Europäisches Parlament
2019-2024

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

2020/0359(COD)

15.10.2021

STELLUNGNAHME

des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Verfasser der Stellungnahme (*): Lukas Mandl

(*) Assoziierter Ausschuss – Artikel 57 der Geschäftsordnung

PA_Legam

KURZE BEGRÜNDUNG

Der Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)[1] ist Teil eines umfassenderen Pakets von Initiativen auf Ebene der Union, mit denen die Widerstandsfähigkeit öffentlicher und privater Einrichtungen gegenüber Bedrohungen erhöht werden soll. Mit dem Vorschlag sollen die Lücken in den bestehenden Rechtsvorschriften angegangen und die in ihren Anwendungsbereich fallenden Einrichtungen in die Lage versetzt werden, besser auf die neuen Herausforderungen zu reagieren, die von der Kommission in ihrer Folgenabschätzung, die auch eine umfassende Konsultation von Interessenträgern beinhaltete, ermittelt wurden. Zu diesen Herausforderungen gehören die zunehmende Digitalisierung des Binnenmarkts und die sich entwickelnde Sicherheitsbedrohungslage.

Die Rechtsgrundlage des Vorschlags bildet Artikel 114 AEUV, d. h der Binnenmarkt. Aus Sicht des LIBE-Ausschusses ist es jedoch wichtig, hervorzuheben, dass die Maßnahmen, die Netz- und Informationssystemen mit der NIS-2-Richtlinie auferlegt wurden, nicht nur dazu dienen, das ordnungsgemäße Funktionieren des Binnenmarkts sicherzustellen. **Die Richtlinie sollte auch zur Sicherheit der gesamten Union beitragen**, unter anderem indem eine unterschiedliche Anfälligkeit der Mitgliedstaaten gegenüber Cybersicherheitsrisiken verhindert wird.

Zu diesem Zweck ist es von entscheidender Bedeutung, **bestehende Unterschiede zwischen den Mitgliedstaaten**, die sich aus verschiedenen Auslegungen der Rechtsvorschriften durch die Mitgliedstaaten ergeben, **zu beseitigen**. Daher begrüßt der Verfasser der Stellungnahme die mit der Verordnung festgelegte einheitliche Bedingung, mit der bestimmt wird, welche Einrichtungen in den Anwendungsbereich der Richtlinie fallen. Um Unterschiede bei der Umsetzung zu verhindern, werden zusätzliche Vorschläge unterbreitet, wobei insbesondere vorgesehen ist, dass die Kommission verpflichtet wird, Leitlinien zur Umsetzung der lex specialis und zu den für KMU geltenden Kriterien herauszugeben (die Rechtssicherheit bieten und unnötigen Aufwand verhindern sollten) und dass die Kooperationsgruppe verpflichtet wird, die nichttechnischen Faktoren, die bei den Lieferketten-Risikobewertungen zu berücksichtigen sind, näher zu bestimmen. Darüber hinaus wird betont, dass die Zusammenarbeit zwischen den zuständigen Behörden, sowohl innerhalb der Mitgliedstaaten als auch *zwischen* den Mitgliedstaaten in Echtzeit stattfinden muss.

Der Entwurf eines Berichts trägt auch einer Reihe von **Empfehlungen des EDSB** Rechnung, die in dessen Stellungnahme zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie[2] unterbreitet wurden. Insbesondere wird sowohl in den Erwägungsgründen als auch im verfügenden Teil des Textes deutlich gemacht, dass die Verarbeitung personenbezogener Daten gemäß der NIS-2-Richtlinie nicht die Verordnung (EU) 2016/679 (DSGVO)[3] und die

[1] 2020/0359(COD).
[2] Stellungnahme Nr. 5/2021: https://edps.europa.eu/system/files/2021-05/21-03-11_edps_nis2-opinion_de_0.pdf
[3] 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

Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)[4] berührt. Da der Begriff „Sicherheit von Netz- und Informationssystemen“ (der nur den Schutz von Technologien abdeckt) enger gefasst ist als der Begriff „Cybersicherheit“ (der auch Tätigkeiten zum Schutz von Nutzern abdeckt), wird der erstgenannte Begriff nur im rein technischen Kontext verwendet. Im Zusammenhang mit Domänennamen und Registrierungsdaten werden Präzisierungen vorgeschlagen, die folgende Aspekte betreffen: die Rechtsgrundlage für die Veröffentlichung „einschlägiger Angaben“ zu Zwecken der Identifizierung und Kontaktaufnahme, 2) die Kategorien von Daten über die Registrierung der Domänennamen, die einer Veröffentlichung unterliegen (beruhend auf einer Empfehlung der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN)) und 3) die Einrichtungen, die „berechtigte Zugangsnachfrager“ darstellen könnten. In dem Rechtstext wird ferner präzisiert, dass der Vorschlag nicht die Zuweisung von Zuständigkeiten und Befugnissen von Datenschutzaufsichtsbehörden gemäß der DSGVO berührt. Schließlich wird eine umfassendere Rechtsgrundlage für die Zusammenarbeit und den Austausch einschlägiger Informationen zwischen den zuständigen Behörden gemäß dem Vorschlag und sonstigen Aufsichtsbehörden, insbesondere Aufsichtsbehörden gemäß der DSGVO, geschaffen.

Weitere Änderungen, die vom Verfasser der Stellungnahme des LIBE-Ausschusses am Vorschlag der Kommission vorgenommen wurden, betreffen die folgenden Aspekte:

- Um für Kohärenz zwischen der NIS-2-Richtlinie und der vorgeschlagenen Richtlinie über die Resilienz kritischer Einrichtungen[5] zu sorgen, wurde der Wortlaut einiger Bestimmungen an den des letztgenannten Vorschlags angeglichen. Im Einklang mit einer ähnlichen Änderung, die für die Richtlinie über die Resilienz kritischer Einrichtungen vorgesehen ist, die die gleichen Sektoren abdecken sollte wie die NIS-2-Richtlinie, wird vorgeschlagen, „Herstellung, Verarbeitung und Vertrieb von Lebensmitteln“ zum Anwendungsbereich hinzuzufügen.
- In Bezug auf personenbezogene Daten wird klargestellt, dass die Überprüfung von Netz- und Informationssystemen durch CSIRTs nicht nur mit der Verordnung (EU) 2016/679 (DSGVO)[6], sondern auch mit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)[7] im Einklang stehen sollte. Internationale Übermittlungen personenbezogener Daten gemäß dieser Richtlinie sollten mit Kapitel V der DSGVO im Einklang stehen.
- Die Kooperationsgruppe sollte zweimal statt einmal jährlich zusammentreten, um eine Bestandsaufnahme der jüngsten Entwicklungen im Bereich der Cybersicherheit

---

Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1.

[4] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

[5] 2020/0365(COD).

[6] 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) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1.

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

vorzunehmen. Der EDSA sollte als Beobachter an den Sitzungen der Kooperationsgruppe teilnehmen.

- Die ENISA sollte jährlich statt alle zwei Jahre Berichte über den Stand der Cybersicherheit in der Union veröffentlichen. Der Bericht sollte auch den Auswirkungen von Cybersicherheitsvorfällen auf den Schutz personenbezogener Daten in der Union Rechnung tragen.
- Die Frist für die Meldung von Vorfällen wird an die Frist für die Meldung von Verstößen gemäß der DSGVO angepasst, die 72 Stunden beträgt.
- Die Meldung tatsächlicher Cybersicherheitsvorfälle durch wesentliche und wichtige Einrichtungen sollte in der Tat verpflichtend sein, die Meldung von Cyberbedrohungen hingegen sollte freiwillig sein, um den Verwaltungsaufwand zu verringern und ausufernde Meldungen zu verhindern. Um als erheblich zu gelten, sollte ein Vorfall tatsächlich einen Schaden verursacht und sich auf andere natürliche und juristische Personen ausgewirkt haben, statt einen derartigen Schaden oder eine derartige Wirkung nur ermöglicht zu haben.
- Die Umstände, die bei der Entscheidung über Sanktionen infolge eines Verstoßes gegen die Cybersicherheitsvorschriften zu berücksichtigen sind, werden an die DSGVO angepasst. Es sollte nicht möglich sein, natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen, da dies den derzeitigen Haftungsregelungen des Unionsrechts zuwiderlaufen würde.
- Um Rufschädigung zu vermeiden, sollten Einrichtungen nicht verpflichtet werden, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen oder die Identität der für den Verstoß verantwortlichen natürlichen oder juristischen Personen öffentlich bekannt zu machen.

ÄNDERUNGSANTRÄGE

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1

Vorschlag für eine Richtlinie
Erwägung 1

Vorschlag der Kommission	*Geänderter Text*
(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher	(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher

Dienste bei Cybersicherheitsvorfällen, um so zum reibungslosen Funktionieren ***der*** Wirtschaft und Gesellschaft ***der Union*** beizutragen.

---

[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Dienste bei Cybersicherheitsvorfällen, um so ***zur Sicherheit der Union und*** zum reibungslosen Funktionieren ***ihrer*** Wirtschaft und Gesellschaft beizutragen.

---

[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe***[12]*** und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk)***[13]*** zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames	(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk) zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames

Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern. ***Darüber hinaus wurde durch die Ausweitung der Online-Tätigkeiten im Rahmen der COVID-19-Pandemie die Bedeutung von Cybersicherheit, die unerlässlich ist, damit die EU-Bürger in Innovation und Konnektivität vertrauen können, und von umfassender Aus- und Weiterbildung in diesem Bereich deutlich. Die Kommission sollte die Mitgliedstaaten daher bei der Konzeption von Bildungsprogrammen zur Cybersicherheit unterstützen, um wichtige und wesentliche Einrichtungen in die Lage zu versetzen, Sachverständige für Cybersicherheit einzustellen, die es ihnen ermöglichen, den sich aus dieser Richtlinie ergebenden Verpflichtungen nachzukommen.***

---

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

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

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

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

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 3

Vorschlag der Kommission

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite,

Geänderter Text

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite,

Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft ***der Union*** großen Schaden zufügen. ***Heute sind daher im Bereich Cybersicherheit*** Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.	Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft ***der Union, der Funktionsfähigkeit unserer Demokratie*** und ***den Werten und Freiheiten, auf denen unsere*** Gesellschaft ***beruht,*** großen Schaden zufügen. ***Vor dem Hintergrund des digitalen Wandels der täglichen Tätigkeiten in der gesamten Union sind daher*** Vorsorge und Wirksamkeit ***im Bereich Cybersicherheit heute*** wichtiger denn je für ***die Sicherheit in der Union und*** das reibungslose Funktionieren des Binnenmarkts. ***Dies erfordert eine engere Zusammenarbeit in und zwischen den Mitgliedstaaten sowie zwischen nationalen Behörden und den zuständigen Stellen der Union.***

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 5

Vorschlag der Kommission	*Geänderter Text*
(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden,	(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. ***Letztendlich können diese Unterschiede zu einer höheren Anfälligkeit einiger Mitgliedstaaten gegenüber Cybersicherheitsbedrohungen führen, deren Auswirkungen auf die gesamte Union übergreifen könnten, sowohl im***

Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

Hinblick auf ihren Binnenmarkt, als auch im Hinblick auf die allgemeine Sicherheit. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit ***in Echtzeit*** zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten ***und zwischen den zuständigen Behörden der Mitgliedstaaten*** vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 6

Vorschlag der Kommission	*Geänderter Text*
(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum	(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen ***nationalen*** Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die ***Verhütung,*** Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang

Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.

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

sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.

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

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 8

Vorschlag der Kommission	*Geänderter Text*
(8) ***Gemäß*** der Richtlinie (EU) 2016/1148 ***waren die Mitgliedstaaten dafür zuständig zu bestimmen***, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“)***.*** ***Um die diesbezüglichen*** großen ***Unterschiede*** zwischen den Mitgliedstaaten ***zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich*** der ***Risikomanagementanforderungen und der Meldepflichten zu gewährleisten***, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15]***,*** die in den Sektoren tätig	(8) ***Die Zuständigkeit der Mitgliedstaaten, die gemäß*** der Richtlinie (EU)2016/1148 ***bestimmen mussten***, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“)***, hat diesbezüglich zu*** großen ***Unterschieden*** zwischen den Mitgliedstaaten ***geführt. Unbeschadet*** der ***in dieser Richtlinie vorgesehenen spezifischen Ausnahmen***, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen***, um diese Unterschiede zu beseitigen und hinsichtlich der Risikomanagementanforderungen und der Meldepflichten für alle einschlägigen Einrichtungen für Rechtssicherheit zu sorgen***. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und

sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.

großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.

---

[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 8 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(8a) Angesichts der Unterschiede bei den nationalen Rahmen für die öffentliche Verwaltung behalten die Mitgliedstaaten ihre Entscheidungsbefugnis in Bezug auf die Benennung von Einrichtungen im Rahmen des Anwendungsbereichs der vorliegenden Richtlinie.

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) ***Allerdings sollten auch*** Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder	(9) ***Auch*** Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie ***auf der Grundlage einer Risikobewertung*** eine

Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.	Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, ***einschließlich Einrichtungen, die gemäß der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[1a] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen definiert sind, sollten*** von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.
	_____
	1aRichtlinie (EU) [XXX/XXX] des Europäischen Parlaments und des Rates vom XXX über die Resilienz kritischer Einrichtungen (ABl. ...).

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die Kommission ***kann*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und ***Kleinstunternehmen*** geltenden Kriterien herausgeben.	(10) Die Kommission ***sollte*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und ***Kleinsteinrichtungen*** geltenden Kriterien herausgeben.

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und	(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und

gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***kann*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***sollte*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der	(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte***, sofern möglich und angebracht,*** dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen

Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***der*** gemäß der vorliegenden Richtlinie zuständigen ***Behörde*** und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über ***Sicherheitsvorfälle*** und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von ***kritischen Einrichtungen*** ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ***ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber*** einer als kritisch eingestuften wesentlichen Einrichtung ***auszuüben***. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

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

gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***den*** gemäß der vorliegenden Richtlinie zuständigen ***Behörden in und zwischen den Mitgliedstaaten*** und der gemäß ***der*** Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über ***Cybersicherheitsvorfälle*** und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten ***in und zwischen den Mitgliedstaaten*** zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von ***den zuständigen Behörden gemäß dieser Richtlinie*** ergriffenen ***für kritische Einrichtungen relevanten*** Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ***die Cybersicherheit*** einer als kritisch eingestuften wesentlichen Einrichtung ***zu bewerten***. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und ***in Echtzeit*** Informationen austauschen.

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

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 18

Vorschlag der Kommission	*Geänderter Text*
(18) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die ***Sicherheit von Netz- und Informationssystemen*** zu begegnen, sollte die vorliegende Richtlinie auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von ihr für eigene Zwecke betrieben werden.	(18) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die ***Cybersicherheit*** zu begegnen, sollte die vorliegende Richtlinie auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von ihr für eigene Zwecke betrieben werden.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Diese wachsenden gegenseitigen	(20) Diese wachsenden gegenseitigen

Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie ***hat*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.	Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, ***Herstellung, Verarbeitung und Vertrieb von Lebensmitteln,*** Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die ***verstärkten Angriffe auf Informationssysteme während der*** COVID-19-Pandemie ***haben*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind. ***Daher sind weitere Investitionen in die Cybersicherheit erforderlich.***

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 20 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(20a) Es ist von entscheidender Bedeutung, in allen kritischen und wichtigen Einrichtungen, einschließlich Einrichtungen der öffentlichen Verwaltung, das Bewusstsein für Cybersicherheit zu schärfen und die Cyberabwehrfähigkeit zu steigern.

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 21

Vorschlag der Kommission	*Geänderter Text*
(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen.	(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen ***und sicherstellen, dass diese über angemessene Ressourcen verfügt, damit sie ihre Aufgaben wirksam und effizient erfüllen kann***.

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 22

Vorschlag der Kommission	*Geänderter Text*
(22) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der ***Sicherheit von Netz-und Informationssystemen*** und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.	(22) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der ***Cybersicherheit*** und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.

Änderungsantrag 17

Vorschlag für eine Richtlinie
Erwägung 23

Vorschlag der Kommission	*Geänderter Text*
(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen ***anderer betroffener*** Mitgliedstaaten weiterzuleiten. Damit sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige behördliche Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.	(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle ***in Echtzeit*** an die zentralen Anlaufstellen ***aller anderen*** Mitgliedstaaten weiterzuleiten. Damit sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige behördliche Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine ***proaktive Überprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Netz-*** und ***Informationssysteme auf Schwachstellen vorzunehmen***. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.	(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] ***und der Richtlinie 2002/58/EG*** im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine ***Sicherheitsüberprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Informationssysteme*** und ***Netzbereiche vorzunehmen, um spezifische Bedrohungen zu erkennen, abzuschwächen oder zu verhindern***. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen. ***Ferner sollten Cybersicherheitsrisiken niemals als Vorwand für Verletzungen der Grundrechte herangezogen werden.***
[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).	[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Änderungsantrag 19

Vorschlag für eine Richtlinie
Erwägung 27

Vorschlag der Kommission	*Geänderter Text*
(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.	(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern ***oder ernsthafte Risiken für die öffentliche Sicherheit in mehreren Mitgliedstaaten oder der gesamten Union darstellen***. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren. ***Die Mitgliedstaaten müssen die Umsetzung der EU-Vorschriften überwachen, sich bei grenzübergreifenden Problemen gegenseitig unterstützen, einen strukturierteren Dialog mit der Privatwirtschaft einrichten und bei Sicherheitsrisiken und Bedrohungen im Zusammenhang mit den neuen Technologien zusammenarbeiten, wie dies auch beim Thema 5G der Fall war.***
[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für	[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für

eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Änderungsantrag 20

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.	(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale ***und sektorspezifische*** Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale ***und sektorspezifische*** Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.

Änderungsantrag 21

Vorschlag für eine Richtlinie
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe ***in Erwägung ziehen***, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, ***etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität***	(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe ***einschlägige***, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, ***insbesondere Europol***, die Agentur der Europäischen Union für Flugsicherheit

(EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit ***einzuladen***.

(EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit ***einladen***.

Änderungsantrag 22

Vorschlag für eine Richtlinie
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. ***Solche Übereinkünfte sollten einen angemessenen Datenschutz gewährleisten***.	(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. ***Soweit personenbezogene Daten an Drittländer oder an internationale Organisationen übermittelt werden, sollte Kapitel V der Verordnung (EU) 2016/679 Anwendung finden***.

Änderungsantrag 23

Vorschlag für eine Richtlinie
Erwägung 37

Vorschlag der Kommission	*Geänderter Text*
(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk	(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk

sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.	sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. ***Wenn die Krise zwei oder mehr Mitgliedstaaten betrifft und mutmaßlichen kriminellen Hintergrund hat, sollte die Aktivierung des Notfallprotokolls der EU für die Reaktion der Strafverfolgungsbehörden in Betracht gezogen werden.*** Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.

Änderungsantrag 24

Vorschlag für eine Richtlinie
Erwägung 45

Vorschlag der Kommission	*Geänderter Text*
(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten	(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten

die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.	die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen***, und potenzielle Cyberangriffe, die sie feststellen, melden***.

Änderungsantrag 25

Vorschlag für eine Richtlinie
Erwägung 46 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(46a) Besondere Aufmerksamkeit sollte dem Umstand gewidmet werden, dass IKT-Dienste, -Systeme oder -Produkte in ihrem Ursprungsland besonderen Anforderungen unterliegen, die ein Hindernis für die Einhaltung der EU-Rechtsvorschriften über die Privatsphäre und den Datenschutz darstellen könnten. Im Rahmen derartiger Risikobewertungen sollte gegebenenfalls der EDSA konsultiert werden. Freie und quelloffene Software sowie quelloffene Hardware könnten in Bezug auf die Cybersicherheit enorme Vorteile bieten, was die Transparenz und die Überprüfbarkeit von Merkmalen betrifft. Da dies dazu beitragen könnte, bestimmte Risiken in der Lieferkette anzugehen und zu mindern, sollte ihrer Verwendung nach Möglichkeit im Einklang mit der Stellungnahme 5/2021 des EDSB[1a]

Vorrang eingeräumt werden.

[1a] Stellungnahme 5/2021 des Europäischen Datenschutzbeauftragten zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie, 11. März 2021.

Änderungsantrag 26

Vorschlag für eine Richtlinie
Erwägung 47

Vorschlag der Kommission	*Geänderter Text*
(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, ***einschließlich derer***, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für	(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, ***die von der Koordinierungsgruppe näher festgelegt werden sollten und zu denen die Faktoren gehören***, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v)

die Tätigkeiten der Einrichtungen.	die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

Änderungsantrag 27

Vorschlag für eine Richtlinie
Erwägung 48 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(48a) Kleine und mittlere Unternehmen (KMU) sind oft nicht groß genug und verfügen nicht über genügend Ressourcen, um in einer vernetzten Welt, in der die Telearbeit zunimmt, eine breite und zunehmende Palette an Cybersicherheitsanforderungen zu erfüllen. Die Mitgliedstaaten sollten daher in ihren nationalen Cybersicherheitsstrategien Leitlinien und Unterstützung für KMU vorsehen.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Erwägung 50

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

erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.

elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.

Änderungsantrag 29

Vorschlag für eine Richtlinie
Erwägung 52

Vorschlag der Kommission	*Geänderter Text*
(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen sollte für die Empfänger kostenlos sein.	(52) Gegebenenfalls sollten die Einrichtungen ***in der Lage sein,*** die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen ***zu*** informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen sollte für die Empfänger kostenlos sein.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Erwägung 53

Vorschlag der Kommission	*Geänderter Text*
(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über	(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die ***Grundsätze der eingebauten Sicherheit und der Sicherheit durch Voreinstellungen***

Maßnahmen zum Schutz ***von Kommunikationsinhalten***, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.	***umsetzen und in der Lage sein, die*** Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz ***ihrer Geräte und Kommunikationsinhalte***, die sie treffen können, ***zu*** informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren. ***Um die Sicherheit der Hardware und Software zu erhöhen, sollten die Anbieter darin bestärkt werden, Open-Source-Hardware zu verwenden.***

Änderungsantrag 31

Vorschlag für eine Richtlinie
Erwägung 54

Vorschlag der Kommission	*Geänderter Text*
(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit ***den Befugnissen*** der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die ***Ermittlung***, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und	(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste ***und zum Schutz der Grundrechte auf Datenschutz und Schutz der Privatsphäre*** sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit ***der Zuständigkeit*** der Mitgliedstaaten ***dafür***, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die ***Verhütung***, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht ***und dem nationalen Recht*** zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit

zugleich eine wirksame Reaktion auf ***Straftaten gewährleisten***.

der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten***. Keine Bestimmung in dieser Verordnung sollte als Versuch, die End-zu-End-Verschlüsselung durch „Hintertüren“ oder ähnliche Lösungen zu schwächen, angesehen werden, da Mängel bei der Verschlüsselung für böswillige Zwecke ausgenutzt werden könnten. Jede Maßnahme mit dem Ziel, die Verschlüsselung zu schwächen oder die Architektur der Technologie zu umgehen, könnte erhebliche Risiken für die damit verbundenen wirksamen Schutzkapazitäten zur Folge haben. Jede unautorisierte Entschlüsselung oder Überwachung elektronischer Kommunikation, die nicht von Justizbehörden vorgenommen wird, sollte verboten werden, um die Wirksamkeit der Technologie*** und ***ihre umfassendere Nutzung sicherzustellen. Es ist wichtig, dass sich die Mitgliedstaaten mit Problemen befassen, mit denen Justizbehörden und Forscher, die sich mit Schwachstellen beschäftigen, konfrontiert sind. In einigen Mitgliedstaaten können Einrichtungen und natürliche Personen, die Forschung zu Schwachstellen betreiben, strafrechtlich und zivilrechtlich zur Verantwortung gezogen werden. Die Mitgliedstaaten werden daher aufgefordert, Leitlinien für den Verzicht auf Strafverfolgung und die Nichthaftung in Bezug auf Forschung im Bereich der Informationssicherheit herauszugeben.***

Änderungsantrag 32

Vorschlag für eine Richtlinie
Erwägung 56

Vorschlag der Kommission	*Geänderter Text*
(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter	(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter

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

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

Änderungsantrag 33

Vorschlag für eine Richtlinie
Erwägung 57

Vorschlag der Kommission	*Geänderter Text*
(57) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen – auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht – dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz	(57) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen – auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht – dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz

personenbezogener Daten ist gegebenenfalls die Unterstützung durch ***das*** EC3 und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

personenbezogener Daten ist gegebenenfalls die Unterstützung durch ***Europols Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (***EC3***)*** und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

Änderungsantrag 34

Vorschlag für eine Richtlinie
Erwägung 58

Vorschlag der Kommission	*Geänderter Text*
(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.	(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der ***Verordnung (EU) 2016/679 und der*** Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

Änderungsantrag 35

Vorschlag für eine Richtlinie
Erwägung 59

Vorschlag der Kommission	*Geänderter Text*
(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-	(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem

Datenschutzrecht im Einklang stehen.	***geltenden*** EU-Datenschutzrecht im Einklang stehen.

Änderungsantrag 36

Vorschlag für eine Richtlinie
Erwägung 62

Vorschlag der Kommission	*Geänderter Text*
(62) ***TLD-Register*** und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***sollten*** Domänennamen-Registrierungsdaten, die ***nicht*** den ***EU-Datenschutzvorschriften unterliegen, z. B. Daten***, ***die juristische Personen betreffen***[25]***,*** öffentlich zugänglich machen. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager ***rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen*** im Einklang mit ***dem EU-Datenschutzrecht*** erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, Anträge ***berechtigter Zugangsnachfrager*** auf Offenlegung von Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf	(62) ***Um eine rechtliche Verpflichtung im Sinne von Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 zu erfüllen, sollten TLD-Register*** und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***bestimmte*** Domänennamen-Registrierungsdaten, die ***in*** den ***für sie geltenden Rechtsvorschriften der Mitgliedstaaten festgelegt sind***, ***wie den Domänennamen und den Namen der juristischen Person*** öffentlich zugänglich machen. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager ***– insbesondere zuständige Behörden gemäß der vorliegenden Richtlinie oder Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679*** im Einklang mit ***ihren Befugnissen – rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen*** erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***rechtmäßige und hinreichend begründete*** Anträge ***von Behörden – einschließlich zuständiger Behörden gemäß dieser Richtlinie, nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständiger Behörden und Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 –*** auf

Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

Offenlegung von Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager ***auf Zugang***. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

---

[25] Erwägungsgrund 14 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.“

Änderungsantrag 37

Vorschlag für eine Richtlinie
Erwägung 63

Vorschlag der Kommission	*Geänderter Text*
(63) ***Alle*** wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, ***sollten*** der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste	(63) ***Für die Zwecke dieser Richtlinie sollten alle*** wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre

erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.

Dienste erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten ***sich auf einzelne Klassifizierungen einigen, nach Möglichkeit*** zusammenarbeiten, einander ***in Echtzeit*** Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.

Änderungsantrag 38

Vorschlag für eine Richtlinie
Erwägung 64

Vorschlag der Kommission	*Geänderter Text*
(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die ***gerichtliche Zuständigkeit*** sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige	(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. ***Für*** die ***Zwecke dieser Richtlinie*** sollte ***die gerichtliche Zuständigkeit*** bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger

Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

Änderungsantrag 39

Vorschlag für eine Richtlinie
Erwägung 69

Vorschlag der Kommission	*Geänderter Text*
(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***sollte im Sinne*** der Verordnung (EU) 2016/679 ein berechtigtes Interesse des jeweiligen Verantwortlichen ***darstellen, wie dies für die Gewährleistung*** der ***Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist***. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen,	(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***in dem Ausmaß, das für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, ist notwendig, damit sie ihre rechtlichen Verpflichtungen gemäß dem nationalen Recht zur Umsetzung dieser Richtlinie erfüllen und fällt somit unter Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3*** der Verordnung (EU) 2016/679***. Zudem sollte eine derartige Verarbeitung*** ein berechtigtes Interesse des jeweiligen Verantwortlichen ***im Sinne von Artikel 6 Absatz 1 Buchstabe f*** der

Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. ***Diese*** Maßnahmen können die Verarbeitung ***folgender Arten*** personenbezogener Daten erfordern***:*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

Verordnung (EU) 2016/679 darstellen. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. ***Häufig ist der Schutz personenbezogener Daten nach Cybersicherheitsvorfällen nicht mehr gewährleistet; deswegen sollten die zuständigen Behörden und die Datenschutzbehörden der EU-Mitgliedstaaten zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen, um sich mit jeglicher Verletzung des Schutzes personenbezogener Daten zu befassen. Die*** Maßnahmen können die Verarbeitung ***bestimmter Kategorien*** personenbezogener Daten erfordern***, einschließlich*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

Änderungsantrag 40

Vorschlag für eine Richtlinie
Erwägung 71

Vorschlag der Kommission	*Geänderter Text*
(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte	(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte

Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der ***Art,*** Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der ***Aufsichtsbehörde*** sowie jedem anderen erschwerenden oder mildernden Umstand. Für die ***Verhängung von*** Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, ***etwaigen relevanten vorherigen Verstößen, der Art und Weise, in der die zuständige Behörde von dem Verstoß Kenntnis erlangt hat,*** der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem ***relevanten*** früheren Verstoß, dem Umfang der Zusammenarbeit mit der ***zuständigen Behörde*** sowie jedem anderen erschwerenden oder mildernden Umstand. Für die ***verhängten*** Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

Änderungsantrag 41

Vorschlag für eine Richtlinie
Erwägung 74

Vorschlag der Kommission	*Geänderter Text*
(74) Die Mitgliedstaaten sollten die ***strafrechtlichen*** Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom	(74) Die Mitgliedstaaten sollten die ***Vorschriften über strafrechtliche*** Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können***. Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen***. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen

Gerichtshof ausgelegt worden ist, führen.

Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.

Änderungsantrag 42

Vorschlag für eine Richtlinie
Erwägung 76

Vorschlag der Kommission	*Geänderter Text*
(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen ***und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen***. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen,	(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil ***der*** oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene

erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf ***wirksamen Rechtsschutz*** und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf ***wirksame gerichtliche Rechtsbehelfe*** und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Änderungsantrag 43

Vorschlag für eine Richtlinie
Erwägung 77

Vorschlag der Kommission	*Geänderter Text*
(77) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße im Zusammenhang mit personenbezogenen Daten vorzugehen.	(77) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden ***gemäß der vorliegenden Richtlinie*** und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße im Zusammenhang mit personenbezogenen Daten vorzugehen.

Änderungsantrag 44

Vorschlag für eine Richtlinie
Erwägung 79

Vorschlag der Kommission	*Geänderter Text*
(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen.	(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen. ***Die EU sollte eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen ermöglichen und Unterstützung anbieten, um zur Erholung nach***

entsprechenden Cyberangriffen beizutragen.

Änderungsantrag 45

Vorschlag für eine Richtlinie
Erwägung 82 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(82a) Die vorliegende Richtlinie gilt nicht für die Organe, Einrichtungen und sonstigen Stellen der Union. Allerdings können Einrichtungen der Union als wesentliche oder wichtige Einrichtungen gemäß dieser Richtlinie angesehen werden. Damit durch kohärente und einheitliche Vorschriften ein einheitliches Schutzniveau erreicht wird, sollte die Kommission einen Legislativvorschlag veröffentlichen, um die Organe, Einrichtungen und sonstigen Stellen der Union bis zum 31. Dezember 2022 in den unionsweiten Cybersicherheitsrahmen zu integrieren.

Änderungsantrag 46

Vorschlag für eine Richtlinie
Erwägung 84

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

	geltenden Rechtsvorschriften der Union zur Regelung dieser Angelegenheiten umgesetzt werden***. Jede Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie erfolgt im Einklang mit der Verordnung (EU) 2016/679 bzw. der Richtlinie 2002/58/EG entsprechend ihren jeweiligen Anwendungsbereichen, unter anderem im Hinblick auf die Aufgaben und Befugnisse der Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Rechtsakte zuständig sind —***

Änderungsantrag 47

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[28] angesehen werden.	(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[28] angesehen werden. ***Artikel 3 Absatz 4 des Anhangs der Empfehlung 2003/361/EG der Kommission findet keine Anwendung.***
[28] 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).	[28] 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).

Änderungsantrag 48

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn	(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie ***auf der Grundlage einer Risikobewertung nach Artikel 18*** jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn

Änderungsantrag 49

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) es sich bei der Einrichtung um den einzigen Anbieter eines Dienstes ***in einem Mitgliedstaat*** handelt;	c) es sich bei der Einrichtung um den einzigen Anbieter eines Dienstes ***auf nationaler oder regionaler Ebene*** handelt;

Änderungsantrag 50

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe d

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

Änderungsantrag 51

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe e

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

Änderungsantrag 52

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Jede Verarbeitung personenbezogener Daten gemäß dieser Richtlinie muss im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG erfolgen und auf das für die Zwecke dieser Richtlinie unbedingt erforderliche und verhältnismäßige Maß beschränkt sein.

Änderungsantrag 53

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs ***relevanten und angemessenen*** Umfang beschränkt. Beim Informationsaustausch ***werden*** die Vertraulichkeit der Informationen gewahrt ***sowie*** die Sicherheit und die geschäftlichen Interessen wesentlicher oder wichtiger Einrichtungen geschützt.	(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs ***notwendigen*** Umfang beschränkt. Beim Informationsaustausch ***wird*** die Vertraulichkeit der Informationen gewahrt***,*** ***und*** die Sicherheit und die geschäftlichen Interessen wesentlicher oder wichtiger Einrichtungen ***werden dabei*** geschützt.

Änderungsantrag 54

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Damit durch kohärente und einheitliche Vorschriften ein einheitliches Schutzniveau erreicht wird, veröffentlicht die Kommission vor dem 31. Dezember 2021 einen Legislativvorschlag, um die Organe, Einrichtungen und sonstigen Stellen der Union in den allgemeinen unionsweiten Cybersicherheitsrahmen zu integrieren.

Änderungsantrag 55

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder	b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, ***in das IT-System integriert sind und für die Bereitstellung der Dienste genutzt werden, für die sie vorgesehen sind,*** oder

Änderungsantrag 56

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die ***Sicherheit von Netz- und Informationssystemen*** in diesem Mitgliedstaat;	4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die ***Cybersicherheit*** in diesem Mitgliedstaat;

Änderungsantrag 57

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 12

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

Änderungsantrag 58

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 22

Vorschlag der Kommission	*Geänderter Text*
22. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;	***entfällt***

Änderungsantrag 59

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 24

Vorschlag der Kommission	*Geänderter Text*
24. „Einrichtung“ jede natürliche Person oder jede nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in	*(Betrifft nicht die deutsche Fassung.)*

eigenem Namen Rechte ausüben und Pflichten unterliegen kann;

Änderungsantrag 60

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten;	a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten ***unter Berücksichtigung des allgemeinen Grads des Cybersicherheitsbewusstseins der Bürgerinnen und Bürger sowie des allgemeinen Sicherheitsniveaus bei vernetzten Geräten der Verbraucherinnen und Verbraucher***;

Änderungsantrag 61

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38] für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.	f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38]***, sowohl in als auch zwischen den Mitgliedstaaten,*** für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.
[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 62

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;	b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge***, unter anderem einschließlich Verschlüsselungsanforderungen und der Förderung der Verwendung von Open-Source-Cybersicherheitsprodukten***;

Änderungsantrag 63

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d a (neu)

Vorschlag der Kommission	*Geänderter Text*
	da) ein Konzept in Bezug auf die Aufrechterhaltung der Nutzung offener Daten und von Open-Source-Produkten im Rahmen der Sicherheit durch Transparenz;

Änderungsantrag 64

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d b (neu)

Vorschlag der Kommission	*Geänderter Text*
	db) ein Konzept zur Förderung des Schutzes und der Sicherheit personenbezogener Daten von Nutzern von Online-Diensten;

Änderungsantrag 65

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen;	e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen***, einschließlich der Entwicklung von Schulungsprogrammen zur Cybersicherheit mit dem Ziel, dafür zu sorgen, dass Einrichtungen Spezialisten und Techniker zur Verfügung stehen***;

Änderungsantrag 66

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen ***bei*** der ***Entwicklung von Cybersicherheitsinstrumenten*** und ***sicherer*** Netzinfrastruktur;	f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen***, die zu*** der ***nationalen Cybersicherheitsstrategie beitragen, indem sie Cybersicherheitsinstrumente*** und ***eine sichere*** Netzinfrastruktur ***entwickeln und bereitstellen, mit denen zu der nationalen Cybersicherheitsstrategie beigetragen wird, einschließlich spezifischer Konzepte zu Angelegenheiten im Zusammenhang mit der Vertretung und einem ausgewogenen Verhältnis von Frauen und Männern in diesem Bereich***;

Änderungsantrag 67

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen	h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen

sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.

sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen ***und ihrer Fähigkeit zur Reaktion auf Cybersicherheitsvorfälle*** bietet.

Änderungsantrag 68

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.	(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können. ***Um dafür zu sorgen, dass die in dem Register enthaltenen Informationen sicher und zugänglich sind, wendet die ENISA dem Stand der Technik entsprechende Sicherheitsmaßnahmen an und stellt die Informationen über entsprechende Schnittstellen in maschinenlesbaren Formaten zur***

	Verfügung.

Änderungsantrag 69

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) die Ziele der nationalen ***Vorsorgenmaßnahmen*** und -tätigkeiten;	a) die Ziele der nationalen ***und, soweit zutreffend und anwendbar, regionalen und grenzübergreifenden Vorsorgemaßnahmen*** und -tätigkeiten;

Änderungsantrag 70

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) auf Ersuchen einer Einrichtung Durchführung einer ***proaktiven Überprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Netz-*** und ***Informationssysteme*** auf ***Schwachstellen (Schwachstellenscan);***	e) auf Ersuchen einer Einrichtung Durchführung einer ***Sicherheitsüberprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Informationssysteme*** und ***Netzbereiche, um spezifische Bedrohungen zu erkennen, abzuschwächen oder zu verhindern; die Verarbeitung personenbezogener Daten im Zusammenhang mit einer solchen Überprüfung ist auf das unbedingt erforderliche Maß beschränkt, in jedem Fall jedoch auf IP- und URL-Adressen***

Änderungsantrag 71

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten	(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten

erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.	erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden ***im Einklang mit ihren jeweiligen Zuständigkeiten***.
[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 72

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.	(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig ***und rechtzeitig*** über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.

Änderungsantrag 73

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst ***nimmt*** an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.	(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst***, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol und der Europäische Datenschutzausschuss nehmen*** an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.

Änderungsantrag 74

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger ***einladen,*** an ihren Arbeiten ***teilzunehmen***.	***Wenn dies für die Erfüllung ihrer Aufgaben von Bedeutung ist, lädt*** die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger ***zur Teilnahme*** an ihren Arbeiten ***und das Europäische Parlament zur Teilnahme als Beobachter ein***.

Änderungsantrag 75

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 8

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

Änderungsantrag 76

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Das CSIRT-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission ***nimmt*** als ***Beobachterin*** am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.	(2) Das CSIRT-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission ***und das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol nehmen*** als ***Beobachter*** am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.

Änderungsantrag 77

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch.	(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ***Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol nimmt als Beobachter an den Tätigkeiten von EU-CyCLONe teil.*** ENISA führt die Sekretariatsgeschäfte des

Netzwerks und unterstützt den sicheren Informationsaustausch.

Änderungsantrag 78

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk zusammen.	(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk ***und mit Strafverfolgungsbehörden im Rahmen des Notfallprotokolls der EU für die Reaktion der Strafverfolgungsbehörden*** zusammen.

Änderungsantrag 79

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen ***zweijährlichen Bericht*** über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:	(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen ***Jahresbericht*** über den Stand der Cybersicherheit in der Union. Dieser Bericht muss ***in einem maschinenlesbaren Format erstellt werden und*** insbesondere Folgendes enthalten:

Änderungsantrag 80

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) die Auswirkungen von Cybersicherheitsvorfällen auf den Schutz personenbezogener Daten in der Union.

Änderungsantrag 81

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c b (neu)

Vorschlag der Kommission	*Geänderter Text*
	cb) einen Überblick über den allgemeinen Grad der Sensibilisierung der Bürger für das Thema Cybersicherheit und das entsprechende Verhalten der Bürger sowie über das allgemeine Sicherheitsniveau verbraucherorientierter vernetzter Geräte, die in der Union in Verkehr gebracht werden.

Änderungsantrag 82

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben.	(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane ***und die zuständigen Sachverständigen für Cybersicherheit*** regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von ***sich wandelnden*** Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben.

Änderungsantrag 83

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um

die Risiken für die ***Sicherheit*** der Netz- und Informationssysteme, die ***diese Einrichtungen bei der*** Erbringung ihrer Dienste ***nutzen***, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein ***Sicherheitsniveau*** der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.	***mit Blick auf*** die ***Sicherstellung der Kontinuität dieser Dienste und die Minderung der*** Risiken für die ***Rechte von Einzelpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Risiken für die Cybersicherheit*** der Netz- und Informationssysteme, die ***für die*** Erbringung ihrer Dienste ***genutzt werden***, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein ***Cybersicherheitsniveau*** der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Änderungsantrag 84

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Einsatz von Kryptografie und Verschlüsselung.	g) Einsatz von Kryptografie und ***einer starken*** Verschlüsselung.

Änderungsantrag 85

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.	(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter ***und verhältnismäßiger*** Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen. ***Die zuständigen Behörden stellen den Einrichtungen Orientierungshilfen für die praktische und verhältnismäßige Anwendung zur Verfügung.***

Änderungsantrag 86

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Die Mitgliedstaaten räumen dem Nutzer eines von einer wesentlichen oder wichtigen Einrichtung bereitgestellten Netz- und Informationssystems das Recht ein, von der Einrichtung Informationen über die technischen und organisatorischen Maßnahmen zu erhalten, die getroffen wurden, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu bewältigen. Die Mitgliedstaaten legen die Beschränkungen für dieses Recht fest.

Änderungsantrag 87

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Kooperationsgruppe ***kann*** in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren ***durchführen***.	(1) Die Kooperationsgruppe ***führt*** in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren ***durch***.

Änderungsantrag 88

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige

Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat***. Gegebenenfalls unterrichten*** diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.	Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich***, in jedem Fall aber innerhalb von 24 Stunden,*** jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat***, sowie den zuständigen Strafverfolgungsbehörden, wenn der Vorfall mutmaßlich oder bekanntermaßen böswilliger Natur ist.*** Diese Einrichtungen ***unterrichten*** die Empfänger ihrer Dienste unverzüglich***, in jedem Fall aber innerhalb von 24 Stunden,*** über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten***, und stellen Informationen bereit, die es ihnen ermöglichen würden, die nachteiligen Auswirkungen der Cyberangriffe abzumildern. In Ausnahmefällen, wenn die Offenlegung weitere Cyberangriffe auslösen könnte, können diese Einrichtungen die Unterrichtung verzögern***. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

Änderungsantrag 89

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT ***unverzüglich*** jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.	(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen ***in der Lage sind,*** den zuständigen Behörden oder dem CSIRT jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung ***zu*** melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.

Änderungsantrag 90

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls ***unterrichten*** diese Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste ***unverzüglich*** über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. ***Die Einrichtungen*** informieren diese Empfänger ***gegebenenfalls*** auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.	Gegebenenfalls ***erhalten*** diese Einrichtungen ***die Möglichkeit,*** die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste über alle Maßnahmen oder Abhilfemaßnahmen ***zu unterrichten***, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. ***Wenn eine derartige Meldung erfolgt,*** informieren ***die Einrichtungen*** diese Empfänger auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.

Änderungsantrag 91

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Einleitung

Vorschlag der Kommission	*Geänderter Text*
c) spätestens einen Monat nach Vorlage des Berichts gemäß Buchstabe a einen ***Abschlussbericht***, der mindestens Folgendes enthält:	c) spätestens einen Monat nach Vorlage des Berichts gemäß Buchstabe a einen ***umfassenden Bericht***, der mindestens Folgendes enthält:

Änderungsantrag 92

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Ziffer ii

Vorschlag der Kommission	*Geänderter Text*
ii) Angaben zur Art der ***Bedrohung*** bzw. zugrunde liegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;	ii) Angaben zur Art der ***Cyberbedrohung*** bzw. zugrunde liegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;

Änderungsantrag 93

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Ziffer iii

Vorschlag der Kommission	*Geänderter Text*
iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.	iii) Angaben zu den getroffenen und laufenden ***Minderungs- oder*** Abhilfemaßnahmen.

Änderungsantrag 94

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.	(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall. ***Wenn der Vorfall zwei oder mehr Mitgliedstaaten betrifft und mutmaßlichen kriminellen Hintergrund hat, unterrichtet die zuständige Behörde oder das CSIRT EUROPOL.*** Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

Änderungsantrag 95

Vorschlag für eine Richtlinie
Artikel 22 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) ***In*** Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten.	(2) ***Nach Abstimmung mit dem EDSA und in*** Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten –, mit denen diese Bereiche abgedeckt werden könnten.

Änderungsantrag 96

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die ***TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen***, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank ***sammeln und pflegen, wobei die*** Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten ***mit der gebotenen Sorgfalt zu beachten sind***.	(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die ***TLD über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird***, ***dass*** genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank ***im Einklang mit den*** Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten ***gesammelt und gepflegt werden. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.***

Änderungsantrag 97

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-	(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-

Registrierungsdaten ***einschlägige*** Angaben enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.	Registrierungsdaten ***die erforderlichen*** Angaben***, nämlich Name, Anschrift, E-Mail-Adresse und Telefonnummer,*** enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.

Änderungsantrag 98

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 3

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

Begründung

Dieser Absatz wurde in Artikel 23 Absatz 1 eingefügt.

Änderungsantrag 99

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, unverzüglich nach der Registrierung eines Domänennamens ***die nicht personenbezogenen***	(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, ***gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679*** unverzüglich

Domänenregistrierungsdaten veröffentlichen.	nach der Registrierung eines Domänennamens ***bestimmte Domänennamen-Registrierungsdaten*** veröffentlichen***, etwa den Domänennamen und den Namen der juristischen Person***.

Änderungsantrag 100

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge ***berechtigten Zugangsnachfragern*** im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.	(5) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge ***von Behörden, einschließlich zuständiger Behörden gemäß dieser Richtlinie, Behörden, die nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständig sind, oder Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679,*** im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle ***rechtmäßigen und hinreichend begründeten*** Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Änderungsantrag 101

Vorschlag für eine Richtlinie
Artikel 24 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. ***Es*** gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.	(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. ***Unbeschadet der Zuständigkeiten der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679*** gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.

Änderungsantrag 102

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:	(1) Die ENISA erstellt und pflegt ein ***sicheres*** Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:

Änderungsantrag 103

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Unbeschadet der Verordnung	(1) Unbeschadet der Verordnung

(EU) 2016/679 stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, sofern	(EU) 2016/679 ***oder der Richtlinie 2002/58/EG*** stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools ***sowie den Aufenthaltsort oder die Identität des Angreifers***, sofern

Änderungsantrag 104

Vorschlag für eine Richtlinie
Artikel 28 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) ***Bei*** der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, ***arbeiten die zuständigen Behörden*** eng mit den ***Datenschutzbehörden*** zusammen.	(2) ***Unbeschadet der Zuständigkeiten, Aufgaben und Befugnisse der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 arbeiten die zuständigen Behörden bei*** der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den ***Aufsichtsbehörden*** zusammen. ***Zu diesem Zweck tauschen die zuständigen Behörden und Aufsichtsbehörden Informationen aus, die für ihren jeweiligen Zuständigkeitsbereich relevant sind. Darüber hinaus stellen die zuständigen Behörden den zuständigen Aufsichtsbehörden auf Verlangen alle Informationen zur Verfügung, die sie im Rahmen von Prüfungen und Untersuchungen im Zusammenhang mit der Verarbeitung personenbezogener Daten erhalten haben.***

Änderungsantrag 105

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 4 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;	***entfällt***

Änderungsantrag 106

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Buchstabe b

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

Änderungsantrag 107

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Diese ***Sanktionen werden*** nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen	Diese ***Sanktion wird*** nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen

verhängt wurden, zu erfüllen.	verhängt wurden, zu erfüllen.

Änderungsantrag 108

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c

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

Änderungsantrag 109

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) alle einschlägigen früheren Verstöße der betroffenen Einrichtung;

Änderungsantrag 110

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c b (neu)

Vorschlag der Kommission	*Geänderter Text*
	cb) die Art und Weise, wie der Verstoß der zuständigen Behörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die Einrichtung den Verstoß gemeldet hat;

Änderungsantrag 111

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Umfang der Zusammenarbeit ***der verantwortlichen natürlichen oder juristischen Person(en)*** mit den zuständigen Behörden***.***	g) Umfang der Zusammenarbeit mit den zuständigen Behörden***, um dem Verstoß abzuhelfen und mögliche nachteilige Auswirkungen der Verstöße zu mindern;***

Änderungsantrag 112

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe g a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ga) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Änderungsantrag 113

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 9

Vorschlag der Kommission	*Geänderter Text*
(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***des betreffenden Mitgliedstaats***, die gemäß	(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***aller Mitgliedstaaten***, die gemäß der

der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.	Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, ***in Echtzeit*** unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.

Änderungsantrag 114

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung ihrer in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;	***entfällt***

Änderungsantrag 115

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) ***und natürliche(n)*** Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;	h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;

Änderungsantrag 116

Vorschlag für eine Richtlinie
Artikel 31 – Absatz 2

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

Änderungsantrag 117

Vorschlag für eine Richtlinie
Artikel 31 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) ***Bei der Entscheidung über die Verhängung einer*** Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.	(3) ***Ob eine*** Geldbuße ***verhängt wird, hängt von den Umständen des Einzelfalls ab,*** und ***bei der Entscheidung über*** deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

Änderungsantrag 118

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung	(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung

zuständigen Aufsichtsbehörden ***innerhalb einer angemessenen Frist***.	zuständigen Aufsichtsbehörden ***unverzüglich und in jedem Fall innerhalb von 24 Stunden***.

Änderungsantrag 119

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 3

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

Änderungsantrag 120

Vorschlag für eine Richtlinie
Artikel 34 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 34 a
	Haftung bei Nichteinhaltung
	Unbeschadet verfügbarer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe haben Empfänger von durch wesentliche oder wichtige Einrichtungen bereitgestellten Diensten, denen aufgrund von Verstößen des Anbieters gegen diese Richtlinie Schäden entstanden sind, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf.

Änderungsantrag 121

Vorschlag für eine Richtlinie
Artikel 35 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Kommission überprüft ***regelmäßig*** die	Die Kommission überprüft ***alle drei Jahre***

Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit ***bewertet***. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … ***54*** Monate nach Inkrafttreten dieser Richtlinie vorzulegen.	die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere ***bewertet, inwieweit die Richtlinie dazu beigetragen hat, ein hohes gemeinsames Maß an Sicherheit und Integrität von Netz- und Informationssystemen sicherzustellen und gleichzeitig das Privatleben und personenbezogene Daten bestmöglich zu schützen, sowie*** die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … ***[36*** Monate nach Inkrafttreten dieser Richtlinie***]*** vorzulegen.

Änderungsantrag 122

Vorschlag für eine Richtlinie
Anhang I – Nummer 5 (Gesundheitswesen) – Spiegelstrich 6 (neu)

Vorschlag der Kommission

Sektor	Teilsektor	Art der Einrichtung
5. Gesundheitswesen		– Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU[90]
		– EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren[91]
		– Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG ausüben[92]
		– Einrichtungen, die pharmazeutische

		Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen – Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 20 der Verordnung XXXX[93] („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

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

[92] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).

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

Geänderter Text

Sektor	Teilsektor	Art der Einrichtung
5. Gesundheitswesen		– Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU[90] – EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren[91] – Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG ausüben[92] – Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen – Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 20 der Verordnung XXXX[93] („Liste

kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

– Einrichtungen, die eine Großhandelsgenehmigung im Sinne des Artikels 79 der Richtlinie 2001/83/EG aufweisen

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

[92] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).

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

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und Aufhebung der Richtlinie (EU) 2016/1148
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021
Stellungnahme von Datum der Bekanntgabe im Plenum	LIBE 21.1.2021
Assoziierte Ausschüsse - Datum der Bekanntgabe im Plenum	20.5.2021
Verfasser(in) der Stellungnahme Datum der Benennung	Lukas Mandl 12.4.2021
Prüfung im Ausschuss	16.6.2021 3.9.2021 11.10.2021
Datum der Annahme	12.10.2021
Ergebnis der Schlussabstimmung	+: 44 –: 14 0: 4
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Erläuterungen:
+ : dafür
- : dagegen
0 : Enthaltung