folgenden verwaltungsrechtlichen Sanktionen bzw. Abhilfemaßnahmen anzuwenden:

a) Erteilung einer Anweisung, wonach die natürliche oder juristische Person die Handlung zu unterlassen und von einer Wiederholung abzusehen hat;

b) 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) jede Art von Maßnahme, auch finanzieller Art, zu ergreifen, um sicherzustellen, dass Finanzunternehmen weiterhin die rechtlichen Anforderungen erfüllen;

d) soweit gemäß nationalem Recht zulässig, bereits existierende Aufzeichnungen von Datenübermittlungen im Besitz einer Telekommunikationsgesellschaft verlangen, 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) öffentliche Bekanntmachungen abgeben, einschließlich öffentlicher Bekanntgaben, in denen die Identität der natürlichen oder juristischen Person und die Art des Verstoßes angegeben sind.

(5) Gelten die in Absatz 2 Buchstabe c und Absatz 4 genannten Bestimmungen für juristische Personen, so statten die Mitgliedstaaten die zuständigen Behörden mit der Befugnis aus, vorbehaltlich der nach nationalem Recht geltenden Bedingungen die verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen gegen Mitglieder des

Leitungsorgans und gegen andere natürliche Personen zu verhängen, die nach nationalem Recht für den Verstoß verantwortlich sind.

(6) Die Mitgliedstaaten stellen sicher, dass alle Entscheidungen zur Verhängung der in Absatz 2 Buchstabe c festgelegten verwaltungsrechtlichen Sanktionen oder Abhilfemaßnahmen ordnungsgemäß begründet werden und dass gegen sie ein Rechtsbehelf eingelegt werden kann.

Artikel 45

Ausübung der Befugnis zur Verhängung von verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen

(1) Die zuständigen Behörden üben die Befugnisse zur Verhängung der in Artikel 44 genannten verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen innerhalb ihres nationalen Rechtsrahmens soweit erforderlich in folgender Weise aus:

a) direkt;

b) in Zusammenarbeit mit anderen Behörden;

c) unter ihrer Verantwortung durch Übertragung an andere Behörden;

d) durch Antragstellung bei den zuständigen Justizbehörden.

(2) Bei der Festlegung von Art und Umfang einer nach Artikel 44 verhängten verwaltungsrechtlichen Sanktion oder Abhilfemaßnahme berücksichtigen die zuständigen Behörden, inwieweit der Verstoß vorsätzlich erfolgte oder das Ergebnis von Fahrlässigkeit ist, und 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 diese sich beziffern lassen;

f) die Bereitschaft der verantwortlichen natürlichen oder juristischen Person zur Zusammenarbeit mit der zuständigen Behörde, unbeschadet des Erfordernisses, die von dieser Person erzielten Gewinne oder verhinderten Verluste einzuziehen;

g) frühere Verstöße der verantwortlichen natürlichen oder juristischen Person.

Artikel 46

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 geeignete 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 und im Zusammenhang mit strafrechtlichen Ermittlungen oder Verfahren, die wegen der Verstöße gegen diese Verordnung eingeleitet wurden, spezifische Informationen zu erhalten und diese anderen zuständigen Behörden sowie der EBA, der ESMA und der EIOPA zur Verfügung zu stellen, um ihre Pflichten zur Zusammenarbeit für die Zwecke dieser Verordnung zu erfüllen.

Artikel 47

Mitteilungspflichten

Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA bis zum [*ABl.: Datum ein Jahr nach Inkrafttreten einfügen*] die Rechts- und 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 48

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, keine Rechtsmittel eingelegt werden können.

(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, 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 zu dem Zeitpunkt, zu dem 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 Anwendung der Kronzeugenregelung im Zusammenhang mit der verhängten Sanktion 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 späterem 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 ab dem Zeitpunkt ihrer Veröffentlichung mindestens fünf Jahre lang auf ihrer amtlichen Website zugänglich bleiben. Enthält die Bekanntmachung personenbezogene Daten, so bleiben diese nur so lange auf der offiziellen Website der zuständigen Behörde einsehbar, wie dies nach den geltenden Datenschutzbestimmungen erforderlich ist.

Artikel 49

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 Prüfer und Sachverständigen.

(3) Unter das Berufsgeheimnis fallende Informationen dürfen keiner anderen Person oder Behörde gegenüber offengelegt werden, es sei denn, dies geschieht aufgrund von Unionsrecht oder nationalem Recht.

(4) Alle im Rahmen 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 den zuständigen Behörden zum Zeitpunkt der Mitteilung für zulässig erklärt oder ist für Gerichtsverfahren erforderlich.

KAPITEL VIII

DELEGIERTE RECHTSAKTE

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 gemäß Artikel 28 Absatz 3 und Artikel 38 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem [Amt für Veröffentlichungen: Datum 5 Jahre nach Inkrafttreten dieser Verordnung] übertragen.

(3) Die Befugnisübertragung gemäß Artikel 28 Absatz 3 und Artikel 38 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 delegierter Rechtsakte, 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 28 Absatz 3 und Artikel 38 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. Diese Frist wird auf Initiative des Europäischen Parlaments oder des Rates um zwei Monate verlängert.

KAPITEL IX

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN

ABSCHNITT I

Artikel 51

Überprüfungsklausel

Bis zum [*Amt für Veröffentlichungen: Datum 5 Jahre nach Inkrafttreten dieser Verordnung einfügen*] führt die Kommission nach Konsultation der EBA, der ESMA, der EIOPA und gegebenenfalls des ESRB eine Überprüfung durch und legt dem Europäischen Parlament und dem Rat je nach Sachlage einen Bericht über die Kriterien für die Benennung kritischer IKT-Drittanbieter gemäß Artikel 28 Absatz 2 vor, gegebenenfalls zusammen mit einem Legislativvorschlag.

ABSCHNITT II

ÄNDERUNGEN

Artikel 52

Änderungen der Verordnung (EG) Nr. 1060/2009

In Anhang I der Verordnung (EG) Nr. 1060/2009 erhält Abschnitt A Nummer 4 Unterabsatz 1 folgende Fassung:

„Eine Ratingagentur verfügt über eine solide Verwaltung und Buchhaltung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates* [DORA].

* Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates […] (ABl. L XX, TT.MM.JJJJ, S. X).“

Artikel 53

Änderungen der Verordnung (EU) Nr. 648/2012

Die Verordnung (EU) Nr. 648/2012 wird wie folgt geändert:

1. Artikel 26 wird wie folgt geändert:

   a) Absatz 3 erhält folgende Fassung:

   „(3) Eine CCP muss dauerhaft über eine Organisationsstruktur verfügen, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet. Sie muss angemessene und geeignete Systeme, Ressourcen und Verfahren einsetzen, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates* [DORA] betrieben werden.

   * Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates […](ABl. L XX, TT.MM.JJJJ, S. X).“;

   b) Absatz 6 wird gestrichen;

2. Artikel 34 wird wie folgt geändert:

   a) Absatz 1 erhält folgende Fassung:

   „(1) Eine CCP hat eine angemessene Strategie zur Fortführung des Geschäftsbetriebs sowie einen Notfallwiederherstellungsplan – der IKT-Pläne zur Fortführung des Geschäftsbetriebs und der Notfallwiederherstellung umfasst, die nach der Verordnung (EU) 2021/xx [DORA] eingerichtet werden – festzulegen, umzusetzen und zu befolgen, um eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten der CCP zu gewährleisten.“;

   b) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„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 Strategie zur Fortführung des Geschäftsbetriebs und an den Notfallwiederherstellungsplan, unter Ausschluss von IKT-Plänen zur Fortführung des Geschäftsbetriebs und der Notfallwiederherstellung, festgelegt werden.“;

3. Artikel 56 Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA Entwürfe für technische Regulierungsstandards, in denen die Einzelheiten der Registrierung gemäß Absatz 1, mit Ausnahme der Anforderungen im Zusammenhang mit dem IKT-Risikomanagement, festgelegt werden.“;

4. Artikel 79 Absätze 1 und 2 erhalten folgende Fassung:

„(1) Ein Transaktionsregister ermittelt Quellen operationeller Risiken und minimiert diese Risiken durch die Entwicklung geeigneter Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2021/xx *[DORA*] betrieben werden.

(2) Ein Transaktionsregister hat eine angemessene Strategie für die Fortführung des Geschäftsbetriebs und einen Notfallwiederherstellungsplan – einschließlich IKT-Plänen zur Fortführung des Geschäftsbetriebs und der Notfallwiederherstellung, die nach der Verordnung (EU) 2021/xx *[DORA]* eingerichtet werden – festzulegen, umzusetzen und zu befolgen, die eine Aufrechterhaltung der Funktionen des Transaktionsregisters, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters gewährleisten.“;

5. Artikel 80 Absatz 1 wird gestrichen.

Artikel 54

Änderungen der Verordnung (EU) Nr. 909/2014

Artikel 45 der Verordnung (EU) Nr. 909/2014 wird wie folgt geändert:

1. Absatz 1 erhält folgende Fassung:

„(1) Ein Zentralverwahrer ermittelt Quellen des internen und externen operationellen Risikos und hält deren Auswirkungen durch den Einsatz geeigneter IKT-Instrumente, Kontrollen und Verfahren, die gemäß der Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates* [*DORA*] eingerichtet und verwaltet werden, sowie durch alle anderen relevanten geeigneten Instrumente, Kontrollen und Verfahren für andere Arten operationeller Risiken, auch für alle von ihm betriebenen Wertpapierliefer- und -abrechnungssysteme, so gering wie möglich.

* Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates […](ABl. L XX, TT.MM.JJJJ, S. X).“;

2. Absatz 2 wird gestrichen;

3. Absätze 3 und 4 erhalten folgende Fassung:

„(3) Für die von ihm erbrachten Dienstleistungen und jedes von ihm betriebene Wertpapierliefer- und -abrechnungssystem legt ein Zentralverwahrer eine angemessene Strategie zur Fortführung des Geschäftsbetriebs sowie einen Notfallsanierungsplan, einschließlich IKT-Plänen zur Fortführung des Geschäftsbetriebs und der Notfallsanierung, die gemäß der Verordnung (EU) 2021/xx [DORA] 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 11 in den Absätzen 5 und 7 der Verordnung (EU) 2021/xx [DORA] vorgesehen.“;

4. Absatz 6 Unterabsatz 1 erhält folgende Fassung:

„Ein Zentralverwahrer ermittelt, überwacht und steuert 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 Ersuchen 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:

„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 Strategien zur Fortführung des Geschäftsbetriebs und der Notfallsanierungspläne nach den Absätzen 3 und 4 sowie der Verfahren zu ihrer Beurteilung präzisiert werden.“.

Artikel 55

Änderungen der Verordnung (EU) Nr. 600/2014

Die Verordnung (EU) Nr. 600/2014 wird wie folgt geändert:

1. Artikel 27g wird wie folgt geändert:

   a) Absatz 4 wird gestrichen;

   b) Absatz 8 Buchstabe c erhält folgende Fassung:

   c) „c) die konkreten organisatorischen Anforderungen nach den Absätzen 3 und 5.“;

2. Artikel 27h wird wie folgt geändert:

a) Absatz 5 wird gestrichen;

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 wird gestrichen;

b) Absatz 5 Buchstabe b erhält folgende Fassung:

„b) die konkreten organisatorischen Anforderungen nach den Absätzen 2 und 4.’.

Artikel 56

Inkrafttreten und Anwendung

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

Sie gilt ab dem *[Amt für Veröffentlichungen: Datum einfügen – 12 Monate nach dem Datum des Inkrafttretens*].

Die Artikel 23 und 24 gelten jedoch ab dem [*Amt für Veröffentlichungen*: *Datum einfügen – 36 Monate nach dem Datum des Inkrafttretens dieser Verordnung*].

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

Geschehen zu Brüssel am […]

Für das Europäische Parlament	*Für den Rat*
Der Präsident	*Der Präsident*

FINANZBOGEN ZU RECHTSAKTEN

(1) RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Art des Vorschlags/der Initiative

1.4. Ziel(e)

1.5. Begründung des Vorschlags/der Initiative

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem(e)

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht über die geschätzten Auswirkungen auf die Ausgaben

3.2.2. Geschätzte Auswirkungen auf die Mittel

3.2.3. Geschätzte Auswirkungen auf die Humanressourcen

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

Anhang

Allgemeine Annahmen

Aufsichtsbefugnisse

FINANZBOGEN ZU RECHTSAKTEN – AGENTUREN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die digitale Betriebsstabilität des Finanzsektors.

1.2. Politikbereich(e)

Politikbereich: Finanzstabilität, Finanzdienstleistungen und Kapitalmarktunion

Tätigkeit: Digitale Betriebsstabilität

1.3. Der Vorschlag betrifft

☑ **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[50]

☐ **den Ausbau einer vorhandenen Maßnahme**

☐ **die Zusammenführung einer oder mehrerer Maßnahmen unter Neuausrichtung auf eine andere/neue Maßnahme**

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Das allgemeine Ziel der Initiative besteht darin, die digitale Betriebsstabilität der Unternehmen des Finanzsektors in der EU zu stärken, indem bestehende Vorschriften gestrafft und modernisiert und bei Defiziten neue Anforderungen eingeführt werden. Dies würde auch das einheitliche Regelwerk in seiner digitalen Dimension verbessern.

Das Gesamtziel lässt sich in drei allgemeine Ziele untergliedern: 1) Verringerung des Risikos finanzieller Störungen und Instabilität, 2) Verringerung des Verwaltungsaufwands und Steigerung der aufsichtlichen Effizienz sowie 3) Erhöhung des Verbraucher- und Anlegerschutzes.

1.4.2. Einzelziele:

Die Einzelziele des Vorschlags sind:

Risiken im Bereich der Informations- und Kommunikationstechnologien (IKT) umfassender anzugehen und das allgemeine Niveau der digitalen Betriebsstabilität des Finanzsektors zu stärken;

Meldungen IKT-bezogener Vorfälle zu straffen und sich überschneidende Meldepflichten zu beseitigen;

Finanzaufsichtsbehörden Zugriff auf Informationen über IKT-bezogene Vorfälle zu ermöglichen;

[50] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

sicherstellen, dass die von diesem Vorschlag erfassten Finanzunternehmen die Wirksamkeit ihrer Präventions- und Gegenmaßnahmen bewerten und IKT-bezogene Anfälligkeiten ermitteln; die Fragmentierung des Binnenmarkts zu verringern und die grenzüberschreitende Anerkennung von Prüfungsergebnissen zu ermöglichen. die vertraglichen Schutzvorkehrungen für Finanzunternehmen bei der Nutzung von IKT-Diensten zu stärken, einschließlich der Vorschriften für Auslagerung (für die Überwachung von IKT-Drittanbietern); eine Aufsicht über die Tätigkeiten kritischer IKT-Drittanbieter einzurichten; Anreize für den Austausch von Informationen über Bedrohungen im Finanzsektor zu schaffen.

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Ein Rechtsakt für die digitale Betriebsstabilität des Finanzsektors würde einen umfassenden Rahmen gewährleisten, der alle Aspekte der digitalen Betriebsstabilität abdeckt, und zur Verbesserung der allgemeinen Betriebsstabilität des Finanzsektors beitragen. Außerdem würden durch einen solchen Rechtsakt die Klarheit und Kohärenz innerhalb des einheitlichen Regelwerks bewahrt.

Auch würde hierdurch die Wechselbeziehung zur NIS-Richtlinie und ihrer Überarbeitung klarer und kohärenter. Finanzunternehmen erhielten Klarheit über die unterschiedlichen Vorschriften für die digitale Betriebsstabilität, die sie einhalten müssen, darunter insbesondere Finanzunternehmen, die über mehrere Zulassungen verfügen und auf verschiedenen Märkten innerhalb der EU operieren.

1.4.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Potenzielle Indikatoren:

Zahl der IKT-bezogenen Vorfälle im EU-Finanzsektor und ihre Auswirkungen

Zahl schwerwiegender IKT-bezogener Vorfälle, die den Aufsichtsbehörden gemeldet wurden

Zahl der Finanzunternehmen, die zur Durchführung bedrohungsorientierter Penetrationstests („TLPT“) verpflichtet wären

Zahl der Finanzunternehmen, die Standardvertragsklauseln für den Abschluss vertraglicher Vereinbarungen mit IKT-Drittanbietern verwenden

Zahl kritischer IKT-Drittanbieter, die von den ESA/Aufsichtsbehörden beaufsichtigt werden

Zahl der Finanzunternehmen, die am Austausch von Informationen über Bedrohungen teilnehmen

Zahl der Behörden, die Meldungen über denselben IKT-bezogenen Vorfall erhalten

Zahl grenzüberschreitender TLPT

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Umsetzung der Initiative

Der Finanzsektor stützt sich in hohem Maße auf Informations- und Kommunikationstechnologien (IKT). Trotz der erheblichen Fortschritte, die durch gezielte politische und legislative Initiativen auf nationaler und europäischer Ebene erzielt wurden, stellen IKT-Risiken nach wie vor eine Herausforderung für die Betriebsstabilität, die Leistungsfähigkeit und die Stabilität des Finanzsystems der EU dar. Mit der Reform, die auf die Finanzkrise von 2008 folgte, wurde in erster Linie die finanzielle Resilienz des EU-Finanzsektors gestärkt und darauf abgezielt, die Wettbewerbsfähigkeit und Stabilität der EU aus wirtschaftlichen, aufsichtsrechtlichen und marktpolitischen Perspektiven zu wahren. Die IKT-Sicherheit und die allgemeine digitale Betriebsstabilität sind Teil des operationellen Risikos, stehen aber weniger im Fokus der Regulierungsagenda für die Zeit nach der Krise und haben sich nur in bestimmten Bereichen der EU-Finanzmarktpolitik und -regulierung

bzw. nur in einigen wenigen Mitgliedstaaten weiterentwickelt. Dies mündet in folgende Herausforderungen, die mit dem Vorschlag angegangen werden sollten:

Der EU-Rechtsrahmen für IKT-Risiken und Betriebsstabilität im Finanzsektor ist fragmentiert und nicht völlig konsistent.

Das Fehlen einheitlicher Meldepflichten für IKT-bezogene Vorfälle führt dazu, dass die Aufsichtsbehörden einen unvollständigen Überblick über Art, Häufigkeit, Bedeutung und Auswirkungen von Vorfällen erlangen.

Bestimmte Finanzunternehmen sind mit komplexen, sich überschneidenden und möglicherweise uneinheitlichen Meldepflichten für denselben IKT-bezogenen Vorfall konfrontiert.

Unzureichender Informationsaustausch und unzureichende Zusammenarbeit im Bereich der Informationen über Cyberbedrohungen auf strategischer, taktischer und operativer Ebene hindern einzelne Finanzunternehmen daran, Cyberbedrohungen angemessen zu bewerten, zu überwachen, sich dagegen zu verteidigen und Gegenmaßnahmen zu ergreifen.

In bestimmten Teilsektoren des Finanzsektors gibt es möglicherweise mehrere und unkoordinierte Rahmen für Penetrations- und Stabilitätstests in Kombination mit der fehlenden grenzübergreifenden Anerkennung von Ergebnissen, während in anderen Teilsektoren solche Testrahmen fehlen.

Der unzureichende Einblick von Aufsichtsbehörden in die Tätigkeiten von Finanzunternehmen, die von IKT-Drittanbietern übernommen werden, führt dazu, dass Finanzunternehmen einzeln und das Finanzsystem insgesamt operationellen Risiken ausgesetzt sind.

Finanzaufsichtsbehörden verfügen weder über ein ausreichendes Mandat noch über Instrumente für die Überwachung und Steuerung der Konzentrations- und Systemrisiken, die sich aus der Abhängigkeit von Finanzunternehmen von IKT-Drittanbietern ergeben.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größere Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer entspricht der „Mehrwert aufgrund des Tätigwerdens der Union“ dem Wert, der sich aus dem Tätigwerden der Union ergibt und zu dem Wert hinzukommt, der andernfalls allein von Mitgliedstaaten geschaffen worden wäre.

Gründe für Maßnahmen auf europäischer Ebene (ex ante):

Die digitale Betriebsstabilität ist ein Thema von gemeinsamem Interesse für die Finanzmärkte der EU. Maßnahmen auf EU-Ebene würden mehr Vorteile und Nutzen bringen als Einzelmaßnahmen auf nationaler Ebene. Ohne diese operativen Bestimmungen zum IKT-Risiko würde das einheitliche Regelwerk zwar die Instrumente zur Bewältigung aller anderen Arten von Risiken auf europäischer Ebene bereitstellen, die Aspekte der digitalen Betriebsstabilität jedoch ausschließen oder fragmentierten und unkoordinierten Initiativen auf nationaler Ebene unterwerfen. Der Vorschlag würde Rechtsklarheit darüber schaffen, ob und wie Vorschriften für digitale Resilienz insbesondere für grenzüberschreitend tätige Finanzinstitute gelten, und es bestünde dann keine Notwendigkeit für die Mitgliedstaaten mehr, als Reaktion auf den derzeit begrenzten Geltungsbereich der EU-Vorschriften und den allgemeinen Charakter der NIS-Richtlinie Vorschriften, Standards und Vorgaben in Bezug auf Betriebsstabilität und Cybersicherheit im Alleingang zu verbessern.

Erwarteter EU-Mehrwert (ex post):

Das Tätigwerden der Union würde die Wirksamkeit der Politik erheblich steigern und gleichzeitig die Komplexität verringern und den finanziellen und administrativen Aufwand für alle Finanzunternehmen verringern. Hierdurch würde ein so eng vernetzter und integrierter Bereich der Wirtschaft, der bereits von einem einheitlichen Regelwerk und einer einheitlichen Aufsicht profitiert, harmonisiert. In Bezug auf die Meldung IKT-bezogener Vorfälle würde der Vorschlag den Meldeaufwand – und die impliziten Kosten – verringern, die anfallen, wenn ein und derselbe IKT-bezogene Vorfall verschiedenen EU- und/oder nationalen Behörden gemeldet wird. Ebenso würde durch ihn die gegenseitige Anerkennung/Akzeptanz der Prüfungsergebnisse von grenzüberschreitend tätigen Unternehmen erleichtert, die in verschiedenen Mitgliedstaaten mehreren Prüfungsrahmen unterliegen.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Neue Initiative

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Das Ziel dieses Vorschlags steht im Einklang mit einer Reihe anderer politischer Maßnahmen der EU und laufenden Initiativen, insbesondere der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) und der Richtlinie über europäische kritische Infrastrukturen (EKI). Mit dem Vorschlag blieben die Vorteile des horizontalen Rahmens für Cybersicherheit erhalten, da die drei Finanzteilsektoren weiterhin in den Anwendungsbereich der NIS-Richtlinie fallen würden. Wenn die Finanzaufsichtsbehörden mit dem NIS-Ökosystem assoziiert bleiben, könnten sie einschlägige Informationen mit den NIS-Behörden austauschen und sich an der NIS-Kooperationsgruppe beteiligen. Der Vorschlag würde sich nicht auf die NIS-Richtlinie auswirken, sondern vielmehr darauf aufbauen und mögliche Überschneidungen durch eine Ausnahme mittels einer Lex specialis beseitigen. Die Wechselbeziehung zwischen der Verordnung über Finanzdienstleistungen und der NIS-Richtlinie würde weiterhin durch eine „Lex specialis"-Klausel geregelt, wodurch Finanzunternehmen von wesentlichen Anforderungen der NIS-Richtlinie ausgenommen wären und Überschneidungen zwischen den beiden Rechtsakten vermieden würden. Darüber hinaus steht der Vorschlag im Einklang mit der Richtlinie über europäische kritische Infrastrukturen (EKI), die derzeit überarbeitet wird, um den Schutz und die Widerstandsfähigkeit kritischer Infrastrukturen gegenüber Nicht-Cyberbedrohungen zu verbessern.

Dieser Vorschlag hätte keine Auswirkungen auf den mehrjährigen Finanzrahmen (MFR). Zunächst wird der Aufsichtsrahmen für kritische IKT-Drittanbieter vollständig durch Gebühren finanziert, die von diesen Anbietern erhoben werden; zweitens werden die zusätzlichen Regulierungsaufgaben im Zusammenhang mit digitaler Betriebsstabilität, die den ESA übertragen werden, durch interne Personalumbesetzungen sichergestellt.

Dies wird in einen Vorschlag zur Aufstockung des bewilligten Personals der Agentur im Rahmen des künftigen jährlichen Haushaltsverfahrens münden. Die Agentur wird weiterhin darauf hinarbeiten, Synergien und Effizienzgewinne zu maximieren (u. a. durch IT-Systeme), und die zusätzliche Arbeitsbelastung im Zusammenhang mit diesem Vorschlag genau überwachen, was sich in der Zahl der von der Agentur im Rahmen des jährlichen Haushaltsverfahrens beantragten bewilligten Mitarbeiter niederschlagen würde.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Es wurden mehrere Finanzierungsoptionen in Betracht gezogen:

Zunächst könnten die zusätzlichen Kosten über den üblichen Finanzierungsmechanismus der ESA finanziert werden. Dies würde jedoch zu einer erheblichen Erhöhung des Beitrags der EU zu den finanziellen Ressourcen der ESA führen.

Diese Option wird für die Kosten gewählt, die mit den Regulierungsaufgaben in Verbindung mit diesem Vorschlag zusammenhängen. Die ESA werden aufgefordert, vorhandenes Personal umzubesetzen, um eine Reihe technischer Standards zu entwickeln. Gleichwohl könnten die zusätzlichen Kosten im Zusammenhang mit der Aufsicht über kritische Drittanbieter nicht durch eine Umschichtung von Ressourcen innerhalb der ESA gedeckt werden, die neben den in diesem Vorschlag und anderen Rechtsvorschriften der Union vorgesehenen Aufgaben noch weitere Aufgaben wahrnehmen. Darüber hinaus erfordern Aufsichtsaufgaben im Zusammenhang mit digitaler Betriebsstabilität besondere technische Fachkenntnisse und Erfahrung. Da der derzeitige Umfang dieser Ressourcen bei den ESA unzureichend ist, sind zusätzliche Ressourcen erforderlich.

Schließlich werden dem Vorschlag zufolge von den kritischen Drittanbietern, die der Aufsicht unterliegen, Gebühren erhoben. Mit diesen Mitteln sollen alle zusätzlichen Ressourcen gedeckt werden, die die ESA für die Wahrnehmung ihrer neuen Aufgaben und Befugnisse benötigen.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

☐ Vorschlag/Initiative gilt von [TT/MM]JJJJ bis [TT/MM]JJJJ

☐ Finanzielle Auswirkungen von JJJJ bis JJJJ

☑ **unbefristete Laufzeit**

Umsetzung mit einer Anlaufphase ab 2021

anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[51]

Direkte Verwaltung durch die Kommission durch

☐ Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☑ **Indirekte Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

☐ internationale Einrichtungen und deren Agenturen (bitte angeben);

☐die EIB und den Europäischen Investitionsfonds;

☑ Einrichtungen im Sinne der Artikel 70 und 71;

☐ öffentlich-rechtliche Körperschaften;

☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten;

☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende finanzielle Garantien bieten;

☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und im maßgeblichen Basisrechtsakt benannt sind.

Anmerkungen

Entfällt.

[51] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Die ESA berichten im Einklang mit bestehenden Vereinbarungen regelmäßig über ihre Tätigkeiten (u. a. interne Berichterstattung an die Geschäftsleitung, Berichterstattung an den Rat der Aufseher und das Direktorium und Erstellung von Jahresberichten), und ihr Ressourceneinsatz und ihre Leistung unterliegen Audits durch den Rechnungshof und den Internen Auditdienst der Kommission. Das Monitoring und die Berichterstattung bezüglich der im Vorschlag enthaltenen Maßnahmen werden die bereits bestehenden sowie alle neuen Anforderungen erfüllen, die sich aus diesem Vorschlag ergeben.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

Die Verwaltung erfolgt indirekt über die ESA. Der Finanzierungsmechanismus würde durch Gebühren umgesetzt, die von den betroffenen kritischen IKT-Drittanbietern erhoben werden.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Was die rechtlichen und wirtschaftlichen Risiken sowie den effizienten und effektiven Einsatz der Mittel anbelangt, wird davon ausgegangen, dass die vorgeschlagene Verordnung keine wesentlichen neuen Risiken birgt, die nicht schon im bestehenden Rahmen für die interne Kontrolle abgedeckt wären. Eine neue Herausforderung könnte jedoch darin bestehen, die rechtzeitige Erhebung von Gebühren bei den betroffenen kritischen IKT-Drittanbietern sicherzustellen.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Die in den ESA-Verordnungen vorgesehenen Verwaltungs- und Kontrollsysteme sind bereits umgesetzt. Um zu gewährleisten, dass in allen Bereichen des Rahmens für die interne Kontrolle angemessene Standards erreicht werden, arbeiten die ESA eng mit dem Internen Auditdienst der Kommission zusammen. Diese Vereinbarungen werden auch im Hinblick auf die Rolle der ESA gemäß dem vorliegenden Vorschlag gelten. In jedem Haushaltsjahr erteilt das Europäische Parlament jeder ESA auf Empfehlung des Rates Entlastung zur Ausführung ihres Haushaltsplans.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen wird die Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) ohne Einschränkung auf die ESA angewandt.

Die ESA verfügen über eine eigene Strategie zur Betrugsbekämpfung und einen entsprechenden Aktionsplan. Die verschärften Maßnahmen der ESA im Bereich der Betrugsbekämpfung werden mit den Vorschriften und Leitlinien im Einklang stehen, die von der Haushaltsordnung (Betrugsbekämpfungsmaßnahmen als Teil der wirtschaftlichen Haushaltsführung), der Betrugsbekämpfungspolitik des OLAF, den Bestimmungen der Betrugsbekämpfungsstrategie der Kommission (KOM(2011)376) sowie dem Gemeinsamen Konzept für die dezentralen Agenturen der EU (Juli 2012) und dem damit verbundenen Fahrplan vorgegeben werden.

Die Verordnungen zur Errichtung der ESA sowie die Haushaltsordnungen der ESA enthalten die Bestimmungen über die Ausführung und Kontrolle der Haushaltspläne und die geltenden Finanzregelungen der ESA, einschließlich derer zur Prävention von Betrug und Unregelmäßigkeiten.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Type of Ausgaben	Beitrag			
	Anzahl	GM/NGM [52]	von EFTA-Ländern [53]	von Kandidatenländern [54]	von Drittstaaten	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung

Neu zu schaffende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Type of Ausgaben	Beitrag			
	Anzahl	GM/NGM	von EFTA-	von Kandidaten	von Drittstaat	nach Artikel 21 Absatz 2 Buchstabe b der

[52] GM = Getrennte Mittel/NGM = Nicht getrennte Mittel.

[53] EFTA: Europäische Freihandelsassoziation.

[54] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

			Ländern	ländern	en	Haushaltsordnung

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.3. Übersicht über die geschätzten Auswirkungen auf die Ausgaben

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	Anzahl	Rubrik

GD: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**INSGE-SAMT**
	Mittelbindungen	(1)									
	Zahlungen	(2)									
Mittelausstattung INSGESAMT für GD <>	Mittelbindungen										
	Zahlungen										

Rubrik des mehrjährigen Finanzrahmens		

in Mio. EUR (3 Dezimalstellen)

		2022	2023	2024	2025	2026	2027	INSGE-SAMT
Generaldirektionen:								
• Personalausgaben								
• Sonstige Verwaltungsausgaben <>								
INSGESAMT GD	Mittel							

Mittelausstattung INSGESAMT unter RUBRIK des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)							

in Mio. EUR (3 Dezimalstellen) in konstanten Preisen

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**INSGE-SAMT**
Mittelausstattung INSGESAMT unter RUBRIKEN 1 des mehrjährigen Finanzrahmens	Mittelbindungen							
	Zahlungen							

3.3.1. Geschätzte Auswirkungen auf die Mittel

☑ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt

☐ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen) in konstanten Preisen

Ziele und Ergebnisse angeben ⇩			2022		2023		2024		2025		2026		2027		**INSGESAMT**	
	ERGEBNISSE															
	Art[55]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	An-zahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[56] …																
- Ergebnis																
Zwischensumme für Einzelziel Nr. 1																
EINZELZIEL Nr. 2 …																
- Ergebnis																
Zwischensumme für Einzelziel Nr. 2																
GESAMTKOSTEN																

[55] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[56] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

3.3.2. Geschätzte Auswirkungen auf die Humanressourcen

3.3.2.1. Zusammenfassung

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

☑ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen) in konstanten Preisen

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**INSGE-SAMT**
Bedienstete auf Zeit (AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Bedienstete auf Zeit (Funktionsgruppe AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Vertragsbedienstete							
Abgeordnete nationale Sachverständige							
INSGESAMT	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personalbedarf (VZÄ):

EBA, EIOPA, ESMA & EUA	2022	2023	2024	2025	2026	2027	**INSGE-SAMT**
Bedienstete auf Zeit (AD) EBA = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Bedienstete auf Zeit (Funktionsgruppe AST) EBA=1, EIOPA=1, ESMA=1	3	3	3	3	3	3	3
Vertragsbedienstete							
Abgeordnete nationale Sachverständige							

INSGESAMT	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Geschätzter Personalbedarf bei den (übergeordneten) GD

☑ Für den Vorschlag/die Initiative wird kein Personal benötigt.

☐ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

		2022	2023	2024	2025	2026	2027
• **Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)**							
• **Externes Personal (in Vollzeitäquivalenten: VZÄ)**[57]							
XX 01 02 01 (VB, ANS und LAK der Globaldotation)							
XX 01 02 02 (VB, ÖB, ANS, LAK und JFD in den Delegationen)							
XX 01 04 **yy**[58]	- am Sitz der Kommission[59]						
	- in den Delegationen						
XX 01 05 02 (VB, ANS und LAK der indirekten Forschung)							
10 01 05 02 (VB, ANS und LAK der direkten Forschung)							
Sonstige Haushaltslinien (bitte angeben)							
INSGESAMT							

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel für Personal, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	
Externes Personal	

Einzelheiten der Kostenberechnung für die VZÄ sind im Anhang V Abschnitt 3 anzugeben.

[57] VB = Vertragsbedienstete; ÖB = Örtliche Bedienstete; ANS = Abgeordnete nationale Sachverständige; LAK = Leiharbeitskräfte; JFD = Juniorfachkräfte in Delegationen.

[58] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

[59] Hauptsächlich für die Strukturfonds, den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und den Europäischen Fischereifonds (EFF).

3.3.3. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

☑ Der Vorschlag/Die Initiative ist mit dem mehrjährigen Finanzrahmen vereinbar.

☐ Der Vorschlag/Die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

☐ Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens.[60]

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge. […]

3.3.4. Finanzierungsbeteiligung Dritter

☐ Der Vorschlag/Die Initiative sieht keine Kofinanzierung durch Dritte vor.

☑ Der Vorschlag/Die Initiative sieht folgende Kofinanzierung vor:

in Mio. EUR (3 Dezimalstellen)

EBA

	2022	2023	2024	2025	2026	2027	Insge-samt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Unternehmen erhoben werden.[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kofinanzierung INSGESAMT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Insges-amt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Unternehmen erhoben werden.[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Kofinanzierung INSGESAMT	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Siehe Artikel 11 und 17 der Verordnung (EU, Euratom) Nr. 1311/2013 des Rates zur Festlegung des mehrjährigen Finanzrahmens für die Jahre 2014–2020.

61 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung

62 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung

	2022	2023	2024	2025	2026	2027	Insge-samt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Unternehmen erhoben werden.[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kofinanzierung INSGESAMT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Geschätzte Auswirkungen auf die Einnahmen

☑ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen

☐ Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushalts-jahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[64]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel …….								

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

[…]

Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

[…]

63 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung

64 Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten anzugeben.

ANHANG

Allgemeine Annahmen

Titel I – Personalausgaben

Bei der Berechnung der Personalausgaben wurden auf der Grundlage des nachstehend erläuterten Personalbedarfs folgende spezifische Annahmen zugrunde gelegt:

- Die Kosten für das 2022 eingestellte zusätzliche Personal werden angesichts der für die Einstellung des zusätzlichen Personals veranschlagten Zeit für 6 Monate veranschlagt.
- Die durchschnittlichen jährlichen Kosten eines Bediensteten auf Zeit belaufen sich auf 150 000 EUR, einschließlich 25 000 EUR an Ausstattungskosten (Gebäude, IT usw.).
- Die Berichtigungskoeffizienten für die Dienstbezüge des Personals in Paris (EBA und ESMA) und Frankfurt (EIOPA) belaufen sich auf 117,7 bzw. 99,4.
- Die Arbeitgeberbeiträge zur Altersversorgung für Bedienstete auf Zeit basieren auf den in den normalen Jahresdurchschnittskosten enthaltenen Grundgehältern, d. h. 95 660 EUR.
- Bei den zusätzlichen Bediensteten auf Zeit handelt es sich um AD5- und AST-Bedienstete.

Titel II – Infrastruktur- und Betriebsausgaben

Die Kosten ergeben sich aus der Multiplikation der Mitarbeiterzahl mit dem Anteil des Jahres der Beschäftigung mit den Standardkosten für Ausstattungen, d. h. 25 000 EUR.

Titel III – Operative Ausgaben

Die Schätzung der Kosten beruht auf den folgenden Annahmen:

- Die Übersetzungskosten werden für jede ESA auf 350 000 EUR pro Jahr festgesetzt.
- Es wird davon ausgegangen, dass die einmaligen IT-Kosten in Höhe von 500 000 EUR pro ESA in den beiden Jahren 2022 und 2023 auf Basis einer 50-50-Aufteilung getragen werden. Die jährlichen Instandhaltungskosten ab 2024 werden auf 50 000 EUR pro ESA geschätzt.
- Die jährlichen Kosten für die Beaufsichtigung vor Ort werden auf 200 000 EUR pro ESA geschätzt.

Die hier dargelegten Schätzungen führen zu folgenden Kosten pro Jahr:

Rubrik des mehrjährigen Finanzrahmens	Anzahl	

Konstante Preise

EBA:			2022	2023	2024	2025	2026	2027	INSGESAMT
Titel 1:	Mittelbindungen	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Zahlungen	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titel 2:	Mittelbindungen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Zahlungen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Mittelbindungen	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Zahlungen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Mittelausstattung INSGESAMT für EBA	Mittelbindungen	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Zahlungen	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	INSGESAMT
Titel 1:	Mittelbindungen	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Zahlungen	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Titel 2:	Mittelbindungen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Zahlungen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Mittelbindungen	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Zahlungen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

Mittelausstattung INSGESAMT für EIOPA	Mittelbindungen	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Zahlungen	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**INSGESAMT**
Titel 1:	Mittelbindungen	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Zahlungen	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titel 2:	Mittelbindungen	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Zahlungen	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titel 3:	Mittelbindungen	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Zahlungen	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Mittelausstattung INSGESAMT für ESMA	Mittelbindungen	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Zahlungen	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Für den Vorschlag werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen) in konstanten Preisen

EBA

Ziele und Ergebnisse angeben ⇩			2022		2023		2024		2025		2026		2027			
	ERGEBNISSE															
	Art[65]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[66] Direkte Aufsicht über kritische IKT-Drittanbieter																
- Ergebnis				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Zwischensumme für Einzelziel Nr. 1																
EINZELZIEL Nr. 2 …																
- Ergebnis																
Zwischensumme für Einzelziel Nr. 2																
GESAMTKOSTEN				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Ziele und Ergebnisse angeben ⇩			2022		2023		2024		2025		2026		2027			
	ERGEBNISSE															
	Art[67]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[68] Direkte Aufsicht über kritische IKT-Drittanbieter																
- Ergebnis				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[66] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

[67] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[68] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Zwischensumme für Einzelziel Nr. 1														
EINZELZIEL Nr. 2 …														
- Ergebnis														
Zwischensumme für Einzelziel Nr. 2														
GESAMTKOSTEN		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Ziele und Ergebnisse angeben			2022		2023		2024		2025		2026		2027			
	ERGEBNISSE															
⇩	Art[69]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[70] Direkte Aufsicht über kritische IKT-Drittanbieter																
- Ergebnis				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Zwischensumme für Einzelziel Nr. 1																
EINZELZIEL Nr. 2 …																
- Ergebnis																
Zwischensumme für Einzelziel Nr. 2																
GESAMTKOSTEN				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[70] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

Die Aufsichtstätigkeiten werden vollständig durch Gebühren finanziert, die von den beaufsichtigten Stellen wie folgt erhoben werden:

EBA

	2022	2023	2024	2025	2026	2027	Insge-samt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Stellen erhoben werden.[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kofinanzierung INSGESAMT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Insge-samt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Stellen erhoben werden.[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Kofinanzierung INSGESAMT	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Insge-samt
Die Kosten werden zu 100 % durch Gebühren gedeckt, die von den beaufsichtigten Stellen erhoben werden.[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kofinanzierung INSGESAMT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPEZIFISCHE INFORMATIONEN

Direkte Aufsichtsbefugnisse

[71] 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung
[72] 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung
[73] 100 % der geschätzten Gesamtkosten zuzüglich der vollen Arbeitgeberbeiträge zur Altersversorgung

Einleitend sei daran erinnert, dass Unternehmen, die der direkten Beaufsichtigung durch die ESMA unterliegen, der ESMA Gebühren zahlen sollten (einmalige Registrierungskosten und wiederkehrende Kosten für die laufende Beaufsichtigung). Dies gilt für Ratingagenturen (siehe die Delegierte Verordnung (EU) Nr. 272/2012 der Kommission) und Transaktionsregister (Delegierte Verordnung (EU) Nr. 1003/2013 der Kommission).

Im Rahmen dieses Legislativvorschlags werden die ESA mit neuen Aufgaben betraut, die darauf abzielen, die Konvergenz der Aufsichtskonzepte in Bezug auf das Risiko durch IKT-Drittanbieter im Finanzsektor zu fördern, indem kritische IKT-Drittanbieter einem Aufsichtsrahmen der Union unterworfen werden.

Der in diesem Vorschlag vorgesehene Aufsichtsrahmen baut auf der bestehenden institutionellen Architektur im Bereich der Finanzdienstleistungen auf, wobei der Gemeinsame Ausschuss der ESA im Einklang mit seinen Aufgaben im Bereich der Cybersicherheit für eine sektorübergreifende Koordinierung aller IKT-Risiken sorgt, die von dem zuständigen Unterausschuss (Aufsichtsforum) unterstützt wird, der vorbereitende Arbeiten für Einzelentscheidungen und gemeinsame Empfehlungen für kritische IKT-Drittanbieter durchführt.

Durch diesen Rahmen erhalten die ESA, die für jeden kritischen IKT-Drittanbieter als federführende Aufsichtsinstanz benannt wurden, Befugnisse, um sicherzustellen, dass Technologieanbieter, die eine entscheidende Rolle für das Funktionieren des Finanzsektors wahrnehmen, europaweit angemessen überwacht werden. Die Aufsichtspflichten sind in dem Vorschlag dargelegt und in der Begründung näher erläutert. Sie umfassen Rechte, um alle einschlägigen Informationen und Unterlagen zur Durchführung allgemeiner Ermittlungen und Inspektionen anzufordern, Empfehlungen abzugeben und im Folgenden Berichte zu den ergriffenen Maßnahmen oder den Abhilfemaßnahmen vorzulegen, die zur Abgabe dieser Empfehlungen umgesetzt wurden.

Daher wird zur Wahrnehmung der in diesem Vorschlag vorgesehenen neuen Aufgaben von den ESA zusätzliches Personal eingestellt, das auf IKT-Risiken spezialisiert ist und sich auf die Bewertung der Abhängigkeiten von Drittanbietern konzentriert.

Der Personalbedarf kann auf 6 VZÄ pro Behörde geschätzt werden (5 AD und 1 AST zur Unterstützung der AD). Den ESA entstehen außerdem zusätzliche IT-Kosten, die auf 500 000 EUR (einmalige Kosten) und jährlich 50 000 EUR an Wartungskosten für jede der drei ESA geschätzt werden. Ein wichtiger Aspekt bei der Erfüllung der neuen Aufgaben sind die Inspektionen und Prüfungen vor Ort, die auf jährlich 200 000 EUR pro ESA geschätzt werden können. Kosten für die Übersetzungen verschiedener Dokumente, die die ESA von den kritischen IKT-Drittanbietern erhalten würden, sind ebenfalls in der Zeile zu den Betriebskosten enthalten und belaufen sich auf 350 000 EUR pro Jahr.

Alle oben genannten Verwaltungskosten werden vollständig aus den jährlichen Gebühren finanziert, die die ESA von den überwachten kritischen IKT-Drittanbietern erheben (keine Auswirkungen auf den EU-Haushalt).