Rat der
Europäischen Union

Brüssel, den 22. Januar 2026
(OR. en)

5627/26

Interinstitutionelles Dossier:
2026/0012 (COD)

CYBER 30
JAI 91
DATAPROTECT 23
TELECOM 30
MI 59
IND 50
CADREFIN 27
FIN 104
BUDGET 4
CODEC 93

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	21. Januar 2026
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2026) 13 final
Betr.:	Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2]

Die Delegationen erhalten als Anlage das Dokument COM(2026) 13 final.

Anl.: COM(2026) 13 final

EUROPÄISCHE
KOMMISSION

Straßburg, den 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Dieser Vorschlag ist Teil eines Maßnahmenpakets, mit dem der Cybersicherheitsrahmen der Union an die Bedürfnisse der Interessenträger in einer zunehmend ausgeklügelten Cyberbedrohungslandschaft und einer komplexen geopolitischen Realität angepasst werden soll. Wesentliche und wichtige Einrichtungen aus kritischen Sektoren sind zunehmend Ziel von Cyberangriffen[1], während staatliche Bedrohungsakteure neue Technologien wie künstliche Intelligenz (KI) nutzen, um ihre Angriffe auszuweiten und zu optimieren. In diesem Zusammenhang wird die Resilienz kritischer Infrastrukturen gegenüber Cyberbedrohungen als strategische Säule unserer Demokratien und der wirtschaftlichen Sicherheit der Union anerkannt. Sowohl durch die Europäische Strategie für eine Union der Krisenvorsorge[2] als auch die Europäische Strategie für die innere Sicherheit (ProtectEU)[3] ist die Cybersicherheit in den Mittelpunkt der Resilienzagenda der Union gerückt. Ebenso werden in der Mitteilung über die Stärkung der wirtschaftlichen Sicherheit der EU[4] die Verhinderung des Zugangs zu sensiblen Informationen und Daten, die die wirtschaftliche Sicherheit der Union aushöhlen könnten, und die Verhinderung und Entschärfung von Störungen kritischer Infrastrukturen der Union, die die Wirtschaft der Union beeinträchtigen, als vorrangige Ziele genannt, bei denen wirksame Cybersicherheitsmaßnahmen eine entscheidende Rolle spielen. Darüber hinaus wurde im Draghi-Bericht hervorgehoben, dass die Sicherheit erhöht und Abhängigkeiten verringert werden müssen[5], da dies einer der wichtigsten Aktionsbereiche in der Union ist. In ihrer Mitteilung „Ein einfacheres und schnelleres Europa“[6] kündigte die Kommission ihr Engagement für ein ehrgeiziges Programm zur Förderung zukunftsorientierter, innovativer Strategien an, die die Wettbewerbsfähigkeit der Union stärken, den Regelungsaufwand für die Menschen, Unternehmen und Verwaltungen verringern und höchste Standards bei der Förderung ihrer Werte wahren sollen.

Vor diesem Hintergrund zielt der vorliegende Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferkette sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)] darauf ab, das Problem der Komplexität und Vielfalt der Cybersicherheitsstrategien anzugehen, die sich auf die Cyberabwehr der Union auswirken, insbesondere durch Klarstellungen und die Erleichterung der Einhaltung für beaufsichtigte Unternehmen.

Das Ziel der vorliegenden Richtlinie sollte als Teil der übergeordneten Ziele des Pakets zur Überarbeitung des derzeitigen Rechtsakts zur Cybersicherheit betrachtet werden, das den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferkette sowie zur Aufhebung

---

1 ENISA, ENISA Threat Landscape 2025.
2 JOIN(2025) 130 final.
3 COM(2025) 148 final.
4 JOIN(2025) 977 final.
5 Europäische Kommission, „Die Zukunft der europäischen Wettbewerbsfähigkeit“, (https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_de).
6 COM(2025) 47 final.

der Verordnung (EU) 2019/881 umfasst. Mit dem Vorschlag für diese Verordnung soll Folgendes angegangen werden: i) die Diskrepanz zwischen dem politischen Rahmen der Union für die Cybersicherheit und den Bedürfnissen der Interessenträger in einer zunehmend feindseligen Bedrohungslage, ii) die ins Stocken geratene Umsetzung des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF), iii) die Komplexität und Vielfalt der Cybersicherheitsstrategien, die sich auf die Cyberabwehr der Union auswirken, und iv) die Erhöhung der Sicherheitsrisiken in den IKT-Lieferketten. In Bezug auf die Komplexität und Vielfalt der Cybersicherheitsstrategien, die sich auf die Cyberabwehr der Union auswirken, wird im Paket zur Überarbeitung des derzeitigen Rechtsakts zur Cybersicherheit – als Teil einer Reform des europäischen Rahmens für die Cybersicherheitszertifizierung – vorgeschlagen, die Zertifizierung als Einhaltungsinstrument für Unternehmen zu fördern und die Entwicklung eines Systems für die Cyberabwehr von Einrichtungen zu ermöglichen, um die Befolgungskosten für Einrichtungen, die der NIS-2-Richtlinie und anderen einschlägigen Cybersicherheitsvorschriften der Union unterliegen, zu senken. Dieser Ansatz wird die regulatorischen Verpflichtungen für Einrichtungen, die mehreren Einhaltungsanforderungen unterliegen, erheblich vereinfachen und eine wirksamere Nutzung der Ressourcen durch die nationalen Behörden gewährleisten.

In der Begründung des Vorschlags für eine Cybersicherheitsverordnung 2 werden die wichtigsten Fragen, die dem Vorschlag zugrunde liegen, sowie die spezifischen Ziele dargelegt, die angegangen werden sollen. Der Vorschlag für eine Richtlinie wird sich mit dem spezifischen Ziel Nr. 4 der Folgenabschätzung zur Überarbeitung des derzeitigen Rechtsakts zur Cybersicherheit befassen, d. h. der Festlegung von Mechanismen und Bedingungen, die dazu beitragen, die Einhaltung der Cybersicherheitsanforderungen zu erleichtern und auf diese Weise ihre Umsetzung kohärenter und wirksamer zu gestalten. Gezielte Änderungen der NIS-2-Richtlinie zielen darauf ab, die Einhaltung bestimmter Aspekte des Cybersicherheitsrahmens zu vereinfachen und eine gestraffte und kohärente Umsetzung zu gewährleisten, auch in Bezug auf den Anwendungsbereich, die Begriffsbestimmungen, die Meldung von Ransomware-Angriffen und die Beaufsichtigung von Einrichtungen, die grenzüberschreitende Dienste erbringen.

Der Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2022/2555 über Vereinfachungsmaßnahmen und die Angleichung an die [Cybersicherheitsverordnung 2] fällt in den Aufgabenbereich des Programms zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT). Zusammen mit der Überarbeitung des derzeitigen Rechtsakts zur Cybersicherheit trägt er erheblich zur Verbesserung der Klarheit, zur Beseitigung von Ineffizienzen und zur Angleichung der Verfahren in allen Rechtsrahmen bei. Er trägt zum reibungslosen Funktionieren des Binnenmarkts bei und gewährleistet gleichzeitig die Sicherheit und strategische Autonomie der Union.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Die Union hat ihr rechtliches und politisches Instrumentarium durch die Annahme einer Reihe von Rechtsinstrumenten und politischen Maßnahmen erweitert: i) Die NIS-2-Richtlinie dient der Stärkung der Cybersicherheit kritischer Infrastrukturen; ii) physische Sicherheitsmaßnahmen sind in ihrer „Schwesterrichtlinie“, der Richtlinie über die Resilienz kritischer Einrichtungen, definiert; iii) mit der Cyberresilienzverordnung wird die Cybersicherheit von Produkten verbessert; iv) mit der Cybersolidaritätsverordnung werden EU-weite Reaktionsfähigkeiten aufgebaut; v) der EU-Cyberkonzeptentwurf[7] fördert die

[7] COM(2025) 66 final.

Zusammenarbeit bei der Krisenbewältigung auf EU-Ebene; vi) das Instrumentarium für die 5G-Cybersicherheit (5G-Instrumentarium) unterstützt die Cybersicherheit in 5G-Netzen; vii) der europäische Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern[8] trägt zur Verbesserung ihrer Cybersicherheit bei; und viii) die Akademie für Cybersicherheitskompetenzen[9] befasst sich mit der wachsenden Herausforderung des Fachkräftemangels im Bereich der Cybersicherheit.

Der oben genannte Rechtsrahmen für die Cybersicherheit wurde durch sektorspezifische Rechtsvorschriften ergänzt, nämlich die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA-Verordnung), den Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse (NCCS) für den Teilsektor Strom und die Vorschriften für die Informationssicherheit (Teil-IS[10]) für den Teilsektor Luftverkehr.

Dieser Richtlinienvorschlag ist – ebenso wie der Verordnungsvorschlag, dem er beigefügt ist – Teil eines breiteren Spektrums rechtlicher und politischer Initiativen, die von der Union angenommen wurden, um die Resilienz von Einrichtungen gegenüber Sicherheits- und Cyberbedrohungen zu verbessern. Der Schwerpunkt liegt auf gezielten Änderungen der NIS-2-Richtlinie, die unter anderem bestimmte Aspekte des Anwendungsbereichs, der Begriffsbestimmungen und der Zuständigkeitsvorschriften klären, den Aufwand bei der Beaufsichtigung wesentlicher und wichtiger Einrichtungen verringern und die Beaufsichtigung grenzüberschreitend tätiger Einrichtungen erleichtern sollen, indem die Rolle der ENISA bei der Unterstützung der operativen Zusammenarbeit gestärkt wird. Darüber hinaus schafft dieser Vorschlag zusammen mit dem Verordnungsvorschlag starke Synergien, die sich aus der Entwicklung der Zertifizierung der Cyberabwehr für die NIS-2-Richtlinie ergeben und möglicherweise die Einhaltung anderer einschlägiger Rechtsakte der Union wie der Datenschutz-Grundverordnung (DSGVO) erleichtern werden, unbeschadet ihrer spezifischen Zertifizierungsanforderungen. Diese Vereinfachungsmaßnahmen sollten Ressourcen freisetzen, um die operative Cybersicherheitsvorsorge von Einrichtungen in den kritischen Sektoren der Union zu stärken.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Mit diesem Vorschlag werden die Sicherheitsanforderungen für Einrichtungen, die Unternehmensbrieftaschen bereitstellen, gemäß dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung europäischer Unternehmensbrieftaschen[11] verschärft. Darüber hinaus wird die Kommission die Kohärenz mit künftigen Initiativen wie der Verordnung über digitale Netze (DNA) sicherstellen. Dieser Vorschlag steht im Einklang mit dem Vorschlag für eine Verordnung zur Vereinfachung der Rechtsvorschriften im digitalen Bereich (Digital-Omnibus-Vorschlag), der unter anderem Änderungen der NIS-2-Richtlinie sowie anderer Rechtsakte der Union umfasst. In der künftigen Digital-Omnibus-Verordnung wird vorgeschlagen, die Einhaltung der Anforderungen an die Cybersicherheitsberichterstattung, unter anderem im Rahmen der NIS-

8 COM(2025) 10 final.
9 COM(2023) 207 final.
10 Durchführungsverordnung (EU) 2023/203 der Kommission und Delegierte Verordnung (EU) 2022/1645 der Kommission.
11 COM(2025) 838 final.

2-Richtlinie, zu erleichtern, indem die Berichterstattung über eine zentrale Anlaufstelle zur Meldung von Vorfällen erfolgt, die von der ENISA aufgebaut und unterhalten wird. Ferner steht dieser Vorschlag mit dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Sicherheit, Resilienz und Nachhaltigkeit von Weltraumtätigkeiten in der Union[12] im Einklang.

Darüber hinaus steht der Vorschlag, wie oben hervorgehoben, im Einklang mit dem Bericht über die Zukunft der europäischen Wettbewerbsfähigkeit von Mario Draghi.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Die Rechtsgrundlage für diese Richtlinie ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), wonach Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten erlassen werden, mit denen die Errichtung und das Funktionieren des Binnenmarkts sichergestellt werden sollen. Mit diesem Vorschlag wird die Richtlinie (EU) 2022/2555 geändert, die auf der Grundlage von Artikel 114 AEUV erlassen wurde.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Das Subsidiaritätsprinzip erfordert eine Bewertung der Notwendigkeit und des Mehrwerts des Handelns der Union. Die Einhaltung des Subsidiaritätsprinzips in diesem Bereich wurde bereits bei der Annahme der Richtlinie (EU) 2022/2555, die durch diesen Vorschlag geändert wird, bestätigt.

Mit diesem Vorschlag wird die Einhaltung der Cybersicherheitsvorschriften der Union erleichtert, werden die Befolgungskosten und die Rechtsunsicherheit für die betroffenen Einrichtungen verringert und wird die Einhaltung der Cybersicherheitsanforderungen gefördert und verbessert. Er trägt auch dazu bei, gleiche Wettbewerbsbedingungen in Bezug auf Ansätze für die Beaufsichtigung und die Kontrolle der Einhaltung der Vorschriften in allen Mitgliedstaaten zu schaffen.

• Verhältnismäßigkeit

Die in dieser Richtlinie vorgeschlagenen Regeln gehen nicht über das für die zufriedenstellende Verwirklichung der spezifischen Ziele erforderliche Maß hinaus. Die vorgesehene Angleichung und Vereinheitlichung des Anwendungsbereichs, von Sicherheitsmaßnahmen und Meldepflichten entsprechen den Forderungen von Mitgliedstaaten und Unternehmen nach einer Verbesserung des geltenden Rahmens.

• Wahl des Instruments

Mit dem Vorschlag wird die bestehende NIS-2-Richtlinie geändert und werden die den Unternehmen auferlegten Verpflichtungen weiter gestrafft, wodurch ein höheres Maß an Harmonisierung in der gesamten Union sichergestellt wird. Die Wahl des Rechtsinstruments für diesen Vorschlag entspricht dem zu ändernden Rechtstext, d. h. der NIS-2-Richtlinie. Dieser Vorschlag baut auf dem Ziel der NIS-2-Richtlinie auf, den Mitgliedstaaten die nötige Flexibilität einzuräumen, um nationalen Besonderheiten Rechnung zu tragen.

[12] COM(2025) 335 final.

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

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2].

- **Konsultation der Interessenträger**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2].

- **Einholung und Nutzung von Expertenwissen**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2].

- **Folgenabschätzung**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2] sowie den begleitenden Folgenabschätzungsbericht.

- **Effizienz der Rechtsetzung und Vereinfachung**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2].

- **Grundrechte**

Siehe Begründung des [Vorschlags für die Cybersicherheitsverordnung 2].

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Bitte konsultieren Sie den Finanzbogen im [Vorschlag für die Cybersicherheitsverordnung 2].

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Gemäß Artikel 40 der NIS-2-Richtlinie wird die Kommission alle 36 Monate die Funktionsweise der Richtlinie überprüfen und dem Europäischen Parlament und dem Rat hierüber Bericht erstatten.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Mit dem Vorschlag soll die Einhaltung der Anforderungen an die Cybersicherheit vereinfacht und sollen Ressourcen freigesetzt werden, um die operative Cybersicherheitsvorsorge von Einrichtungen in den kritischen Sektoren der Union zu stärken.

Es werden gezielte Änderungen an der NIS-2-Richtlinie vorgenommen, um bestimmte Aspekte des Cybersicherheitsrahmens zu vereinfachen, die Rechtssicherheit zu erhöhen und die Umsetzung zu harmonisieren.

Damit Einrichtungen und Anbieter bzw. Lieferanten die Einhaltung der NIS-2-Richtlinie einfacher nachweisen können, werden Einrichtungen, die unter die NIS-2-Richtlinie fallen, im Einklang mit dem Verordnungsvorschlag, der diesem Vorschlag beigefügt ist, Zertifikate im Rahmen organisatorischer Systeme für die Cybersicherheitszertifizierung erlangen können, die im Zuge des Rahmens für die Cybersicherheitszertifizierung entwickelt wurden.

Um die Einhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit für länderübergreifende Einrichtungen, die der Aufsicht durch die zuständigen Behörden

mehrerer Mitgliedstaaten unterliegen, weiter zu erleichtern, wird der ENISA eine neue Rolle übertragen, die darin besteht, die Mitgliedstaaten bei der Beaufsichtigung dieser Einrichtungen zu unterstützen, die Amtshilfe zu fördern und einen besseren Überblick über die Einrichtungen zu schaffen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen.

Darüber hinaus sieht der Vorschlag vor, dass die Kommission Leitlinien für die Anwendung der Anforderungen an die Sicherheit der Lieferkette erlässt, die Einrichtungen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, an ihre Lieferanten weitergeben, um Rechtssicherheit zu gewährleisten und eine unzulässige Abwälzung von Verpflichtungen auf Einrichtungen, die nicht in den Anwendungsbereich der NIS-2-Richtlinie fallen, zu verhindern.

Weitere gezielte Änderungen der NIS-2-Richtlinie umfassen Folgendes:

- Präzisierung des Anwendungsbereichs und der Begriffsbestimmungen,
- Streichung von DNS-Diensteanbietern, die Kleinst- und -Kleinunternehmen sind, aus dem Anwendungsbereich,
- Einführung einer größtmöglichen Harmonisierung für Durchführungsrechtsakte gemäß Artikel 21 Absatz 5 (Festlegung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit), um den Einrichtungen die Einhaltung der Vorschriften und den Behörden die Aufsicht zu erleichtern,
- Einführung einer neuen Kategorie kleiner Midcap-Unternehmen im Einklang mit der Empfehlung der Kommission zur Definition kleiner Midcap-Unternehmen[18] von 2025, Einrichtungen, die als kleine Midcap-Unternehmen gelten, sind als wichtige Unternehmen zu benennen, wodurch ihr Befolgungsaufwand und der Beaufsichtigungsaufwand für die zuständigen Behörden verringert werden,
- Anforderung an die Mitgliedstaaten, im Rahmen ihrer nationalen Cybersicherheitsstrategie Konzepte für die Migration zur Post-Quanten-Kryptografie (PQC) anzunehmen, und
- Einführung einer harmonisierten Erhebung von Daten über Ransomware-Angriffe.

2026/0012 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2]

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

nach Stellungnahme des Ausschusses der Regionen[2],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) In der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[3] werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern. Seit Inkrafttreten der Richtlinie (EU) 2022/2555 sind Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Gleichzeitig sind bei der Umsetzung durch die Mitgliedstaaten bestimmte Herausforderungen aufgetreten, unter anderem im Hinblick auf den Anwendungsbereich der Richtlinie, die Umsetzung der Verpflichtungen in Bezug auf das Cybersicherheitsrisikomanagement und die Pflichten zur Meldung von Sicherheitsvorfällen sowie die Beaufsichtigung grenzüberschreitend tätiger Einrichtungen. Aufbauend auf dem [Vorschlag für die Cybersicherheitsverordnung 2] sollte die Richtlinie (EU) 2022/2555 gezielt geändert werden, um diesen Herausforderungen zu begegnen, indem bestimmte Aspekte vereinfacht werden, sodass die Rechtssicherheit erhöht und eine einheitliche Umsetzung der Richtlinie (EU) 2022/2555 sichergestellt wird.

---

1 ABl. C […], […], S. […].

2 ABl. C […], […], S. […].

3 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS- 2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(2) Um den Befolgungsaufwand für Einrichtungen und den Aufsichtsaufwand für die zuständigen Behörden zu verringern, sollte im Einklang mit der Empfehlung (EU) 2025/1099 der Kommission[4] eine neue Kategorie kleiner Midcap-Unternehmen in die Richtlinie (EU) 2022/2555 aufgenommen werden. Einrichtungen der in Anhang I der Richtlinie (EU) 2022/2555 genannten Art, die als kleine Midcap-Unternehmen im Sinne der genannten Empfehlung gelten, sollten in der Regel als wichtige Einrichtungen benannt werden. Um das Ziel der Kommission, die Verwaltungskosten im Allgemeinen um 25 % und für kleine und mittlere Unternehmen um 35 % zu senken, zu erreichen, sollte der in der Richtlinie (EU) 2022/2555 festgelegte allgemeine Schwellenwert für die Größe, nach dem alle Einrichtungen, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission[5] als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und die in den Sektoren tätig sind und die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, auf Domänennamensystem-Diensteanbieter Anwendung finden.

(3) Bei der Umsetzung der Richtlinie (EU) 2022/2555 gab es Probleme mit der Auslegung der Bestimmungen über ihren Anwendungsbereich. Daher sollten bestimmte anwendungsbezogene Bestimmungen in Bezug auf Gesundheitsdienstleister, Stromerzeuger, Wasserstoffunternehmen und Einrichtungen der chemischen Industrie präzisiert werden, um Rechtssicherheit zu schaffen und den Befolgungsaufwand sowohl für die Einrichtungen als auch für die nationalen Behörden zu verringern.

(4) Um die Verhältnismäßigkeit in Bezug auf Stromerzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates[6] zu wahren, sollten nur Stromerzeuger mit einer Gesamterzeugungskapazität von mehr als 1 MW als wesentliche oder wichtige Einrichtungen im Sinne der Richtlinie (EU) 2022/2555 gelten, sofern sie den Schwellenwert für die Größe erreichen. Dies sollte Stromerzeuger umfassen, bei denen die Kapazität einer einzelnen Stromerzeugungsanlage mehr als 1 MW beträgt, sowie Stromerzeuger, die mehrere Erzeugungsanlagen betreiben, die zusammen eine Erzeugungskapazität von mehr als 1 MW haben. Ein solcher Ansatz ermöglicht ein Gleichgewicht zwischen der Notwendigkeit, diejenigen Einrichtungen zu erfassen, bei denen ein Eingriff in ihr Netz- und Informationssystem zu einem Verlust, einer Nichtkontrollierbarkeit oder einer externen Kontrolle von Erzeugungskapazitäten führen könnte, die für sich genommen für die Sicherheit und Stabilität des Stromnetzes von Bedeutung sind, und der Notwendigkeit, den Unternehmen im Rahmen der Richtlinie (EU) 2022/2555 keinen unverhältnismäßigen Verwaltungsaufwand aufzuerlegen.

---

4 Empfehlung (EU) 2025/1099 der Kommission vom 21. Mai 2025 zur Definition kleiner Midcap-Unternehmen (ABl. L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

5 Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).

(5) Europäische Brieftaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[7] sind ein wesentlicher Bestandteil der digitalen Infrastruktur der Union und ermöglichen eine sichere Identifizierung und Authentifizierung sowie den Austausch elektronischer Dokumente, einschließlich elektronischer Attributsbescheinigungen. Angesichts ihrer entscheidenden Rolle für die Öffentlichkeit und für die Bereitstellung öffentlicher und privater Dienste könnte jeder Cybersicherheitsvorfall, der diese Brieftaschen betrifft, weitreichende Auswirkungen haben. Um die Erbringung ihrer Dienste sicherzustellen, sollten die Anbieter europäischer Brieftaschen für die digitale Identität dazu verpflichtet werden, geeignete technische, operative und organisatorische Maßnahmen zu ergreifen, um Cybersicherheitsrisiken zu bewältigen sowie Sicherheitsvorfälle zu verhindern bzw. darauf zu reagieren, und mit den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 zusammenarbeiten. Sie sollten daher unabhängig von ihrer Größe zu den Einrichtungen gehören, die unter die genannte Richtlinie fallen, und als wesentliche Einrichtungen eingestuft werden. Europäische Unternehmensbrieftaschen bieten ähnliche Funktionen und Dienste, die auf die Bedürfnisse von Wirtschaftsteilnehmern und öffentlichen Stellen zugeschnitten sind und auf dem EU-Rahmen für die digitale Identität aufbauen; sie sind für die Sicherheit und Integrität der digitalen Wirtschaft ebenso unverzichtbar. Folglich sollten Anbieter europäischer Unternehmensbrieftaschen, die gemäß [Vorschlag für eine Verordnung über die Einrichtung europäischer Unternehmensbrieftaschen][8] eingerichtet wurden, denselben Cybersicherheitsanforderungen und -pflichten unterliegen wie Anbieter europäischer Brieftaschen für die digitale Identität, sodass ein einheitliches und hohes Sicherheitsniveau im gesamten Ökosystem der digitalen Identität gewährleistet wird.

(6) Unterseeische Datenübertragungsinfrastrukturen umfassen nicht nur Seekabel, sondern auch alle mit ihrem Betrieb zusammenhängenden Infrastrukturen. Dazu gehören Landungsstellen und die sie verbindenden terrestrischen Teile des Seekabels, wie z. B. Landstrecken vom Uferschacht bis zur Landungsstelle, zum Rechenzentrum oder zum Netzknotenpunkt. Unterseeische Datenübertragungsinfrastrukturen werden in der Regel von Einrichtungen betrieben, die bereits unter die Richtlinie (EU) 2022/2555 fallen, einschließlich Anbietern öffentlicher elektronischer Kommunikationsnetze und -dienste oder Anbietern von Cloud-Computing-Diensten. Unterseeische Datenübertragungsinfrastrukturen können jedoch auch von anderen Arten von Einrichtungen betrieben werden, die derzeit nicht in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, z. B. unterseeische Datenübertragungsinfrastrukturen, die von Anbietern nicht öffentlicher elektronischer Kommunikationsnetze oder von Einrichtungen betrieben werden, die den Betrieb unterseeischer Datenübertragungsinfrastrukturen ganz oder teilweise an Anbieter öffentlicher elektronischer Kommunikationsnetze vermieten. Angesichts der zunehmenden Risiken für unterseeische Datenübertragungsinfrastrukturen und ihrer daraus resultierenden hohen Kritikalität muss sichergestellt werden, dass alle Arten von Betreibern unterseeischer Datenübertragungsinfrastrukturen unter die Richtlinie (EU) 2022/2555 fallen. Andere kritische maritime Infrastrukturen wie Seestromkabel sowie unterseeische Erdgas-, Wasserstoff- und Erdölfernleitungen fallen in der Regel

---

[7] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

[8] COM(2025) 838 final.

bereits unter die Richtlinie (EU) 2022/2555, da sie von Übertragungsnetzbetreibern in den Teilsektoren Strom, Erdgas, Wasserstoff und Erdöl betrieben werden.

(7) Damit Einrichtungen, die Dienste in mehreren Mitgliedstaaten erbringen, von kohärenteren und weniger aufwendigen Aufsichtsansätzen im gesamten Binnenmarkt profitieren können, sollten diese Einrichtungen in der Lage sein, die Einhaltung bestimmter oder aller in der Richtlinie (EU) 2022/2555 festgelegten Verpflichtungen zum Cybersicherheitsrisikomanagement nachzuweisen, indem sie im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung ein Zertifikat über die Cyberabwehr erlangen. Die Entwicklung eines solchen Systems wird vom Erlass von Durchführungsrechtsakten über die technischen und methodischen sowie sektorspezifischen Anforderungen an Cybersicherheitsrisikomanagementmaßnahmen gemäß der Richtlinie (EU) 2022/2555 profitieren, die auf einer größtmöglichen Harmonisierung beruhen.

(8) Angesichts der stetig zunehmenden Abhängigkeit unserer Gesellschaft und Wirtschaft von digitaler Technik müssen Maßnahmen zur Eindämmung der Quantenbedrohung ergriffen werden. Die Möglichkeit von Angriffen, bei denen heute Daten für eine spätere Entschlüsselung gesammelt werden (*„harvest now – decrypt later“*), die wahrscheinlich bereits jetzt stattfinden, und die künftigen Risiken, die durch Quantenangriffe in Bezug auf die Fälschung von Signaturen entstehen, sowie die geplante Abwertung bestimmter Algorithmusimplementierungen und die vollständige Nichtanerkennung derzeitiger Public-Key-Verschlüsselungsalgorithmen erhöhen die Dringlichkeit, Maßnahmen zur Umstellung auf Post-Quanten-Kryptografie (PQC) einzuleiten. Daher sollten die Mitgliedstaaten verpflichtet werden, im Rahmen ihrer nationalen Cybersicherheitsstrategie Konzepte für die Migration zur PQC anzunehmen. Solche Konzepte sollten die Beschleunigung der strategischen Planung und die Schaffung von Unterstützungsmaßnahmen und -instrumenten erleichtern, um die Exposition kryptografischer Werte gegenüber den von Quantencomputern ausgehenden Risiken zu bewerten. Darüber hinaus sollten sie bei der Erstellung eines Migrationsplans und bei der Erprobung der Einführung von PQC in digitalen Anwendungen und Netzen helfen und gleichzeitig die Entstehung und Einführung förmlich überprüfter und bewerteter europäischer PQC-Lösungen fördern, die den Einhaltungsrahmen für Produkte und Dienstleistungen entsprechen. Diese Konzepte sollten mit den Etappenzielen im Einklang stehen, die in den Rechtsakten und Strategien der Union sowie in den von der NIS-Kooperationsgruppe angenommenen Dokumenten festgelegt sind, insbesondere im von der NIS-Kooperationsgruppe im Juni 2025 angenommenen Fahrplan für die koordinierte Umsetzung des Übergangs zur PQC, sodass die Migration zur PQC für kritische Anwendungsfälle bis 2030 und für Anwendungsfälle mit mittlerem und niedrigem Niveau bis 2035 erreicht wird.

(9) Gemäß Artikel 21 Absatz 2 Buchstabe d der Richtlinie (EU) 2022/2555 müssen wesentliche und wichtige Einrichtungen für ein angemessenes Sicherheitsniveau in ihren Lieferketten sorgen. In der Praxis hat diese Verpflichtung zahlreiche Einrichtungen dazu veranlasst, bei ihren Lieferanten umfassende Auskünfte mithilfe heterogener Fragebögen, Formate und Verfahren einzuholen. Solche Anfragen zielen zwar darauf ab, die Sorgfaltspflicht und das Risikomanagement zu unterstützen, können aber auch einen erheblichen Verwaltungsaufwand für Lieferanten wesentlicher und wichtiger Einrichtungen mit sich bringen, insbesondere wenn ähnliche Informationen wiederholt in unterschiedlicher Form bereitgestellt werden müssen. Um diesen Aufwand zu verringern und einen kohärenten, verhältnismäßigen und effizienten Ansatz für die Bewertungen der Sicherheit der Lieferkette zu fördern, sollte

die Kommission Leitlinien ausarbeiten, in denen ein angemessener Detailgrad, eine angemessene Struktur und ein angemessenes Format für solche Anfragen empfohlen werden. Diese Leitlinien sollten die Harmonisierung erleichtern, unnötige Doppelarbeit verringern und sowohl den Einrichtungen als auch ihren Lieferanten helfen, ihren Verpflichtungen aus der Richtlinie (EU) 2022/2555 wirksam nachzukommen.

(10) Ransomware-Angriffe, bei denen Daten und Systeme durch Malware verschlüsselt werden und eine Lösegeldzahlung für die Freigabe verlangt wird, stellen nach wie vor eine der größten Bedrohungen für wesentliche und wichtige Einrichtungen dar. Die Harmonisierung und Verbesserung der Erhebung von Daten über Ransomware-Angriffe gegen betroffene wesentliche und wichtige Einrichtungen würde den Computer-Notfallteams (CSIRTs) und den nationalen Behörden Einblicke verschaffen und es ihnen ermöglichen, für künftige Maßnahmen gegen Ransomware-Angriffe zu sorgen, die angemessen und wirksam sind, Einrichtungen dabei zu unterstützen, ihre Resilienz zu erhöhen und künftige Angriffe zu verhindern, und die Erkenntnisse und Beweise zusammenzutragen, die Strafverfolgungsbehörden benötigen, um Ransomware-Banden zu stören und zu zerschlagen und ihre Täter zu bestrafen. Angesichts des potenziell sensiblen Charakters der Informationen, die über Ransomware-Angriffe ausgetauscht werden sollen, insbesondere darüber, ob eine Einrichtung ein Lösegeld gezahlt hat, und wenn ja, in welcher Höhe und an wen, sollten diese Informationen den CSIRTs oder gegebenenfalls den zuständigen Behörden nur auf deren Ersuchen übermittelt werden. Für die Zwecke dieses Informationsaustauschs sollten wesentliche und wichtige Einrichtungen aufgefordert werden, eine Person zu benennen, die als Kontaktstelle fungiert und die Vertraulichkeit und Vertrauenswürdigkeit des Informationsaustauschs gewährleistet. Im Rahmen der Internationalen Initiative zur Bekämpfung von Ransomware hat die Union eine unverbindliche internationale Grundsatzerklärung gebilligt, wonach einschlägige Institutionen, die unter der Aufsicht der beteiligten nationalen Regierungen stehen, keine Erpressungsforderungen durch Ransomware erfüllen sollten.

(11) Die Einhaltung der Verpflichtungen zur Meldung einschlägiger Informationen über Ransomware-Vorfälle sollte nicht zur Auferlegung zusätzlicher Verpflichtungen im Rahmen der Richtlinie (EU) 2022/2555 führen, denen die Einrichtung ohne die Meldung der Informationen nicht unterlegen hätte. Zu diesem Zweck sollten die Mitgliedstaaten im Rahmen ihrer nationalen Rechtsordnungen mögliche Risiken angehen, die sich aus einer höheren Haftung im Zusammenhang mit der Meldung einschlägiger Informationen über Ransomware-Vorfälle ergeben.

(12) Angesichts der grenzüberschreitenden Dimension vieler wesentlicher und wichtiger Einrichtungen im gesamten Binnenmarkt und der Notwendigkeit, Kohärenz zu gewährleisten und Konvergenz und Effizienz in Bezug auf Aufsichtskonzepte zu fördern, sollte die ENISA die Mitgliedstaaten bei der Amtshilfe für wesentliche und wichtige Einrichtungen unterstützen, die Dienste in mehr als einem Mitgliedstaat erbringen oder die Dienste in einem oder mehreren Mitgliedstaaten erbringen und deren Netz- und Informationssysteme sich in einem oder mehreren anderen Mitgliedstaaten befinden. Dazu sollten die Mitgliedstaaten dem von der ENISA geführten Register der Einrichtungen zusätzliche Informationen übermitteln. Auf der Grundlage der im Register wesentlicher und wichtiger Einrichtungen enthaltenen Informationen sollte die ENISA eine umfassende Analyse der grenzüberschreitenden Cybersicherheitsrisiken in Bezug auf wesentliche und wichtige Einrichtungen

durchführen. Die Analyse sollte auf einer Methodik beruhen, die gemeinsam mit der Kommission und der NIS-Kooperationsgruppe entwickelt wurde. Bei dieser Methodik könnte berücksichtigt werden, inwieweit wesentliche und wichtige Einrichtungen ihre Dienste auf breiter grenzüberschreitender Basis bereitstellen, auf grenzüberschreitende Dienste angewiesen sind, dem Risiko einer Lieferkettenkonzentration ausgesetzt sind, als Quelle für das Risiko einer Lieferkettenkonzentration bestimmt werden können, Sicherheitsvorfällen ausgesetzt sind, die erhebliche Störungen grenzüberschreitender Dienste verursachen könnten, oder sich bei der Erbringung ihrer Dienste auf Netz- und Informationssysteme stützen, die sich in verschiedenen Mitgliedstaaten und außerhalb der Union befinden. Auf der Grundlage des Risikoanalyseberichts sollte die ENISA den jeweils zuständigen Behörden empfehlen, gemeinsame Untersuchungsteams einzurichten, um zur Beaufsichtigung von Einrichtungen mit einem höheren Risiko für das reibungslose Funktionieren des Binnenmarkts im Falle von Sicherheitsvorfällen beizutragen und die zuständigen Behörden auf deren Ersuchen bei der Durchführung gemeinsamer Aufsichtsmaßnahmen zu unterstützen.

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

(14) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[9] angehört und haben am [Datum] eine gemeinsame Stellungnahme abgegeben —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Änderungen der Richtlinie (EU) 2022/2555

Die Richtlinie (EU) 2022/2555 wird wie folgt geändert:

1. Artikel 2 wird wie folgt geändert:

a) Absatz 2 Buchstabe a wird wie folgt geändert:

i) Ziffer iii erhält folgende Fassung:

„iii) Domänennamenregister der Domänen oberster Stufe;“

ii) Die folgenden Ziffern iv und v werden angefügt:

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

„iv) Anbieter europäischer Brieftaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014;

v) Anbieter europäischer Unternehmensbrieftaschen gemäß der Verordnung (EU) [...]*.

_____

* Verordnung (EU) [...] [Vorschlag für eine Verordnung über die Einrichtung europäischer Unternehmensbrieftaschen].“

b) Folgender Absatz 3a wird eingefügt:

„(3a) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie für Einrichtungen, die gemäß der Verordnung (EU) [...]** als Eigentümer und Betreiber strategischer Infrastrukturen mit doppeltem Verwendungszweck ermittelt wurden.

_____

** Verordnung (EU) [...] [Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für Maßnahmen zur Erleichterung der unionsweiten Beförderung von militärischer Ausrüstung, militärischen Gütern und militärischem Personal].“

2. Artikel 3 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

i) Die Buchstaben a und b erhalten folgende Fassung:

„a) Einrichtungen der in Anhang I aufgeführten Art, die die Schwellenwerte für Midcap-Unternehmen überschreiten;

b) qualifizierte Vertrauensdiensteanbieter, Anbieter europäischer Brieftaschen für die digitale Identität, Anbieter europäischer Unternehmensbrieftaschen und Domänennamenregister der Domänen oberster Stufe, unabhängig von ihrer Größe;“

ii) Folgender Buchstabe h wird angefügt:

„h) Einrichtungen, die gemäß der Verordnung (EU) [...] [Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für Maßnahmen zur Erleichterung der unionsweiten Beförderung von militärischer Ausrüstung, militärischen Gütern und militärischem Personal] als Eigentümer und Betreiber strategischer Infrastrukturen mit doppeltem Verwendungszweck ermittelt wurden.“

b) Absatz 4 Unterabsatz 1 erhält folgende Fassung:

„Für die Zwecke der Erstellung der in Absatz 3 genannten Liste schreiben die Mitgliedstaaten vor, dass die in jenem Absatz genannten Einrichtungen den zuständigen Behörden mindestens die folgenden Informationen übermitteln:

a) Name der Einrichtung,

b) gegebenenfalls, einschlägiger Sektor, Teilsektor und Art der Einrichtung gemäß Anhang I oder II,

c) Anschrift der Einrichtung oder gegebenenfalls der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen ist, Anschrift ihres nach Artikel 26 Absatz 3 benannten Vertreters,

d) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen, Telefonnummern, einheitlicher Kennung und gegebenenfalls digitaler Adressen der europäischen Unternehmensbrieftasche der Einrichtung, und ihres gemäß Artikel 26 Absatz 3 benannten Vertreters,

e) die Mitgliedstaaten, in denen die Einrichtung Dienste erbringt,

f) die IP-Adressbereiche der Einrichtung.“

3. Artikel 5 erhält folgende Fassung:

„*Artikel 5*

Mindestharmonisierung

Unbeschadet des Artikels 21 Absatz 5 Unterabsatz 5 hindert diese Richtlinie die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen.“

4. In Artikel 6

werden die folgenden Nummern 42 und 43 angefügt:

„42. ‚kleines Midcap-Unternehmen‘ ein kleines Midcap-Unternehmen im Sinne der Definition im Anhang der Empfehlung (EU) 2025/1099 der Kommission***;

43. ‚unterseeische Datenübertragungsinfrastruktur‘ Seekabel, die Daten übertragen, sowie die zugehörigen Infrastrukturen und andere Einrichtungen oder Elemente im Zusammenhang mit der Datenübertragung.

_____

*** Empfehlung (EU) 2025/1099 der Kommission vom 21. Mai 2025 zur Definition kleiner Midcap-Unternehmen (ABl. L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).“

5. In Artikel 7 Absatz 2 wird folgender Buchstabe k angefügt:

„k) für den Übergang zur Post-Quanten-Kryptografie, unter Berücksichtigung der Übergangsfristen und der einschlägigen Anforderungen, die in den geltenden Rechtsakten und Maßnahmen der Union festgelegt sind.“

6. Artikel 15 Absatz 2 Satz 1 erhält folgende Fassung:

„Das CSIRTs-Netzwerk setzt sich aus Vertretern der gemäß Artikel 10 benannten oder eingerichteten CSIRTs der Mitgliedstaaten, des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) und der ENISA zusammen.“

7. Artikel 21 Absatz 5 wird wie folgt geändert:

a) Unterabsatz 2 erhält folgende Fassung:

„Die Kommission kann Durchführungsrechtsakte erlassen, in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die

sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf andere als die in Unterabsatz 1 des vorliegenden Absatzes genannten wesentlichen und wichtigen Einrichtungen festgelegt werden. Die Kommission bewertet regelmäßig, ob Durchführungsrechtsakte gemäß diesem Unterabsatz für bestimmte Sektoren oder Arten von Einrichtungen zu erlassen sind, um das Funktionieren des Binnenmarkts zu verbessern. Bei der Ausarbeitung solcher Bewertungen konzentriert sich die Kommission insbesondere auf den grenzüberschreitenden Charakter von Sektoren oder Arten von Einrichtungen und führt ein offenes, transparentes und inklusives Konsultationsverfahren mit den einschlägigen Interessenträgern und den Mitgliedstaaten durch.“

b) Folgender Unterabsatz 5 wird angefügt:

„Erlässt die Kommission Durchführungsrechtsakte gemäß den Unterabsätzen 1 und 2 des vorliegenden Absatzes, so erlegen die Mitgliedstaaten den in den Anwendungsbereich dieser Durchführungsrechtsakte fallenden Einrichtungen keine weiteren technischen, methodischen oder sektorspezifischen Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen auf.“

8. In Artikel 23 werden folgende Absätze 12 und 13 angefügt:

„(12) Beim Erlass eines Durchführungsrechtsakts gemäß Absatz 11 Unterabsatz 1 nimmt die Kommission Anforderungen auf, wonach die folgenden Informationen in Bezug auf Ransomware-Angriffe gemäß Absatz 1 übermittelt werden müssen:

a) ob die Einrichtung einen Ransomware-Angriff festgestellt hat,

b) den Angriffsvektor des Ransomware-Angriffs,

c) ob Abhilfemaßnahmen umgesetzt wurden.

(13) Die Mitgliedstaaten stellen sicher, dass die betroffenen Einrichtungen im Falle eines erheblichen Sicherheitsvorfalls, der durch einen Ransomware-Angriff verursacht wurde, auf Ersuchen des CSIRT oder gegebenenfalls der zuständigen Behörde über einen vom CSIRT oder gegebenenfalls der zuständigen Behörde bereitgestellten Kommunikationskanal Folgendes mitteilen:

a) ob die Einrichtung eine Lösegeldforderung erhalten hat und gegebenenfalls von wem,

b) ob ein Lösegeld gezahlt wurde, und wenn ja, in welcher Höhe und an welchen Empfänger oder welche Empfängerseite, gegebenenfalls einschließlich der Anbieter von Kryptowerten und Krypto-Dienstleistungen.“

9. In Artikel 24 werden folgende Absätze 4, 5 und 6 angefügt:

„(4) Zum Nachweis der Einhaltung des Artikels 21 können die Mitgliedstaaten von wesentlichen und wichtigen Einrichtungen verlangen, im Rahmen eines nach Artikel 75 der Verordnung (EU) XXX/XXX **** [Vorschlag für die Cybersicherheitsverordnung 2] angenommenen europäischen Systems für die Cybersicherheitszertifizierung ein Zertifikat über die Cyberabwehr zu erlangen.

(5) Wird die Cyberabwehr einer wesentlichen oder wichtigen Einrichtung im Rahmen eines gemäß Artikel 74 der Verordnung (EU) XXXX/XXX**** [Vorschlag für die Cybersicherheitsverordnung 2] angenommenen europäischen Systems für die Cybersicherheitszertifizierung zertifiziert und geht aus dem Zertifikat hervor, dass

die Anforderungen, die in einem gemäß Artikel 21 Absatz 5 der vorliegenden Richtlinie erlassenen Durchführungsrechtsakt oder in nationalen Rechtsvorschriften zur Umsetzung von Artikel 21 Absätze 1 und 2 der vorliegenden Richtlinie festgelegt sind, erfüllt werden, so unterwerfen die zuständigen Behörden diese Einrichtung bezüglich der unter das Zertifikat fallenden Anforderungen keinen zusätzlichen Maßnahmen gemäß Artikel 32 Absatz 2 Buchstabe b bzw. Artikel 33 Absatz 2 Buchstabe b.

(6) Eine Zertifizierung gemäß Absatz 4 berührt nicht die Verantwortung der wesentlichen oder wichtigen Einrichtung für die Einhaltung dieser Richtlinie.

_____

**** Verordnung (EU) XXX/XXX [Vorschlag für die Cybersicherheitsverordnung 2].“

10. Artikel 26 wird wie folgt geändert:

a) In Absatz 1 wird folgender Buchstabe d angefügt:

„d) Luftfahrtunternehmen, die der rechtlichen Zuständigkeit des Mitgliedstaats unterliegen, dessen zuständige Genehmigungsbehörde der Einrichtung gemäß der Verordnung (EG) Nr. 1008/2008 des Europäischen Parlaments und des Rates***** die Betriebsgenehmigung erteilt hat, oder – falls die Betriebsgenehmigung oder eine gleichwertige Genehmigung nicht gemäß der genannten Verordnung erteilt wurde – die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben.

_____

***** Verordnung (EG) Nr. 1008/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 über gemeinsame Vorschriften für die Durchführung von Luftverkehrsdiensten in der Gemeinschaft (Neufassung) (ABl. L 293 vom 31.10.2008, S. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj).“

b) Absatz 3 erhält folgende Fassung:

„(3) Hat eine wesentliche oder wichtige Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist. Handelt es sich bei einer solchen Einrichtung um eine Einrichtung im Sinne von Absatz 1 Buchstabe a, so wird davon ausgegangen, dass sie der Zuständigkeit des Mitgliedstaats unterliegt, in dem sie ihre Dienste erbringt. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie einleiten.“

11. Artikel 27 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die ENISA erstellt und pflegt ein Register der wesentlichen und wichtigen Einrichtungen sowie der Einrichtungen, die Domänennamen-

Registrierungsdienste erbringen, auf der Grundlage der Informationen, die sie von den zentralen Anlaufstellen gemäß Artikel 4 erhalten hat. Auf Anfrage gewährt die ENISA den zuständigen Behörden Zugang zu Informationen über DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke und Luftfahrtunternehmen, die in diesem Register gespeichert sind, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.“

b) Absatz 2 wird gestrichen.

c) Absätze 3, 4 und 5 erhalten folgende Fassung:

„(3) Die Mitgliedstaaten stellen sicher, dass im Falle einer Änderung der gemäß Artikel 3 Absatz 4 übermittelten Angaben die wesentlichen und wichtigen Einrichtungen die zuständige Behörde unverzüglich über diese Änderung, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung, unterrichten.

(4) Nach Erhalt der in Artikel 3 Absatz 4 genannten Angaben leitet die zentrale Anlaufstelle des betreffenden Mitgliedstaats diese unverzüglich an die ENISA weiter.

(5) Gegebenenfalls werden die in Artikel 3 Absatz 4 Unterabsatz 1 genannten Angaben über den in Artikel 3 Absatz 4 Unterabsatz 4 genannten nationalen Mechanismus übermittelt.“

12. Folgender Artikel 37a wird eingefügt:

„Artikel 37a

Die Rolle der ENISA bei der Amtshilfe

(1) Die ENISA unterstützt die Mitgliedstaaten bei der Amtshilfe im Sinne des Artikels 37 und trägt dazu bei, solche Kooperationsprozesse für wesentliche und wichtige Einrichtungen zu erleichtern, die Dienste in mehr als einem Mitgliedstaat erbringen oder die Dienste in einem oder mehreren Mitgliedstaaten erbringen und deren Netz- und Informationssysteme sich in einem oder mehreren anderen Mitgliedstaaten befinden.

(2) Für die Zwecke des Absatzes 1 führt die ENISA bis zum ... [15 Monate nach Inkrafttreten dieser Verordnung] eine umfassende Analyse der grenzüberschreitenden Cybersicherheitsrisiken im Zusammenhang mit wesentlichen und wichtigen Einrichtungen durch, die Dienste in mehr als einem Mitgliedstaat erbringen oder die Dienste in einem oder mehreren Mitgliedstaaten erbringen und deren Netz- und Informationssysteme sich in einem oder mehreren anderen Mitgliedstaaten befinden. Bei der Analyse wird das Ausmaß möglicher grenzübergreifender und den Binnenmarkt erfassender Folgen von Sicherheitsvorfällen, die solche wesentlichen und wichtigen Einrichtungen betreffen, bewertet. Für die Zwecke dieser Analyse entwickelt die ENISA in Zusammenarbeit mit der Kommission und der Kooperationsgruppe eine Methodik. Auf der Grundlage der Analyse erstellt die ENISA einen umfassenden Bericht über die Bewertung des grenzüberschreitenden Cybersicherheitsrisikos, der jährlich aktualisiert wird.

(3) Auf der Grundlage des umfassenden Berichts über die Bewertung des grenzüberschreitenden Cybersicherheitsrisikos unternimmt die ENISA folgende Schritte:

a) gegebenenfalls Empfehlung an die jeweils zuständigen Behörden, gemeinsame Untersuchungsteams einzurichten, um die Beaufsichtigung bestimmter Einrichtungen zu unterstützen;

b) Ausarbeitung von Leitlinien für gemeinsame Aufsichtsmaßnahmen;

c) auf Ersuchen der zuständigen Behörden der betreffenden Mitgliedstaaten: Festlegung praktischer Regelungen für die Durchführung gemeinsamer Aufsichtsmaßnahmen;

d) auf Ersuchen der zuständigen Behörden der betreffenden Mitgliedstaaten sowie unter Berücksichtigung ihrer eigenen Ressourcen und im angemessenen Verhältnis zu diesen: Teilnahme an gemeinsamen Aufsichtsmaßnahmen;

e) auf Ersuchen der zuständigen Behörden der betroffenen Mitgliedstaaten: Unterstützung bei der Bewertung des Stands der Umsetzung der in Artikel 21 festgelegten Cybersicherheitsrisikomanagementmaßnahmen durch eine wesentliche oder wichtige Einrichtung.

(4) Für die Zwecke des Absatzes 3 Buchstabe e übermitteln die zuständigen Behörden der betreffenden Mitgliedstaaten der ENISA, soweit verfügbar, eine Liste der von der wesentlichen oder wichtigen Einrichtung gemäß Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit, eine Liste der durchgeführten Aufsichts- oder Durchsetzungsmaßnahmen sowie die einschlägigen Unterlagen, einschließlich Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsaudits, die die zuständigen Behörden gemäß den Artikeln 32 und 33 in Bezug auf diese Einrichtung durchgeführt haben.

(5) Erhält ein Mitgliedstaat Amtshilfe gemäß Artikel 37 Absatz 1 Unterabsatz 1 Buchstabe c, so teilt die zentrale Anlaufstelle der ENISA mit, dass Amtshilfe geleistet wurde. Dabei gibt die zentrale Anlaufstelle gegebenenfalls an, welcher grenzüberschreitende Sicherheitsvorfall gemäß Artikel 23 Absatz 6 mit der Amtshilfe in Verbindung stand.“

13. Die Anhänge I und II werden nach Maßgabe des Anhangs dieser Richtlinie geändert.

Artikel 2
Umsetzung

(1) Bis zum … [12 Monate nach dem Inkrafttreten dieser Richtlinie] erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Vorschriften ab dem ... [einen Tag nach dem im ersten Unterabsatz genannten Datum] an.

(2) Bei Erlass der in Absatz 1 genannten Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten legen die Einzelheiten der Bezugnahme fest.

Artikel 3

Inkrafttreten

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

Artikel 4

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident/Die Präsidentin*
[...]	*[...]*