Gemeinsame Stellungnahme [4/2026] des EDSA und des EDSB

zu dem Vorschlag für eine Cybersicherheitsverordnung 2 und zu dem Vorschlag zur Änderung der NIS-2-Richtlinie

Angenommen am 18. März 2026

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Inhaltsverzeichnis

1 Hintergrund 5

2 Allgemeine Bemerkungen 6

3 Unterstützung der Umsetzung der Unionspolitik und des Unionsrechts durch die ENISA sowie Zusammenarbeit mit anderen Einrichtungen der Union 7

4 Operative Zusammenarbeit, gemeinsame Lageerfassung im Bereich der Cybersicherheit und Schutz personenbezogener Daten 8

5 Zentrale Anlaufstelle für die Meldung von Vorfällen (Artikel 15 CSA2) 11

6 Europäischer Kompetenzrahmen für Cybersicherheit (ECSF) (Artikel 19 CSA2) 11

7 Europäischer Zertifizierungsrahmen für die Cybersicherheit (Titel III) 13

8 Rahmen für vertrauenswürdige IKT-Lieferketten (Titel IV) 15

9 Zusätzliche wesentliche Einrichtungen im Rahmen des NIS-2-Vorschlags 15

10 Erhebung von Daten über Ransomware-Angriffe 16

Zusammenfassung

Am 20. Januar 2026 legte die Europäische Kommission einen Vorschlag für eine Verordnung über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2) sowie einen Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2] vor. Am 21. Januar 2026 konsultierte die Kommission den EDSA und den EDSB gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 förmlich.

Der EDSA und der EDSB erinnern daran, dass das Verhältnis zwischen Datenschutz und Cybersicherheit zwei Seiten hat. Einerseits dient die Cybersicherheit dem Schutz personenbezogener Daten, weil damit die Risiken des unerwünschten Zugriffs, der Veränderung oder der Nichtverfügbarkeit dieser Daten begrenzt werden. Andererseits können einige Cybersicherheitsmaßnahmen die Rechte und Freiheiten des Einzelnen beeinträchtigen, insbesondere das Recht auf Privatsphäre und Datenschutz. Daher müssen, auch wenn der Fokus von Cybersicherheitsmaßnahmen auf ihrer Wirksamkeit liegt, die Notwendigkeit und Verhältnismäßigkeit solcher Maßnahmen gleichfalls berücksichtigt werden.

Der EDSA und der EDSB unterstützen das allgemeine Ziel der Vorschläge, die Rolle der ENISA zu stärken und die Nutzung der Cybersicherheitszertifizierung zu fördern, jeweils vorbehaltlich der in dieser gemeinsamen Stellungnahme dargelegten spezifischen Empfehlungen. Sie begrüßen auch das Ziel, in der Richtlinie (EU) 2022/2555 Mechanismen und Bedingungen festzulegen, die dazu beitragen, die Einhaltung der Cybersicherheitsanforderungen zu erleichtern und so ihre Umsetzung kohärenter und wirksamer zu gestalten, sowie das Ziel, die verschiedenen Risiken für die IKT-Lieferketten, einschließlich der nichttechnischen Risiken, weiter anzugehen. Der EDSA und der EDSB unterstützen auch nachdrücklich das Ziel der Einrichtung einer zentralen Anlaufstelle für die Meldung von Verletzungen des Schutzes personenbezogener Daten, da dies den Verwaltungsaufwand für Organisationen verringern würde, ohne das Schutzniveau für die betroffenen Personen zu beeinträchtigen.

Der EDSA und der EDSB begrüßen ferner, dass der Vorschlag für die Cybersicherheitsverordnung 2 (im Folgenden „CSA2-Vorschlag“) weitere Klarstellungen zu den Modalitäten der Unterstützung verschiedener Interessenträger durch die ENISA enthalten würde, und empfehlen, auch den EDSB als Stelle aufzunehmen, die die ENISA um Beratung ersuchen kann. Der EDSA und der EDSB unterstützen nachdrücklich, dass eine solche Beratung nur auf Ersuchen erfolgen würde, da dies eine klare Koordinierung und eine eindeutige Abgrenzung der Zuständigkeiten gewährleistet.

Was die Zusammenarbeit zwischen der ENISA und anderen Einrichtungen der Union im Allgemeinen betrifft, so begrüßen der EDSA und der EDSB die Synergien, die sich aus einer solchen Zusammenarbeit im Einklang mit den jeweiligen Aufgaben und Mandaten ergeben können. Sie empfehlen, ausdrücklich auch den EDSB als Einrichtung der Union zu nennen, mit der die ENISA zusammenarbeiten würde.

Der EDSA und der EDSB sind der Auffassung, dass für den Fall, dass die künftigen Aufgaben der ENISA als Informationsdrehscheibe die Verarbeitung personenbezogener Daten in erheblichem Umfang erfordern, dies in den Bestimmungen des Basisrechtsakts, der die jeweiligen Aufgaben regelt, ausdrücklich festgelegt werden müsste, einschließlich der wesentlichen Elemente einer etwaigen Verarbeitung in großem Umfang und der entsprechenden Schutzvorkehrungen. Falls hingegen das Ziel darin besteht, der ENISA vor allem die Erhebung und Weiterverarbeitung vorwiegend aggregierter, nicht-personenbezogener Daten zu ermöglichen, so sollte dies ebenfalls klargestellt werden.

Der EDSA und der EDSB erinnern daran, dass grundsätzlich nur Entscheidungen über sehr technische (praktische) Einzelheiten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der Verwaltungsautonomie der betreffenden EU-Einrichtung (in diesem Fall des Verwaltungsrats einer dezentralen Agentur) überlassen bleiben sollten. Darüber hinaus empfehlen der EDSA und der EDSB, in Artikel 66 des CSA2-Vorschlags vorzusehen, dass der EDSB vor der Annahme solcher Vorschriften zu konsultieren ist.

In Bezug auf den Europäischen Kompetenzrahmen für Cybersicherheit (European Cybersecurity Skills Framework, ECSF) empfehlen der EDSA und der EDSB den beiden gesetzgebenden Organen, Artikel 19 Absatz 2 des CSA2-Vorschlags dahin gehend zu ändern, dass der ECSF nicht ausschließlich auf „Cybersicherheitsfachkräfte“ beschränkt ist, sondern auch Profile für die allgemeine Belegschaft umfasst.

Was den Europäischen Rahmen für die Cybersicherheitszertifizierung betrifft, so empfehlen der EDSA und der EDSB, den Anwendungsbereich des Artikels 80 Absatz 1 Buchstabe w CSA2 und das Verhältnis zur DSGVO-Zertifizierung weiter zu präzisieren. Darüber hinaus empfehlen der EDSA und der EDSB, die ENISA zu verpflichten, vor der Annahme eines Zertifizierungssystems nach Artikel 80 Absatz 1 Buchstabe w CSA2 den EDSA zu konsultieren, damit für Kohärenz gesorgt wird.

Der EDSA und der EDSB betonen, dass nicht nur die Wirksamkeit von Cybersicherheitsmaßnahmen, sondern auch deren Notwendigkeit und Verhältnismäßigkeit berücksichtigt werden müssen. Der EDSA und der EDSB empfehlen, klarzustellen, dass Zertifizierungssysteme so weit wie möglich Sicherheitskontrollen umfassen sollten, die dazu beitragen können, die Erfüllung der Anforderungen der DSGVO nachzuweisen, insbesondere wenn die Systeme für IKT-Produkte, ¬Dienste oder ¬Prozesse und für verwaltete Sicherheitsdienste gelten, die bei Datenverarbeitungsvorgängen wahrscheinlich verwendet werden.

Der EDSA und der EDSB begrüßen ferner die vorgeschlagene Maßnahme, mit der ein vertrauenswürdiger Rahmen für die IKT-Lieferkette sichergestellt und nichttechnische Risiken in Sektoren mit hoher Kritikalität angegangen werden sollen.

In Bezug auf den Vorschlag zur Änderung der NIS-2-Richtlinie begrüßen der EDSA und der EDSB die Einstufung der Anbieter europäischer Brieftaschen für die digitale Identität und europäischer Brieftaschen für Unternehmen als „wesentliche Einrichtungen“ und unterstützen uneingeschränkt das wichtige Ziel, künftige Ransomware-Angriffe zu verhindern und die dahinter stehenden kriminellen Organisationen zu stören und zu zerschlagen.

Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte —

gestützt auf Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG,

haben folgende gemeinsame Stellungnahme (im Folgenden „Stellungnahme“) angenommen:

1 HINTERGRUND

1. Am 20. Januar 2026 veröffentlichte die Europäische Kommission (im Folgenden „Kommission“) einen Vorschlag für eine Verordnung über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)[1] und einen Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2][2] (im Folgenden „CSA2-Vorschlag“, „Vorschlag zur Änderung der NIS-2-Richtlinie“ und zusammen „Vorschläge“). Am 21. Januar 2026 konsultierte die Kommission den EDSA und den EDSB gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 (im Folgenden „EU-DSVO“) förmlich[3].
2. Mit dem CSA2-Vorschlag soll der geltende Rechtsakt zur Cybersicherheit[4] ersetzt werden, um 1) die Rolle der ENISA zu stärken, wobei der Schwerpunkt auf den Bedürfnissen der Interessenträger angesichts einer zunehmend feindseligen Bedrohungslage liegt, 2) die Umsetzung des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF) wieder in Gang zu bringen, 3) die Komplexität und Vielfalt der Cybersicherheitsstrategien zu verringern und 4) Sicherheitsrisiken in den IKT-Lieferketten weiter anzugehen[5].
3. Der Vorschlag zur Änderung der NIS-2-Richtlinie befasst sich insbesondere mit dem dritten Ziel, indem Klarstellungen eingeführt werden und die Einhaltung für beaufsichtigte Unternehmen erleichtert werden soll[6].

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).
[4] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj) in der durch die Verordnung (EU) 2025/37 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste (Text von Bedeutung für den EWR) geänderten Fassung (ABl. L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] Begründung, COM(2026) 11 final, S. 1.
[6] COM(2026) 13 final.

4. Ziel dieser gemeinsamen Stellungnahme ist es, auf die einschlägigen Aspekte der Vorschläge einzugehen, die für den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten von besonderer Bedeutung sind.

2 ALLGEMEINE BEMERKUNGEN

5. Der CSA2-Vorschlag zielt darauf ab, das Mandat der ENISA zu erweitern und ihre Funktionsfähigkeit zu stärken. Der EDSA und der EDSB befürworten die Stärkung der Rolle der ENISA und das Ziel, die Nutzung der Cybersicherheitszertifizierung zu fördern, jeweils vorbehaltlich der nachstehenden spezifischen Empfehlungen.

6. Der EDSA und der EDSB begrüßen außerdem das Ziel, in der Richtlinie (EU) 2022/2555[7] (im Folgenden „NIS-2-Richtlinie“) Mechanismen und Bedingungen festzulegen, um die Einhaltung der Cybersicherheitsanforderungen zu erleichtern und so ihre Umsetzung kohärenter und wirksamer zu gestalten, sowie das Ziel, die verschiedenen Risiken für die IKT-Lieferketten, einschließlich nichttechnischer Risiken, weiter anzugehen.

7. Wie bereits in ihrer gemeinsamen Stellungnahme zum Digital-Omnibus-Vorschlag[8] dargelegt, unterstützen der EDSA und der EDSB nachdrücklich das Ziel der Einrichtung einer zentralen Anlaufstelle für die Meldung von Verletzungen des Schutzes personenbezogener Daten, da dies den Verwaltungsaufwand für Organisationen verringern würde, ohne das Schutzniveau für die betroffenen Personen zu beeinträchtigen.

8. Nach Artikel 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 (DSGVO) ist die Sicherheit einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten. In Artikel 32 DSGVO wird diese Verpflichtung, die sowohl für Verantwortliche als auch für Auftragsverarbeiter gilt, weiter ausgeführt, um ein angemessenes Maß an Sicherheit zu gewährleisten. Aus beiden Bestimmungen geht eindeutig hervor, dass die Sicherheit der Verarbeitung personenbezogener Daten für die Einhaltung des EU-Datenschutzrechts von wesentlicher Bedeutung ist.

9. Das Verhältnis zwischen Datenschutz und Cybersicherheit hat zwei Seiten. Einerseits dient die Cybersicherheit dem Schutz personenbezogener Daten, weil damit die Risiken des unerwünschten Zugriffs, der Veränderung oder der Nichtverfügbarkeit dieser Daten begrenzt werden. Andererseits können einige Cybersicherheitsmaßnahmen die Rechte und Freiheiten des Einzelnen beeinträchtigen, insbesondere das Recht auf Privatsphäre und Datenschutz[9].

[7] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).
[8] Gemeinsame Stellungnahme 2/2026 des EDSA und des EDSB zu dem Vorschlag für eine Verordnung hinsichtlich der Vereinfachung des digitalen Rechtsrahmens (Digital-Omnibus-Verordnung), angenommen am 10. Februar 2026.
[9] Vgl. EDSB, Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie, 11. März 2021, Rn. 10 und 11; EDSB, Stellungnahme 7/2022 zu dem Vorschlag für eine Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union, 17. Mai 2022, Rn. 9 und 10; EDSB, Stellungnahme 2/2024 zum Vorschlag für eine Verordnung zur Änderung des Gesetzes über die Cybersicherheit in Bezug auf verwaltete Sicherheitsdienste, 10. Januar 2024, Rn. 5.

10. Der EDSA und der EDSB erinnern daran, dass in Erwägungsgrund 49 der DSGVO anerkannt wird, dass Cybersicherheitsmaßnahmen, die die Verarbeitung personenbezogener Daten umfassen, ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen, wobei gleichzeitig betont wird, dass die Maßnahmen für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig sein sollten. Daher sollten Cybersicherheitsmaßnahmen nicht nur an Wirksamkeitserwägungen orientiert sein, sondern es sollte auch berücksichtigt werden, ob ihre Auswirkungen auf die Grundrechte auf das notwendige und verhältnismäßige Maß beschränkt bleiben.

3 UNTERSTÜTZUNG DER UMSETZUNG DER UNIONSPOLITIK UND DES UNIONSRECHTS DURCH DIE ENISA SOWIE ZUSAMMENARBEIT MIT ANDEREN EINRICHTUNGEN DER UNION

11. Gemäß Artikel 5 Absatz 1 des CSA2-Vorschlags trägt die ENISA in einer Vielzahl von Bereichen zur Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie die verschiedenen in diesem Artikel aufgeführten Interessenträger unterstützt.

12. Unter anderem würde die ENISA gemäß Artikel 5 Absatz 1 Buchstabe h des CSA2-Vorschlags auf Ersuchen des europäischen Datenschutzausschusses Beratung zur Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre bereitstellen. Der EDSA und der EDSB merken an, dass Artikel 5 Absatz 1 Buchstabe h des CSA2-Vorschlags keine völlig neue Bestimmung ist. Artikel 5 Absatz 5 Buchstabe c des geltenden Rechtsakts zur Cybersicherheit sieht schon jetzt vor, dass die ENISA „die Mitgliedstaaten bei der Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre [unterstützt], was – auf dessen Ersuchen die Beratung des Europäischen Datenschutzausschusses einschließt“.

13. Der EDSA und der EDSB begrüßen, dass die Modalitäten der Zusammenarbeit mit dem CSA2-Vorschlag weiter präzisiert und gleichzeitig die Kernelemente des Artikels 5 Absatz 5 Buchstabe c des Rechtsakts zur Cybersicherheit beibehalten würden. Mit dem neuen Artikel 5 Absatz 1 Buchstabe h würde klargestellt, dass der EDSA als Einrichtung der Union berechtigt ist, die Beratung durch die ENISA direkt anzufordern (ohne an die Umsetzung spezifischer Cybersicherheitsaspekte der Politik und des Rechts der Union in Bezug auf den Datenschutz und den Schutz der Privatsphäre durch die Mitgliedstaaten gebunden zu sein).

14. Gleichzeitig empfehlen der EDSA und der EDSB, angesichts der Rolle des EDSB als Aufsichtsbehörde für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union auch den EDSB als mögliche ersuchende Stelle in Artikel 5 Absatz 1 Buchstabe h der CSA2 aufzunehmen. Wenn sowohl der EDSA als auch der EDSB auf die Fachkompetenz der ENISA im Bereich der Cybersicherheit zurückgreifen können, kann dies dazu beitragen, dass ihre Leitlinien und Entscheidungen im Bereich des Datenschutzes auf dem neuesten Kenntnisstand im Bereich der Cybersicherheit beruhen. Die Beratung und Zusammenarbeit könnte für mehrere Themenbereiche von Nutzen sein, unter anderem für Cybersicherheitsstandards und operative Verfahrensweisen sowie in Bezug auf den Einsatz von Technologien zum Schutz der Privatsphäre im Zusammenhang mit der Cybersicherheit.

15. Der EDSA und der EDSB unterstützen nachdrücklich, dass die in Artikel 5 Absatz 1 Buchstabe h CSA2 genannte Beratung nur auf vorheriges Ersuchen des EDSA oder, wie hier vorgeschlagen, des EDSB erfolgt. Wenn festgelegt wird, dass die ENISA nur auf Ersuchen des EDSA oder des EDSB tätig wird, würde mit Artikel 5 Absatz 1 Buchstabe h eine klare Koordinierung und eine klare Aufteilung der Zuständigkeiten gewährleistet[10].

16. Der EDSA und der EDSB stellen fest, dass Artikel 5 Absatz 1 Buchstabe h des CSA2-Vorschlags eine spezifische Ausprägung einer allgemeineren Verpflichtung zur Zusammenarbeit zu sein scheint, die in Artikel 68 des CSA2-Vorschlags verankert ist, mit dem die Zusammenarbeit der ENISA mit anderen Einrichtungen der Union geregelt wird. Gemäß Artikel 68 arbeitet die ENISA in Fragen der Cybersicherheit mit anderen EU-Einrichtungen, einschließlich des Europäischen Datenschutzausschusses, zusammen, um Kohärenz zu gewährleisten, Synergien zu schaffen und Fragen von gemeinsamem Interesse anzugehen. Diese Zusammenarbeit kann durch den Austausch von Know-how und bewährten Verfahren, die Bereitstellung von Beratung und die Veröffentlichung von Leitlinien zu Fragen im Zusammenhang mit der Cybersicherheit sowie die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben, nach Konsultation der Kommission, erfolgen.

17. Der EDSA und der EDSB begrüßen die Zusammenarbeit und die Synergien zwischen der ENISA und anderen Einrichtungen der Union im Einklang mit ihren jeweiligen Aufgaben und Mandaten. In diesem Zusammenhang empfehlen der EDSA und der EDSB aus Gründen der Rechtsklarheit, Artikel 68 des CSA2-Vorschlags dahin gehend zu ändern, dass auch der EDSB als Einrichtung der Union, mit der die ENISA zusammenarbeiten würde, ausdrücklich erwähnt wird[11].

4 OPERATIVE ZUSAMMENARBEIT, GEMEINSAME LAGEERFASSUNG IM BEREICH DER CYBERSICHERHEIT UND SCHUTZ PERSONENBEZOGENER DATEN

[10] Indem die Einbindung der ENISA an ein Ersuchen der Aufsichtsbehörden geknüpft wird, bleibt ein strukturierter Konsultationsprozess gewahrt, in dem die ENISA technische Expertise bereitstellt, während die Aufsichtsbehörden die volle Kontrolle über Entscheidungen im Zusammenhang mit dem Datenschutz behalten. So wird auch sichergestellt, dass jedes Eingreifen der ENISA koordiniert erfolgt, wobei der EDSA oder der EDSB die Federführung übernehmen und die geeignete Vorgehensweise bestimmen. Durch die Achtung der vorgesehenen Rollen wird die Kohärenz gefördert, eine Fragmentierung der Rechtsvorschriften verhindert und die Rechenschaftspflicht der Datenschutzbehörden in ihrer Aufsichtsfunktion gestärkt.

[11] Der EDSA und der EDSB sind der Auffassung, dass sich Artikel 7 Absatz 2 des geltenden Rechtsakts zur Cybersicherheit bereits auf den EDSB erstreckt, da die ENISA nach diesem Artikel verpflichtet ist, auf operativer Ebene mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammenzuarbeiten und Synergien mit diesen Stellen zu entwickeln, zu denen auch die für die Aufsicht über den Datenschutz zuständigen Stellen zählen, um Fragen von gemeinsamem Interesse anzugehen.

18. Gemäß den Artikeln 10 und 11 des CSA2-Vorschlags, der eine Weiterentwicklung des derzeitigen Artikels 7 des Rechtsakts zur Cybersicherheit wäre, würde die ENISA ihre Rolle als zentrale Drehscheibe für die operative Zusammenarbeit ausweiten, was auch die Verarbeitung erheblicher Mengen an Informationen über Bedrohungen mit sich bringen würde[12]. Dies könnte den Schluss zulassen, dass die von der ENISA im Rahmen ihrer Rolle verarbeiteten Informationen personenbezogene Daten wie IP-Adressen, Nutzerdaten, Nutzerprotokolle, Finanzaustausch oder Einzelheiten zu beeinträchtigten Konten umfassen können.

19. Aufgrund der Erläuterungen der Europäischen Kommission[13] gehen der EDSA und der EDSB davon aus, dass die CSA 2 keine Beauftragung und Genehmigung der Verarbeitung personenbezogener Daten in großem Umfang durch die ENISA vorsieht[14].

    Der EDSA und der EDSB nehmen zwar zur Kenntnis, dass die ENISA hauptsächlich aggregierte, nicht-personenbezogene Daten erheben und weiterverarbeiten würde, weisen jedoch darauf hin, dass für den Fall, dass die künftigen Aufgaben der ENISA als Informationsdrehscheibe die Verarbeitung personenbezogener Daten in großem Umfang erfordern würden, dies in den Bestimmungen des Basisrechtsakts, der die jeweiligen Aufgaben regelt, ausdrücklich festgelegt werden müsste, einschließlich der wesentlichen Elemente einer etwaigen Verarbeitung in großem Umfang und geeigneter Schutzvorkehrungen. Falls hingegen das Ziel darin besteht, der ENISA vor allem die Erhebung und Weiterverarbeitung vorwiegend aggregierter, nicht-personenbezogener Daten zu ermöglichen, so sollte dies zumindest im Wege eines Erwägungsgrundes ebenfalls klargestellt werden.

20. Der EDSA und der EDSB stellen fest, dass die ENISA weiterhin personenbezogene Daten für Verwaltungszwecke verarbeiten wird[15]. Artikel 66 Absatz 1 des CSA2-Vorschlags enthält, ähnlich wie der geltende Rechtsakt zur Cybersicherheit[16], einen allgemeinen Verweis auf die geltenden Datenschutzvorschriften (d. h. auf die EU-DSVO), ohne dass weitere spezifische Vorschriften genannt werden.

[12] Vgl. COM(2026) 11 final, Finanz- und Digitalbogen zu Rechtsakten, S. 19: „Die neuen Elemente/Aufgaben des Vorschlags werden einen Mehrwert für die europäischen Interessenträger mit sich bringen, die davon profitieren würden, wenn die ENISA als Informationsdrehscheibe fungieren, zur Informationsweitergabe beitragen und ihnen Warnmeldungen zukommen lassen würde.“ Ferner S. 95: „In den letzten Jahren ist die ENISA zu einer Informationsdrehscheibe für Informationen aus verschiedenen Quellen geworden. In diesem Sinne sind zahlreiche der Aufgaben der ENISA mit der Weiterverwendung und dem Recycling von Informationen für die Zwecke verschiedener Analysen verbunden.“

[13] Wie in einer Ad-hoc-Sitzung der Untergruppe der Technologieexperten des EDSA am 27. Februar 2026 dargelegt.

[14] Nach Angaben der Kommission hat die ENISA kein Mandat zur operativen Analyse von Sicherheitsvorfällen und keinen Zugang zu Daten aus den Sicherheitsvorfällen selbst. Stattdessen werden die Daten in aggregierter Form verarbeitet. Warnmeldungen der nationalen Computer-Notfallteams (CSIRTs) enthalten in der Regel keine operativen personenbezogenen Daten, sondern Verwaltungsdaten (z. B. Kontaktdaten). Ebenso könnten Unternehmen, die sich für den Erhalt von Frühwarnmeldungen anmelden, ihre Kontaktdaten angeben. Nach Angaben der Europäischen Kommission hätte die ENISA in dem seltenen Fall, dass die ihr übermittelten aggregierten Informationen zu Bedrohungen oder Vorfällen IP-Adressen enthalten, weder einen operativen Bedarf noch folglich die rechtliche und tatsächliche Möglichkeit, den hinter der IP-Adresse stehenden Abonnenten zu ermitteln. Die Europäische Kommission stellte ferner klar, dass der in Artikel 13 vorgesehene Helpdesk beratender Art ist und beispielsweise Auskunft darüber erteilt, an welche zuständige Behörde des Mitgliedstaats man sich wenden kann.

[15] Beispielsweise bei der Prüfung von Anträgen auf Zulassung als befugter Bescheinigungsanbieter im Rahmen des Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen (Artikel 22), im Rahmen des Beschwerdeverfahrens gegen getroffene Entscheidungen (Artikel 36 ff.), bei der Bearbeitung von Beschwerden natürlicher oder juristischer Personen im Zusammenhang mit Zertifizierungen oder EU-Konformitätserklärungen (Artikel 88 Absatz 6 Buchstabe h) oder im Zusammenhang mit Cybersicherheitszertifizierungen (Artikel 96).

[16] Siehe Artikel 41 Absatz 1 der Verordnung (EU) 2019/881.

21. Im selben Sinne übernimmt Artikel 66 Absatz 2 des CSA2-Vorschlags den derzeitigen Artikel 41 Absatz 2 des Rechtsakts zur Cybersicherheit, wonach der Verwaltungsrat der ENISA „zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind, festlegen [kann]“ [17], ohne dass der Verwaltungsrat verpflichtet ist, spezifische Maßnahmen zu ergreifen. In der Bestimmung des Artikels 66 Absatz 2 des CSA2-Vorschlags werden weder der Anwendungsbereich und die Art solcher zusätzlichen Datenschutzmaßnahmen noch das anzuwendende Annahmeverfahren festgelegt. Es wird auch nicht klargestellt, welche Rolle der EDSB in dem Verfahren spielt[18].

22. Nach dem Verständnis des EDSA und des EDSB sollte der Verwaltungsrat der ENISA, falls er entscheidet, Artikel 66 Absatz 2 des CSA2-Vorschlags anzuwenden, in der/den entsprechenden Entscheidung(en) genauer darlegen, wie die ENISA personenbezogene Daten verarbeitet.

23. Der EDSA und der EDSB erinnern daran, dass grundsätzlich nur Entscheidungen über sehr technische (praktische) Einzelheiten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der Verwaltungsautonomie der betreffenden EU-Einrichtung, in diesem Fall des Verwaltungsrats einer dezentralen Agentur, überlassen bleiben sollten. Dies liegt daran, dass die Genehmigung von Eingriffen in Grundrechte besser dem Gesetzgeber und höchstens der Kommission im Wege von Durchführungsrechtsakten oder delegierten Rechtsakten vorbehalten bleiben sollte[19]. Daher sollte in der verfügenden Bestimmung der Verordnung ausdrücklich klargestellt werden, was genau in Satz 2 des Entwurfs des Artikels 66 Absatz 2 mit „zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind“, gemeint ist.

24. Wird es dennoch für notwendig erachtet, dass der Verwaltungsrat Maßnahmen ergreift, die über die in Rechtsvorschriften oder delegierten Rechtsakten bzw. Durchführungsrechtsakten bereits vorgesehenen technischen (praktischen) Einzelheiten der Verarbeitung hinausgehen, sollten diese Maßnahmen – neben einer klareren Abgrenzung ihres Anwendungsbereichs – klar und präzise sein und ihre Anwendung für die betroffenen Personen vorhersehbar sein. Dazu gehört auch, dass die genannten Vorschriften angemessen bekannt gemacht werden. Darüber hinaus sollten darin die erforderlichen Schutzvorkehrungen vorgesehen werden, um die Einhaltung der wichtigsten Datenschutzgrundsätze und -garantien wie Zweckbindung, Speicherbegrenzung, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sicherzustellen. Des Weiteren empfehlen der EDSA und der EDSB als wichtige zusätzliche Schutzvorkehrung in solchen Fällen, dass Artikel 66 des CSA2-Vorschlags eine vorherige Konsultation des EDSB vor der Annahme solcher Vorschriften vorsieht[20].

[17] Am 21. November 2019 hat der Verwaltungsrat der ENISA eine Entscheidung über interne Vorschriften zur Beschränkung bestimmter Rechte betroffener Personen in Bezug auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit der ENISA gemäß Artikel 25 der EU-DSVO angenommen.

[18] So sieht beispielsweise Artikel 18a Absatz 5 der Verordnung (EU) 2016/794 (Europol-Verordnung) vor, dass der Verwaltungsrat von Europol auf Vorschlag des Exekutivdirektors und **nach Anhörung des EDSB**, die Bedingungen für die Übermittlung und Verarbeitung personenbezogener Daten festlegt (Hervorhebung hinzugefügt).

[19] Siehe EDSB, „Guidance for co-legislators on key elements of legislative proposals“, abrufbar unter https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, Rn. 76.

[20] Ähnlich den Bestimmungen des Artikels 18a Absatz 5 der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (Europol-Verordnung) (ABl. L 135 vom 24.5.2016, S. 53).

5 ZENTRALE ANLAUFSTELLE FÜR DIE MELDUNG VON VORFÄLLEN (ARTIKEL 15 CSA2)

25. Gemäß Artikel 15 des CSA2-Vorschlags muss die ENISA für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung unter anderem der gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichteten einheitlichen Meldeplattform und der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle für die Meldung von Vorfällen sorgen. Mit diesen Instrumenten sollen die verschiedenen Berichtspflichten im Zusammenhang mit der Cybersicherheit vereinfacht werden[21].

26. Wie bereits in ihrer gemeinsamen Stellungnahme zum Digital-Omnibus-Vorschlag [22] dargelegt, unterstützen der EDSA und der EDSB nachdrücklich das Ziel der Einrichtung einer zentralen Anlaufstelle für die Meldung von Verletzungen des Schutzes personenbezogener Daten, da dies den Verwaltungsaufwand für Organisationen verringern würde, ohne das Schutzniveau für die betroffenen Personen zu beeinträchtigen. In seiner Erklärung von Helsinki [23] hat der EDSA bereits seine Unterstützung für eine mögliche vorschriftenübergreifende europäische Lösung zur Meldung von Vorfällen bekräftigt, da dies dazu beitragen würde, die Einhaltung der DSGVO zu erleichtern. Der EDSA und der EDSB erinnern auch daran, wie wichtig es ist, die Sicherheit der Meldungen zu gewährleisten, die bei der zentralen Anlaufstelle eingereicht und über diese weitergeleitet werden, da Meldungen über Datenschutzverletzungen häufig sensible Informationen enthalten[24].

6 EUROPÄISCHER KOMPETENZRAHMEN FÜR CYBERSICHERHEIT (ECSF) (ARTIKEL 19 CSA2)

27. Nach Artikel 19 des CSA2-Vorschlags wäre die ENISA verpflichtet, einen europäischen Kompetenzrahmen für Cybersicherheit (European Cybersecurity Skills Framework, ECSF) zu entwickeln und öffentlich zugänglich zu machen. Der ECSF würde dazu beitragen, dass Cybersicherheitsfachkräfte, Arbeitgeber, Schulungsanbieter und Behörden in allen Mitgliedstaaten ein gemeinsames Verständnis dafür entwickeln, welche Anforderungen bestimmte Berufe im Bereich Cybersicherheit stellen. Er würde klare Stellenprofile, transparente Qualifikationsanforderungen und eine bessere Abstimmung zwischen Bildung und Arbeitsmarktbedarf fördern. Die ENISA würde den ECSF als Grundlage für die Durchführung von Schulungen nutzen, insbesondere um die Umsetzung der EU-Rechtsvorschriften zur Cybersicherheit, die operative Zusammenarbeit zwischen den Mitgliedstaaten und Sensibilisierungsmaßnahmen zu unterstützen. Dies bedeutet, dass der ECSF als Grundlage für strukturierte Schulungsprogramme im Bereich der Cybersicherheit dient, insbesondere für Behörden und Einrichtungen, die unter die EU-Rechtsvorschriften zur Cybersicherheit fallen.

---

[21] Siehe Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 und COM(2025) 837 final, S. 8.

[22] Gemeinsame Stellungnahme 2/2026 des EDSA und des EDSB zu dem Vorschlag für eine Verordnung hinsichtlich der Vereinfachung des digitalen Rechtsrahmens (Digital-Omnibus-Verordnung), angenommen am 10. Februar 2026.

[23] EDSA, „The Helsinki Statement on enhanced clarity, support and engagement, A fundamental rights approach to innovation and competitiveness“, angenommen am 2. Juli 2025.

[24] Siehe Kapitel 8.3 der gemeinsamen Stellungnahme des EDSA und des EDSB 2/2026 zu dem Vorschlag für eine Verordnung hinsichtlich der Vereinfachung des digitalen Rechtsrahmens (Digital-Omnibus-Verordnung), angenommen am 10. Februar 2026.

28. Der EDSA und der EDSB begrüßen das Ziel, die Fachkräfte im Bereich der Cybersicherheit in der EU zu stärken, und betonen, dass die grenzüberschreitende Übertragbarkeit und Anerkennung von Qualifikationen für das Funktionieren des digitalen Binnenmarkts wichtig sind.

29. Gleichzeitig stellen sie fest, dass die in Artikel 19 Absatz 2 des CSA2-Vorschlags festgelegten Profile derzeit auf Cybersicherheitsfachkräfte beschränkt sind. Der Vorschlag enthält kein Profil der erforderlichen Kompetenzen für Bürgerinnen und Bürger, Beamte oder nicht spezialisierte Arbeitskräfte. Wie in Erwägungsgrund 21 des CSA2-Vorschlags anerkannt wird, ist der Erwerb digitaler Kompetenzen entscheidend, um die Bürgerinnen und Bürger resilienter zu machen; dennoch verfügt knapp die Hälfte der erwachsenen Bevölkerung nicht über grundlegende digitale Kompetenzen, obwohl mehr als 90 % der Arbeitsplätze diese voraussetzen. Daher sollte der ECSF ein Profil „Cybersicherheit für Nichtfachkräfte“ umfassen, das die Mindestfertigkeiten abdeckt, über die alle in der EU ansässigen Personen im erwerbsfähigen Alter verfügen sollten, um im digitalen Binnenmarkt sicher interagieren zu können, und das nicht nur sie selbst, sondern auch ihre Organisation und andere insbesondere vor KI-gestütztem Phishing, Deepfakes, Identitätsbetrug und Social-Engineering-Angriffen schützt. Ein solches Profil könnte von öffentlichen oder privaten Organisationen zur Schulung ihres Personals verwendet werden, um durch menschliche Fehler bedingte Risiken für sie zu minimieren und damit das Risiko von Datenschutzverletzungen insgesamt zu verringern.

30. Der EDSA und der EDSB weisen darauf hin, dass in Erwägungsgrund 45 des Vorschlags ausdrücklich zwischen dem ECSF und dem Europäischen Referenzrahmen für digitale Kompetenzen (DigComp 3.0) unterschieden wird, wobei klargestellt wird, dass Letzterer für das tägliche Leben, die Teilhabe an der Gesellschaft, die Arbeit und das Lernen bestimmt ist und sowohl von Erwachsenen als auch von Kindern genutzt werden kann[25], während der ECSF für ein spezialisiertes Publikum bestimmt ist und einen einfachen Rahmen bietet, in dem die Cybersicherheitsfunktionen und die damit verbundenen Aufgaben, Fähigkeiten und Kenntnisse festgelegt sind, die für die Ausübung dieser Funktionen erforderlich sind.

[25] Der EDSA und der EDSB erinnern auch daran, dass die Europäische Kommission zwischen 2022 und 2024 die Entwicklung eines auf DigComp beruhenden europäischen Zertifikats für digitale Kompetenzen (EDSC) geprüft hat. Das Zertifikat würde dazu beitragen, dass die digitalen Kompetenzen der Menschen von Arbeitgebern, Bildungsanbietern und anderen schnell und einfach anerkannt werden. Diese Initiative sollte ein europaweites Qualitätssiegel für die Zertifizierung digitaler Kompetenzen bieten. Im Anschluss an eine Machbarkeitsstudie (siehe Centeno, C., Cosgrove, J., Cachia, R., Mora, T., Di Legge, A., Vivarelli, S., Bulian, G., Moyes Prellezo, N., Piña de Santisteban, P., Schulz, C., Hüsing, T., Cuartas-Acosta, A. und Troia, S., European Digital Skills Certificate (EDSC) Feasibility Study, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344) und ein Pilotprojekt unter Beteiligung mehrerer EU-Länder kam die Europäische Kommission zu dem Schluss, dass ein solches Qualitätssiegel den europäischen Bürgerinnen und Bürgern keinen ausreichenden Mehrwert bringen würde. Der DigComp-Referenzrahmen, 2013 erstmals veröffentlicht, besteht jedoch nach wie vor (Cosgrove, J., und Cachia, R., „DigComp 3.0: European Digital Competence Framework“, fünfte Ausgabe, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121). Darin werden die Anforderungen an digitale Kompetenz in der heutigen Gesellschaft beschrieben; zugleich wird mit dem Rahmen die Entwicklung digitaler Kompetenz bei Menschen jeden Alters unterstützt. DigComp deckt ein breites Spektrum an Kompetenzstufen von Grundlagenkenntnissen bis hin zu sehr fortgeschrittenem Wissen ab. Mehrere der im DigComp-Referenzrahmen erfassten Kompetenzen betreffen ausdrücklich die Cybersicherheit, darunter die Punkte 4.1 „Protecting devices“ (Schutz von Geräten), 4.2 „Protecting personal data and privacy“ (Schutz personenbezogener Daten und der Privatsphäre) und sogar 4.4 „Protecting the environment“ (Schutz der Umwelt) (Vermeidung von Datenverlusten aus Altgeräten). Auch andere Bereiche betreffen einschlägige Kompetenzen: So umfasst Bereich 1 Kompetenzen, die zur Abwehr von Social Engineering entscheidend sind, Bereich 2 Kompetenzen zur Verringerung der Risiken durch Insider-Bedrohungen und zur Verhinderung der versehentlichen Offenlegung von Informationen und Bereich 5 Kompetenzen zur schnelleren Erkennung von Vorfällen.

31. Der EDSA und der EDSB unterstützen alle genannten Initiativen, unabhängig davon, ob sie von der ENISA oder – im Falle des DigComp-Referenzrahmens – von der Gemeinsamen Forschungsstelle (JRC) der Europäischen Kommission durchgeführt werden, da sie bei ausreichender Verbreitung dazu beitragen würden, das Risiko von Datenschutzverletzungen zu verringern. Daher fordern sie alle Beteiligten dazu auf, nach Möglichkeiten zur Stärkung der Wirksamkeit der Rahmenwerke zu suchen.

32. Gleichzeitig sind der EDSA und der EDSB der Auffassung, dass der DigComp-Referenzrahmen ein spezielles Cybersicherheitssystem für Nichtfachkräfte nicht ersetzt[26], und empfehlen den beiden gesetzgebenden Organen, Artikel 19 Absatz 2 des CSA2-Vorschlags dahin gehend zu ändern, dass der ECSF nicht ausschließlich auf „Cybersicherheitsfachkräfte“ beschränkt ist, sondern auch Profile für die allgemeine Belegschaft oder für Bürgerinnen und Bürger umfasst. Begleitend dazu sollte Erwägungsgrund 45 entsprechend geändert werden.

33. Darüber hinaus halten es der EDSA und der EDSB für erforderlich, in die Berufsprofile des ECSF ein Modul aufzunehmen, das sich mit der Notwendigkeit befasst, die Übereinstimmung von Cybersicherheitsmaßnahmen mit dem EU-Datenschutzrecht sicherzustellen, insbesondere im Hinblick auf die praktische Umsetzung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 DSGVO), und fordern die gesetzgebenden Organe auf, zu diesem Zweck einen Erwägungsgrund hinzuzufügen.

7 EUROPÄISCHER ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT (TITEL III)

34. In Artikel 71 und Artikel 80 Absatz 1 Buchstabe w des CSA2-Vorschlags ist der Anwendungsbereich der Cybersicherheitszertifizierung geregelt. In Artikel 80 Absatz 1 Buchstabe w wird als Sicherheitsziel der europäischen Systeme für die Cybersicherheitszertifizierung die „Gewährleistung, dass die Einrichtung in der Lage ist, für die Sicherheit der Verarbeitung personenbezogener Daten zu sorgen“, hinzugefügt.

35. Der EDSA und der EDSB stellen fest, dass der Wortlaut des Artikels 80 Absatz 1 Buchstabe w des CSA2-Vorschlags den Anforderungen der DSGVO an die Sicherheit der Verarbeitung sehr nahekommt[27]. Vor diesem Hintergrund könnte der Anwendungsbereich des neuen Zertifizierungssystems so ausgelegt werden, dass er Anforderungen gemäß der DSGVO umfasst. Der rechtliche und operative Anwendungsbereich ist jedoch nicht ganz klar, da die Bestimmung keinen Querverweis auf Bestimmungen der DSGVO (z. B. Artikel 5 Absatz 1 Buchstabe f, Artikel 32, Artikel 25 DSGVO) enthält und in eine Liste von „Sicherheitszielen“ (Artikel 80 Absatz 1 Satz 1) aufgenommen wurde.

[26] Im DigComp-Referenzrahmen sind die auf Sicherheit bezogenen Inhalte auf 21 Kompetenzen verteilt; zudem fehlen explizite Bedrohungsmodelle, es werden keine organisatorischen Sicherheitsrisiken operationalisiert, und es wird keine direkte Zuordnung zu den Compliance-Verpflichtungen vorgenommen. Während der ECSF in seiner derzeitigen Form für die Kompetenzen von Cybersicherheitsfachkräften gelten würde, fehlt es an einem strukturierten Rahmen auf EU-Ebene für Beschäftigte, die nicht im Bereich der Cybersicherheit tätig sind. Der EDSA und der EDSB erinnern daran, dass die meisten Verstöße auf Phishing, Social Engineering, den Missbrauch von Zertifikaten, Fehlkonfigurationen und die Verwendung von „Schatten-IT“ zurückzuführen sind. Dies sind Verhaltensweisen von Nichtfachkräften. Mit einem Cybersicherheitsrahmen für Nichtfachkräfte könnten Risiken verdeutlicht, rollenspezifische Erwartungen (z. B. für die Bereiche Humanressourcen oder Finanzen) formuliert und messbare Ergebnisse unterstützt werden.

[27] Siehe Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO.

36. Der EDSA und der EDSB erinnern daran, dass sich der Begriff „Sicherheit“ im Rahmen der DSGVO auf Risiken für die Grundrechte und Grundfreiheiten natürlicher Personen bezieht. Während die rechtliche Definition der Cybersicherheit nach Unionsrecht allgemein den Schutz von Nutzern und anderen Personen umfasst [28], deckt der Anwendungsbereich von Cybersicherheitsmaßnahmen in der Regel Risiken aller Art für die betreffende Organisation ab. Dennoch besteht die Möglichkeit, Synergien zu schaffen, damit der Schutz der Rechte und Freiheiten des Einzelnen in die Bewertung der Sicherheitsrisiken einbezogen werden kann.

37. Der EDSA und der EDSB erinnern ferner daran, dass die DSGVO ein eigenes Zertifizierungsverfahren vorsieht (Artikel 42 und 43 DSGVO), und sind der Auffassung, dass sich die Cybersicherheitszertifizierung von der Datenschutzzertifizierung gemäß Artikel 42 DSGVO unterscheidet.

38. Unabhängig davon aber können nach Auffassung des EDSA und des EDSB Synergien zwischen der Cybersicherheits- und der Datenschutzzertifizierung bestehen. So könnte zum Beispiel die Zertifizierung nach der CSA2 als Nachweis für die Erfüllung einiger Anforderungen der Zertifizierung nach der DSGVO dienen, soweit dies die Cybersicherheit betrifft. Der EDSA und der EDSB weisen jedoch darauf hin, dass in Artikel 80 Absatz 1 Buchstabe w des CSA2-Vorschlags das Verhältnis zur Zertifizierung nach Artikel 42 und 43 DSGVO nicht klar zum Ausdruck kommt. Im Interesse der Rechtssicherheit empfehlen der EDSA und der EDSB, den Anwendungsbereich des Artikels 80 Absatz 1 Buchstabe w CSA2 und das Verhältnis zur DSGVO-Zertifizierung weiter zu präzisieren. Darüber hinaus empfehlen der EDSA und der EDSB, die ENISA zu verpflichten, vor der Annahme eines Zertifizierungssystems nach Artikel 80 Absatz 1 Buchstabe w CSA2 den EDSA zu konsultieren, um Kohärenz zu gewährleisten.

39. Der EDSA und der EDSB betonen, dass nicht nur die Wirksamkeit von Cybersicherheitsmaßnahmen, sondern auch deren Notwendigkeit und Verhältnismäßigkeit berücksichtigt werden müssen. Bestimmte Cybersicherheitskontrollen bergen spezifische Datenschutzrisiken. Dies kann bei der Überwachung und Protokollierung, bei der Deep Packet Inspection oder der Analyse des Nutzerverhaltens der Fall sein. Ein gut konzipiertes System zur Zertifizierung der Sicherheit der Verarbeitung könnte Kontrollen vorsehen, die sicherstellen, dass Sicherheitsvorkehrungen in einer Weise umgesetzt werden können, die mit den Datenschutzvorschriften im Einklang steht (z. B. sollten bestimmte Aspekte konfigurierbar sein; dies könnte etwa für den Detaillierungsgrad der zu Sicherheitszwecken protokollierten Daten gelten, da dies die Einhaltung der Grundsätze der Sicherheit und der Datenminimierung nach der DSGVO durch den Verantwortlichen ermöglichen oder erleichtern kann; ebenso sollten Speicherfristen konfigurierbar sein, damit der Verantwortliche im Rahmen der von ihm durchgeführten Verarbeitung festlegen kann, wie lange personenbezogene Daten gespeichert werden, bevor sie gelöscht oder mittels zertifizierter Verfahren anonymisiert werden).

[28] Siehe Artikel 2 Nummer 1 des CSA2-Vorschlags, bei dem es sich um eine aus dem früheren Rechtsakt übernommene Bestimmung handelt und der wie folgt lautet: „‚Cybersicherheit‘ [bezeichnet] alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.“

40. Daher empfehlen der EDSA und der EDSB, in einem Erwägungsgrund zu erläutern, dass Zertifizierungssysteme so weit wie möglich so konzipiert, umgesetzt und aufrechterhalten werden sollten, dass Sicherheitskontrollen berücksichtigt werden, die zum Nachweis der Erfüllung der Anforderungen gemäß DSGVO beitragen können, wenn die Systeme für IKT-Produkte, Dienste und Prozesse und verwaltete Sicherheitsdienste gelten, die bei Datenverarbeitungsvorgängen wahrscheinlich verwendet werden. Es sei auch darauf hingewiesen, dass einige Kontrollen dazu beitragen können, den Schutz der Privatsphäre und den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten.

8 RAHMEN FÜR VERTRAUENSWÜRDIGE IKT-LIEFERKETTEN (TITEL IV)

41. Der CSA2-Vorschlag sieht die Aufnahme von Maßnahmen für die Sicherheit der IKT-Lieferketten vor und trägt damit insbesondere nichttechnischen Risiken Rechnung, darunter Faktoren im Zusammenhang mit geopolitischen, rechtlichen und eigentumsrechtlichen Aspekten sowie mit Abhängigkeiten und strategischer Einmischung, die sich auf die IKT-Lieferketten in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren auswirken. Solche Maßnahmen zur Lieferkettensicherheit zielen zwar in erster Linie auf die Abwehr von Risiken ab, die nicht unmittelbar mit dem Datenschutz zusammenhängen, können sich aber auch positiv auf den Schutz der Grundrechte auswirken, indem sie die Einflussnahme aus dem Ausland auf die Daten betroffener Personen in der EU durch Tätigkeiten wie Spionage und Überwachung begrenzen.

42. Der EDSA und der EDSB begrüßen die vorgeschlagene Maßnahme, mit der ein vertrauenswürdiger Rahmen für IKT-Lieferketten sichergestellt und nichttechnische Risiken in Sektoren mit hoher Kritikalität angegangen werden sollen.

9 ZUSÄTZLICHE WESENTLICHE EINRICHTUNGEN IM RAHMEN DES NIS-2-VORSCHLAGS

43. Der Vorschlag zur Änderung der NIS-2-Richtlinie würde Anbieter von europäischen Brieftaschen für die digitale Identität und von europäischen Brieftaschen für Unternehmen unabhängig von ihrer Größe als „wesentliche Einrichtungen“ einbeziehen. Als „wesentlich“ eingestufte Einrichtungen unterliegen den uneingeschränkten Risikomanagementverpflichtungen des NIS-2-Rahmens im Bereich der Cybersicherheit und müssen die nach Artikel 21 der NIS-2-Richtlinie erforderlichen Sicherheitsmaßnahmen umsetzen, einschließlich Risikoanalyse und Sicherheitskonzepte, Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebs und Krisenmanagement, Sicherheit der Lieferkette, Behandlung von Schwachstellen, Konzepte für Kryptografie und Verschlüsselung sowie Zugriffskontrolle und Management von Anlagen.

44. Der EDSA und der EDSB begrüßen die Benennung der Anbieter von europäischen Brieftaschen für die digitale Identität und von europäischen Brieftaschen für Unternehmen als „wesentliche Einrichtungen“. Der EDSA und der EDSB sind der Auffassung, dass Brieftaschen für die digitale Identität ein Kernbestandteil der digitalen Infrastruktur der EU sind und sie betreffende Vorfälle folglich weitreichende grenzüberschreitende Auswirkungen haben könnten. Sie unterstützen die sichere Identifizierung, Authentifizierung und elektronische Bescheinigungen. Für die digitale Wirtschaft sind Brieftaschen für Unternehmen ebenso wichtig wie europäische Brieftaschen für die digitale Identität. Folglich werden beide Arten von Brieftaschenanbietern ähnlich behandelt wie die bereits im Rahmen der NIS-2-Richtlinie als „wesentliche Einrichtungen“ eingestuften Vertrauensdiensteanbieter und wie andere Betreiber hochkritischer Infrastrukturen.

10 ERHEBUNG VON DATEN ÜBER RANSOMWARE-ANGRIFFE

45. Gemäß Artikel 5 Absatz 8 des Vorschlags zur Änderung der NIS-2-Richtlinie, in dem vorgeschlagen wird, für den Fall von Ransomware-Angriffen neue Absätze 12 und 13 in Artikel 23 der NIS-2-Richtlinie anzufügen, können die betroffenen Einrichtungen aufgefordert werden, bestimmte Informationen über Ransomware-Vorfälle an Computer-Notfallteams (Computer Security Incident Response Teams, CSIRTs) zu übermitteln, u. a. Informationen darüber, ob eine Einrichtung Lösegeld gezahlt hat, und wenn ja, in welcher Höhe und an wen (Anbieter von Kryptowerten/Krypto-Dienstleistungen), sowie Angaben zur Identität der Person, die als Kontaktstelle fungiert.

46. Nach Artikel 23 Absatz 11 der NIS-2-Richtlinie ist die Kommission befugt, Durchführungsrechtsakte zu erlassen, in denen die Art der Angaben, das Format und das Verfahren zur Erfüllung der Meldepflichten näher bestimmt werden. Der Anwendungsbereich des entsprechenden Durchführungsrechtsakts würde auf die neuen Meldepflichten im Falle von Ransomware-Angriffen ausgeweitet.

47. Der EDSA und der EDSB unterstützen uneingeschränkt das wichtige Ziel, künftige Ransomware-Angriffe zu verhindern und die dahinter stehenden kriminellen Organisationen zu stören und zu zerschlagen. Der EDSA und der EDSB weisen darauf hin, dass die über Ransomware-Angriffe auszutauschenden Informationen potenziell sensiblen Charakter haben können, wie die Kommission in Erwägungsgrund 10 des Vorschlags zur Änderung der NIS-2-Richtlinie näher erläutert. Darüber hinaus können solche Meldungen die Verarbeitung personenbezogener Daten mit sich bringen. Der EDSA und der EDSB begrüßen den in den Absätzen 12 und 13 gewählten mehrstufigen Ansatz, der vorsieht, dass die sensibleren Informationen gemäß Absatz 13 nur auf Ersuchen gemeldet werden.

48. Gleichzeitig empfehlen der EDSA und der EDSB angesichts der Sensibilität der gemeldeten Daten und im Einklang mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit für den Fall, dass die Meldung von Ransomware-Angriffen die Verarbeitung personenbezogener Daten umfassen würde, im Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 der NIS-2-Richtlinie die anwendbaren Vorkehrungen zum Schutz personenbezogener Daten festzulegen. In diesem Zusammenhang erinnern sie auch an die Pflicht der Kommission gemäß Artikel 42 Absatz 1 EU-DSVO, den EDSB zu den Entwürfen von Durchführungsrechtsakten und delegierten Rechtsakten zu konsultieren, sofern diese Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben.