EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17. Mai 2022

Stellungnahme 8/2022

zu dem Vorschlag für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

edps.europa.eu

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU) 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden"; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig.

Am 5. Dezember 2019 wurde Wojciech Rafał Wiewiorówski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.

*Gemäß **Artikel 42 Absatz 1** der Verordnung (EU) 2018/1725 konsultiert die Kommission den Europäischen Datenschutzbeauftragten „[n]ach der Annahme von Vorschlägen für einen Gesetzgebungsakt, für Empfehlungen oder Vorschläge an den Rat nach Artikel 218 AEUV sowie bei der Ausarbeitung von delegierten Rechtsakten und Durchführungsrechtsakten, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben".*

Diese Stellungnahme befasst sich mit dem Vorschlag der Kommission für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union. Die vorliegende Stellungnahme schließt künftige zusätzliche Kommentare oder Empfehlungen des EDSB nicht aus, insbesondere wenn weitere Probleme festgestellt oder neue Informationen bekannt werden. Diese Stellungnahme greift etwaigen künftigen Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß der Verordnung (EU) 2018/1725 ergreifen mag, nicht vor.

Zusammenfassung

Am 22. März 2022 nahm die Europäische Kommission einen Vorschlag für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union („Vorschlag“) an.

Der EDSB begrüßt das Ziel des Vorschlags, den Cybersicherheitsstand der Organe, Einrichtungen und sonstigen Stellen der Union zu verbessern, und begrüßt gleichermaßen die neue Rolle des ehemaligen „Reaktionsteams für IT-Sicherheitsvorfälle“, das nun die Bezeichnung „Cybersicherheitszentrum“ (CERT-EU) trägt, wobei der verstärkten Digitalisierung, der sich rasch wandelnden Bedrohungslage im Bereich der Cybersicherheit und der in jüngster Zeit stark zunehmenden Digitalisierung aufgrund der COVID-19-Pandemie Rechnung getragen wird.

Der EDSB bedauert, dass sich der Vorschlag nicht an die NIS-Richtlinie und den NIS-2-Vorschlag anpasst, damit kohärente und homogene Vorschriften für die Mitgliedstaaten und die Organe und Einrichtungen der Union erreicht werden und so ein Beitrag zum allgemeinen Cybersicherheitsniveau der Union geleistet wird. Der EDSB empfiehlt, in den Vorschlag aufzunehmen, dass dessen Mindestsicherheitsanforderungen mindestens den Mindestsicherheitsanforderungen der Einrichtungen des NIS- und NIS 2.0-Vorschlags entsprechen oder darüber hinausgehen sollten.

Um mit dem Vorschlag in Einklang zu stehen, müssen die Organe und Einrichtungen der Union sowie das CERT-EU bestimmte Cybersicherheitsverfahren und -maßnahmen einführen, die zwangsläufig zusätzliche Verarbeitungen personenbezogener Daten mit sich bringen. Um Rechtssicherheit und Vorhersehbarkeit zu erreichen und die Einhaltung der EU-DSVO zu gewährleisten, empfiehlt der EDSB nachdrücklich, dass der Vorschlag oder zumindest ein delegierter Rechtsakt, der später von der Kommission erlassen wird, eine eindeutige Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch das CERT-EU und die Organe, Einrichtungen und sonstigen Stellen der Union bieten muss, insbesondere mit Blick auf die Zwecke der Verarbeitung und die Kategorien personenbezogener Daten.

Der EDSB betont, wie wichtig es ist, die Perspektive des Schutzes der Privatsphäre und des Datenschutzes in das Cybersicherheitsmanagement einzubeziehen, um positive Synergien zwischen dem Vorschlag und den Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz zu erzielen, und gibt konkrete Empfehlungen dazu ab, wie solche Synergien erreicht werden können, einschließlich einer spezifischen Verpflichtung für EU-Bedienstete, die für Cybersicherheit zuständig sind, eng mit dem im Einklang mit der EU-DSVO benannten Datenschutzbeauftragten zusammenzuarbeiten.

Der EDSB empfiehlt nachdrücklich, in dem Vorschlag eine enge Zusammenarbeit zwischen dem CERT-EU und dem EDSB bei Tätigkeiten wie der Bewältigung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten führen, dem Umgang mit erheblichen Schwachstellen, erheblichen Sicherheitsvorfällen oder schweren Angriffen, die potenziell Verletzungen des Schutzes personenbezogener Daten zu verursachen können, sowie bei Tätigkeiten vorzusehen, bei denen dem CERT-EU Hinweise darauf vorliegen, dass ein Verstoß gegen den Vorschlag eine Verletzung des Schutzes personenbezogener Daten nach sich zieht.

Der EDSB empfiehlt ferner nachdrücklich, in dem Vorschlag die Beteiligung des EDSB am Interinstitutionellen Cybersicherheitsbeirat (IICB) vorzusehen.

Inhalt

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[1], insbesondere auf Artikel 42 Absatz 1, –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1. Am 22. März 2022 nahm die Europäische Kommission einen Vorschlag für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union[2] („Vorschlag“) an.

2. Am selben Tag nahm die Europäische Kommission den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union[3] („Infosec-Vorschlag“) an.

3. Beide Vorschläge waren in der am 16. Dezember 2020 vorgelegten Cybersicherheitsstrategie der EU für die digitale Dekade[4] („Strategie“) vorgesehen. Oberstes Ziel der Strategie ist es, die strategische Autonomie der Union im Bereich der Cybersicherheit zu stärken, ihre Resilienz und ihre kollektive Reaktion zu verbessern und ein globales und offenes Internet mit starken Schutzvorkehrungen aufzubauen, um den Risiken für die Sicherheit, die Grundrechte und die Grundfreiheiten der Menschen in Europa zu begegnen.[5]

4. Der Vorschlag ist eine der Regulierungsinitiativen der Strategie, und zwar insbesondere im Bereich der Cybersicherheit für die Organe, Einrichtungen und sonstigen Stellen der EU. Gemäß der Begründung des Vorschlags werden mit dem Vorschlag zwei Ziele verfolgt:

   - höhere Investitionen, weil die Cyberbedrohungen zunehmend feindseliger werden und die Organe, Einrichtungen und sonstigen Stellen der EU immer häufiger komplexen Cyberangriffen ausgesetzt sind und deshalb einen hohen Grad an „Cyberreife“ erreichen müssen, und

   - Stärkung des Reaktionsteams der EU für IT-Sicherheitsvorfälle (CERT-EU) durch einen verbesserten Finanzierungsmechanismus, damit es den Organen, Einrichtungen und sonstigen Stellen der EU dabei helfen kann, die neuen Cybersicherheitsvorschriften anzuwenden und ihre Abwehrfähigkeit gegenüber Cyberangriffen zu verbessern.

5. Der EDSB hält fest, dass der Gegenstand des vorliegenden Vorschlags mit dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur

Aufhebung der Richtlinie (EU) 2016/1148 („NIS-2-Vorschlag“) eng verknüpft ist. Der EDSB erinnert an seine Stellungnahme 5/2021 zur Cybersicherheitsstrategie[6] und zur NIS-2-Richtlinie („NIS-2-Stellungnahme“)[7]. Daher wird in der vorliegenden Stellungnahme auf die NIS-2-Stellungnahme verwiesen.

6. Im Einklang mit der Strategie zielt der Vorschlag darauf ab, die Resilienz aller Organe, Einrichtungen und sonstigen Stellen der Union und ihre Kapazitäten zur Reaktion auf Sicherheitsvorfälle weiter zu verbessern. Er steht ferner im Einklang mit den Prioritäten der Kommission, Europa für das digitale Zeitalter zu rüsten und eine zukunftsfähige Wirtschaft zu schaffen, die im Dienste des Menschen steht. Darüber hinaus wird darin unterstrichen, dass die Sicherheit und Resilienz der öffentlichen Verwaltung ein Eckpfeiler des digitalen Wandels der Gesellschaft insgesamt ist.

7. In der Begründung heißt es, dass mit dem Vorschlag

   - Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus für die Organe, Einrichtungen und sonstigen Stellen der Union skizziert werden;

   - ein „Interinstitutioneller Cybersicherheitsbeirat“ eingerichtet wird, der für die Überwachung der Durchführung der vorgeschlagenen Verordnung zuständig ist;

   - für das Reaktionsteam für IT-Sicherheitsvorfälle für die Organe, Einrichtungen und sonstigen Stellen der Union („CERT-EU“)[8] als „Cybersicherheitszentrum“ für die Organe, Einrichtungen und sonstigen Stellen der Union im Einklang mit den Entwicklungen in den Mitgliedstaaten und weltweit eine neue Rolle definiert wird.

8. Am 22. März 2022 ersuchte die Kommission den EDSB gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 („EU-DSVO“)[9] um eine Stellungnahme zu dem Vorschlag. Die Anmerkungen und Empfehlungen in dieser Stellungnahme beschränken sich auf diejenigen Bestimmungen des Vorschlags, die für den Datenschutz größte Relevanz haben.

2. Allgemeine Anmerkungen

9. Der EDSB **hält fest**, dass der NIS-2-Vorschlag für öffentliche und private wesentliche und wichtige Einrichtungen gilt, der Vorschlag jedoch auf die Organe, Einrichtungen und sonstigen Stellen der Union Anwendung findet.

10. Der EDSB möchte betonen, dass für den NIS-2-Vorschlag, der Verpflichtungen für die Mitgliedstaaten vorsieht, die Anwendung der Verordnung (EU) 2016/679 („DSGVO“) und der Richtlinie 2002/58/EG („Datenschutzrichtlinie für elektronische Kommunikation“) bei der Verarbeitung personenbezogener Daten von Bedeutung ist, dass jedoch für den vorliegenden Vorschlag, in dem Vorschriften für die Organe, Einrichtungen und sonstigen Stellen der Union festgelegt werden, **die EU-DSVO gilt und eine gleichermaßen wichtige Rolle spielt**.

11. Der EDSB **begrüßt** das Ziel des Vorschlags, den Cybersicherheitsstand der Organe, Einrichtungen und sonstigen Stellen der Union durch ein eigenständiges und spezielles Rechtsinstrument in Form einer Verordnung zu verbessern. Der EDSB begrüßt

gleichermaßen die neue Rolle des CERT-EU, mit der der verstärkten Digitalisierung, der sich rasch wandelnden Bedrohungslage im Bereich der Cybersicherheit und der in jüngster Zeit stark zunehmenden Digitalisierung aufgrund der COVID-19-Pandemie Rechnung getragen wird.

12. Der EDSB **empfiehlt**, in einem gesonderten Erwägungsgrund entsprechend der gängigen Praxis Folgendes hinzuzufügen: „Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates konsultiert und hat am [Datum der Stellungnahme des EDSB] eine Stellungnahme abgegeben".

13. Der EDSB erinnert daran, dass er in seiner NIS-2-Stellungnahme den Mitgesetzgebern empfohlen hat, **eine realisierbare Verbindung zwischen dem NIS-2-Vorschlag und den künftigen Legislativmaßnahmen auf der Ebene der Organe und Einrichtungen der Union herzustellen, um kohärente und einheitliche Vorschriften** für die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union zu erreichen.[1] Dies ist von größter Bedeutung, um ein gemeinsames hohes Maß an Wirksamkeit und Abwehrfähigkeit zu gewährleisten, insbesondere im Hinblick auf das Funktionieren der gesamten öffentlichen Verwaltung auf nationaler und EU-Ebene, da letztere auf der Grundlage der Verträge eine immer wichtigere Rolle spielt.

14. Der EDSB **bedauert**, dass der Vorschlag weder in der Begründung noch in den einschlägigen Erwägungsgründen 4 und 5 hinreichend erläutert, auf welche Weise er sich an die NIS-Richtlinie und den NIS-2-Vorschlag anpasst und inwiefern er durch die Verknüpfung mit der NIS-Richtlinie und dem NIS-2-Vorschlag einen Beitrag zum Cybersicherheitsniveau der Union insgesamt leistet.

15. Angesichts der wesentlichen und wichtigen Rolle der Organe, Einrichtungen und sonstigen Stellen der Union für das Funktionieren der Union **vertritt der EDSB die Auffassung, dass die Mindestsicherheitsanforderungen des Vorschlags** im Einklang mit Artikel 3 des NIS-2-Vorschlags („Mindestharmonisierung") **zumindest den Mindestsicherheitsanforderungen der Einrichtungen entsprechen sollten, die in den Anwendungsbereich der NIS-Richtlinie und des NIS-2-Vorschlags fallen**. Daher **empfiehlt** der EDSB, in einen Erwägungsgrund aufzunehmen, dass **der Vorschlag auf dem NIS-2-Vorschlag aufbaut**, und in den Erwägungsgründen 4 und 5 den Zusammenhang zwischen dem Vorschlag und der NIS-Richtlinie sowie dem NIS-2-Vorschlag näher zu erläutern. Darüber hinaus empfiehlt der EDSB, folgenden Wortlaut in den verfügenden Teil aufzunehmen: „Die Mindestsicherheitsanforderungen sollten mindestens den Mindestsicherheitsanforderungen der in den Anwendungsbereich des NIS-2-Vorschlags fallenden Einrichtungen entsprechen oder darüber liegen."

16. Insbesondere **stellt** der EDSB **fest**, dass der Vorschlag in den folgenden Punkten **nicht vollständig mit dem NIS-2-Vorschlag übereinstimmt**:

- In Artikel 5 Absatz 1 des NIS-2-Vorschlags heißt es: „Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden".

[1] *Ziffer 25 der NIS-2-Stellungnahme des EDSB.*

Der EDSB schlägt vor, in dem Vorschlag die Annahme **einer gemeinsamen Cybersicherheitsstrategie aller Organe, Einrichtungen und sonstigen Stellen der Union** vorzusehen, die den Anforderungen des Artikels 5 des NIS-2-Vorschlags entspricht.

- Es scheint eine gewisse Diskrepanz zwischen den Mindestcybersicherheitsmaßnahmen[2] des Vorschlags und den in Artikel 18 des NIS-2-Vorschlags aufgeführten Mindestmaßnahmen zu geben. In diesem Zusammenhang **bedauert der EDSB, dass der Vorschlag keinen ausdrücklichen Verweis auf die Verwendung von Kryptografie und Verschlüsselung (und End-to-End-Verschlüsselung) enthält**, bei denen es sich um wesentliche Technologien zum Schutz aller ruhenden Informationen und von Informationen während der Übertragung sowie zum Schutz der elektronischen Kommunikation handelt.

- Im Gegensatz zum NIS-2-Vorschlag[3] enthält der Vorschlag keine Bestimmungen über die **Zusammenarbeit** zwischen dem CERT-EU und dem Interinstitutionellen Cybersicherheitsbeirat **mit dem Europäischen Datenschutzbeauftragten**. **Der EDSB empfiehlt nachdrücklich, diese Zusammenarbeit durch eine Bestimmung des Vorschlags zu institutionalisieren**, damit der EDSB Entwicklungen im Bereich der Cybersicherheit, die sich auf die Sicherheit personenbezogener Daten der Organe, Einrichtungen und sonstigen Stellen der Union auswirken könnten, beobachten und die Einhaltung der Cybersicherheitsmaßnahmen überwachen kann. Auf diesen Punkt wird in Abschnitt 3.3 näher eingegangen.

3. Spezifische Anmerkungen

3.1. Anwendungsbereich des Vorschlags und Verhältnis zu den Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre

17. Der EDSB stellt fest, dass es sich bei den unter den Vorschlag fallenden Einrichtungen um dieselben Einrichtungen handelt, die der EU-DSVO unterliegen, also um die „Organe, Einrichtungen und sonstigen Stellen der Union“ (Union institutions, bodies, offices and agencies). Dieser Begriff findet sich zwar im Titel des Vorschlags, doch wird im restlichen Text der Begriff „Organe, Einrichtungen und sonstige Stellen der Union“ (Union institutions, bodies and agencies) verwendet. Der EDSB **empfiehlt**, den Begriff **„Organe, Einrichtungen und sonstige Stellen der Union“** im gesamten Vorschlag einheitlich zu verwenden, um Missverständnisse zu vermeiden.

18. Der EDSB weist erneut darauf hin[4], dass in Artikel 4 Absatz 1 Buchstabe f EU-DSVO **die Sicherheit als einer der wichtigsten Grundsätze für die Verarbeitung**

[2] *Anhänge I und II des Vorschlags*
[3] *Erwägungsgründe 58 und 77, Artikel 28 und 32 des NIS-2-Vorschlags.*
[4] *Ziffer 10 der NIS-2-Stellungnahme des EDSB.*

personenbezogener Daten verankert ist. In Artikel 33 EU-DSVO wird diese Verpflichtung, die sowohl für Verantwortliche als auch für Auftragsverarbeiter gilt, weiter ausgeführt, um ein angemessenes Maß an Sicherheit personenbezogener Daten zu gewährleisten. Beide Bestimmungen besagen in aller Deutlichkeit, dass **die Sicherheit personenbezogener Daten für die Einhaltung des EU-Datenschutzrechts unerlässlich ist**.

19. Der EDSB stellt einerseits fest, dass der Vorschlag die gleiche Definition von Cybersicherheit verwendet wie der NIS-2-Vorschlag: „*Tätigkeiten, die zum Schutz der Netz- und Informationssysteme, der Nutzer dieser Systeme und anderer von Cyberbedrohungen betroffener Personen erforderlich sind*“, wobei Cyberbedrohung „*alle potenziellen Umstände, Ereignisse oder Handlungen bezeichnet, die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnten*“[5]. Aus dieser Definition geht klar hervor, dass das Ziel der Cybersicherheit einen anderen Schwerpunkt hat als die Sicherheitsbestimmungen in Artikel 4 Absatz 1 Buchstabe f und Artikel 33 („Sicherheit personenbezogener Daten“) EU-DSVO. Während die Cybersicherheit darauf abzielt, „*Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen*“ vor Cyberbedrohungen zu schützen, verfolgt die Sicherheit personenbezogener Daten ein anderes spezifisches Ziel, nämlich den Schutz personenbezogener Daten vor **allen Bedrohungen** (einschließlich Cyberbedrohungen), die nachteilige Auswirkungen auf die **Rechte und Freiheiten des Einzelnen** haben können. Aus diesem Grund hat der EDSB in Ziffer 10 der NIS-2-Stellungnahme erklärt, dass **durch die Verbesserung der Cybersicherheit auch die Sicherheit personenbezogener Daten sowie der Privatsphäre in der elektronischen Kommunikation verbessert werden**. Diese Bemerkung behält auch im vorliegenden Zusammenhang ihre Gültigkeit.

20. Der EDSB weist jedoch darauf hin[6], dass die Verfolgung der Ziele der Cybersicherheit zur Anwendung von Maßnahmen führen kann, die in die Rechte des Einzelnen auf Datenschutz und Privatsphäre eingreifen. Das bedeutet, dass **jede potenzielle Einschränkung des Rechts auf Schutz personenbezogener Daten und der Privatsphäre den Anforderungen von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union entsprechen muss**, insbesondere wenn sie im Wege legislativer Maßnahmen erlassen werden, die sowohl notwendig als auch verhältnismäßig sein und den Wesensgehalt des Rechts achten müssen.

21. Um mit dem Vorschlag in Einklang zu stehen, müssen die Organe, Einrichtungen und sonstigen Stellen der Union sowie das CERT-EU bestimmte Cybersicherheitsverfahren und -maßnahmen einführen, **die zwangsläufig zusätzliche Verarbeitungen personenbezogener Daten mit sich bringen**. Solche Maßnahmen würden in Bezug auf das Cybersicherheitsrisikomanagement ergriffen oder weil sie auf der Liste der Mindestmaßnahmen im Bereich der Cybersicherheit[7], wie Zugangskontrolle, Kommunikationssicherheit, Bewältigung von Sicherheitsvorfällen und Multifaktor-Authentifizierung, stehen.

---

[5] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final.
[6] Ziffer 11 der NIS-2-Stellungnahme des EDSB.
[7] Anhänge I und II des Vorschlags.

22. Vor diesem Hintergrund stellt der EDSB fest, dass Organisationen, die als Verantwortliche und Auftragsverarbeiter fungieren, nicht immer erkennen, dass die in Cybersicherheitssystemen und -diensten verarbeiteten Daten personenbezogene Daten darstellen können (z. B. IP-Adressen, Gerätekennungen, Netzwerkprotokolldateien, Protokolldateien für Zugangskontrollen usw.). Dies erhöht die Gefahr der Nichteinhaltung der Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre, z. B. der Grundsätze der Rechtmäßigkeit der Verarbeitung, der Zweckbindung, der Datenminimierung, der Speicherbeschränkungen und der Verpflichtungen für rechtmäßige Datenübermittlungen. Um alle Zweifel auszuräumen, sollte nach Auffassung des EDSB in einem neuen Erwägungsgrund Folgendes klargestellt werden: **„Alle Cybersicherheitssysteme und -dienste, die an der Prävention und Erkennung von Cyberbedrohungen und der Reaktion darauf beteiligt sind, sollten mit dem geltenden Datenschutzrahmen und dem Rahmen für den Schutz der Privatsphäre im Einklang stehen und entsprechende technische und organisatorische Sicherheitsvorkehrungen treffen, um über diese Einhaltung auch Rechenschaft ablegen zu können“**.

23. Der EDSB **begrüßt** Erwägungsgrund 22, wonach alle im Rahmen dieses Vorschlags verarbeiteten personenbezogenen Daten im Einklang mit den Datenschutzvorschriften, einschließlich der Verordnung (EU) 2018/1725, verarbeitet werden sollten. Darüber hinaus empfiehlt der EDSB, in diesem Erwägungsgrund Folgendes hinzuzufügen: **„Der Vorschlag zielt nicht darauf ab, die Anwendung der geltenden EU-Rechtsvorschriften über die Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse des EDSB, zu beeinträchtigen“.**

24. Der EDSB **hält fest**, dass nach Artikel 18 Absatz 3 die Verarbeitung personenbezogener Daten im Rahmen dieses Vorschlags der EU-DSVO unterliegt, was den Eindruck erweckt, dass dies nur im Zusammenhang mit der Informationsverarbeitung durch das CERT-EU und die Organe, Einrichtungen und sonstigen Stellen der Union erforderlich ist. Zur Vermeidung jeglicher Fehlinterpretation **empfiehlt** der EDSB, die Bestimmung von Artikel 18 Absatz 3 in den Erwägungsgrund 22 zu verschieben, damit **jede Verarbeitung personenbezogener Daten** durch das CERT-EU und die Organe, und Einrichtungen und sonstigen Stellen der Union im Zusammenhang mit dem Vorschlag abgedeckt ist, darunter, wenn auch nicht ausschließlich, die Cybersicherheitsdienste des CERT-EU nach Artikel 12, die Weitergabe von Informationen nach Artikel 18, die Weitergabepflichten nach Artikel 19, Maßnahmen mit Verarbeitung personenbezogener Daten im Zusammenhang mit den Cybersicherheitsrisikomanagement nach Artikel 4 sowie die Liste der Mindestmaßnahmen im Bereich Cybersicherheit[8] des Vorschlags, bei denen personenbezogene Daten verarbeitet werden.

25. Sieht ein Rechtsakt der Union die Verarbeitung personenbezogener Daten vor, so müssen die betreffenden Rechtsvorschriften der Union klare und präzise Regeln für den Anwendungsbereich und die Anwendung der betreffenden Maßnahme festlegen und Mindestgarantien vorsehen, damit die Personen, deren Daten verarbeitet werden, ausreichende Garantien dafür haben, dass ihre personenbezogenen Daten wirksam vor Missbrauchsrisiken und vor unrechtmäßigem Zugriff und unrechtmäßiger Nutzung dieser Daten geschützt sind (vgl. EuGH, Urteil vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 54, und entsprechend, in Bezug auf Artikel 8

[8] *Anhänge I und II des Vorschlags.*

EMRK, EGMR, *Liberty u. a./Vereinigtes Königreich*, Urteil vom 1. Juli 2008, Nr. 58243/00, Rn. 62 und 63; *Rotaru/Rumänien*, Rn. 57 bis 59, und *S. und Marper/Vereinigtes Königreich*, Rn. 99)

26. Um Rechtssicherheit und Vorhersehbarkeit zu erreichen und die Einhaltung der EU-DSVO, insbesondere von Artikel 5 Absatz 1 Buchstabe a und Absatz 2, zu gewährleisten, **empfiehlt der EDSB nachdrücklich, im Vorschlag eine eindeutige Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch das CERT-EU und die Organe, Einrichtungen und sonstigen Stellen der Union zu schaffen**, und unter anderem insbesondere die Zwecke der Verarbeitung und die Kategorien personenbezogener Daten zu regeln. Darüber hinaus sollten die folgenden Elemente ausdrücklich festgelegt werden: a) Angabe des/der Verantwortlichen, des Auftragsverarbeiters oder gegebenenfalls der gemeinsam Verantwortlichen; b) Kategorien betroffener Personen; c) Aufbewahrungsfristen oder zumindest Kriterien für die Festlegung solcher Zeiträume. Nach Auffassung des EDSB sollten diese Elemente ausdrücklich in dem Vorschlag oder zumindest in einem delegierten Rechtsakt enthalten sein, der später von der Kommission erlassen wird. Der Vorschlag sollte einen solchen delegierten Rechtsakt vorsehen.

3.2. Synergien mit dem Datenschutz und dem Schutz der Privatsphäre

27. Der EDSB weist erneut[9] darauf hin, dass **die Einbeziehung der Perspektive des Schutzes der Privatsphäre und des Datenschutzes in das traditionelle Cybersicherheitsmanagement einen ganzheitlichen Ansatz gewährleisten und somit wichtige Synergien für die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verwaltung der Cybersicherheit und beim Schutz der von ihnen verarbeiteten Informationen ohne sinnlose Mehrarbeit ermöglichen wird.**

28. Der Einsatz von Technologien zur Verbesserung der Cybersicherheit sollte die Rechte und Freiheiten des Einzelnen nicht unangemessen beeinträchtigen. Der erste Schritt zur Vermeidung oder Minderung dieser Risiken besteht in der Anwendung der Anforderungen des **Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen** gemäß Artikel 27 EU-DSVO, die dazu beitragen werden, geeignete Garantien wie **Pseudonymisierung, Verschlüsselung, Richtigkeit der Daten, Datenminimierung** bei der Gestaltung und Nutzung von Cybersicherheitstechnologien und -systemen zu integrieren.

29. Der EDSB möchte erneut darauf hinweisen, **dass Verschlüsselung, einschließlich End-to-End-Verschlüsselung, eine entscheidende und unersetzliche Technologie für einen wirksamen Datenschutz und einen wirksamen Schutz der Privatsphäre ist**. Verschlüsselung ist **sehr wirksam im Hinblick auf Cybersicherheitsrisiken**, und dazu erreicht sie dies **ohne zusätzliche Verarbeitung personenbezogener Daten**.

30. Angesichts der immer häufigeren Nutzung und Einführung von Cloud-Diensten durch die Organe, Einrichtungen und sonstigen Stellen der Union **empfiehlt der EDSB**

[9] *Ziffer 16 der NIS-2-Stellungnahme des EDSB.*

nachdrücklich, „Verschlüsselung im Ruhezustand", „Verschlüsselung während der Übertragung" sowie „End-to-End-Verschlüsselung" in die Liste der Mindestmaßnahmen im Bereich der Cybersicherheit in Anhang II des Vorschlags aufzunehmen.

31. Wie bereits bei früheren Gelegenheiten betont, ist das Management der Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten eine Verpflichtung nach Artikel 33 EU-DSVO. Während die Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit in Artikel 4 des Vorschlags darauf abzielen, Netz- und Informationssysteme der Organisation (und die darin enthaltenen Daten) zu schützen, zielt Artikel 33 EU-DSVO darauf ab, Einzelpersonen (die nicht unbedingt derselben Organisation angehören) und ihre Rechte durch den Schutz ihrer Daten zu schützen. Es gibt einen Unterschied zwischen den Gütern, die bei den beiden Tätigkeiten geschützt werden sollen, was unter bestimmten Umständen zu unterschiedlichen Schlussfolgerungen führen könnte. Zugleich kann das Verfahren für das Risikomanagement im Bereich Cybersicherheit dazu beitragen, die Auswirkungen von Schwachstellen bei der Sicherheit personenbezogener Daten auf den Datenschutz zu bewerten. Aus diesem Grund empfiehlt der EDSB, **die Aspekte des Schutzes der Privatsphäre und des Datenschutzes in das Cybersicherheitsrisikomanagement einzubeziehen**, um einen ganzheitlichen Ansatz zu gewährleisten und Synergien ohne sinnlose Mehrarbeit zu ermöglichen.

32. Was schließlich Cybersicherheitsvorfälle betrifft, die möglicherweise eine Verletzung des Schutzes personenbezogener Daten zur Folge haben, oder eine Verletzung des Schutzes personenbezogener Daten, die auf einen Cybersicherheitsvorfall hindeutet, ist es **dringend ratsam, in einem entsprechenden Erwägungsgrund** die Vorteile eines **integrierten Verfahrens zur Bewältigung von Sicherheitsvorfällen zu erläutern[10], das sowohl den Cybersicherheits- als auch den Datenschutzverpflichtungen bei Meldungen von Verletzungen des Schutzes personenbezogener Daten dient**. Auf diese Weise kann der Verantwortliche Zeit und Ressourcen sparen und in beiden Bereichen viel effizienter auf Vorfälle reagieren.

33. Um solche Synergien zwischen Cybersicherheit und Datenschutz sicherzustellen, **empfiehlt der EDSB nachdrücklich, dass der Vorschlag eine spezifische Verpflichtung für den lokalen Cybersicherheitsbeauftragten im Sinne von Artikel 4 Absatz 5 vorsieht, mit dem gemäß Artikel 43 EU-DSVO benannten Datenschutzbeauftragten zusammenzuarbeiten**, wenn es um sich überschneidende Tätigkeiten wie die Anwendung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf Cybersicherheitsmaßnahmen, die Auswahl von Cybersicherheitsmaßnahmen, bei denen personenbezogene Daten betroffen sind, ein integriertes Risikomanagement und die integrierte Behandlung von Sicherheitsvorfällen geht.

[10] *Siehe auch die Leitlinien des EDPS zur Meldung von Verletzungen des Schutzes personenbezogener Daten.*

3.3. Die Rolle des EDSB

34. Der EDSB stellt fest, dass der Vorschlag trotz des oben beschriebenen wichtigen Zusammenspiels zwischen Cybersicherheit und Datenschutz und Schutz der Privatsphäre **keinen Verweis auf den EDSB enthält**.

35. Der EDSB muss in beide Aspekte einbezogen werden, um einerseits **Entwicklungen im Bereich der Cybersicherheit zu überwachen**, die Auswirkungen auf den Datenschutz und den Schutz der Privatsphäre haben können, und andererseits **die Einhaltung der Cybersicherheitsmaßnahmen**, die personenbezogene Daten betreffen, **zu überwachen und sicherzustellen**.

36. Im Gegensatz zum Vorschlag enthalten die Artikel 28 und 32 des NIS-2-Vorschlags spezifische Bestimmungen für die **Zusammenarbeit zwischen Cybersicherheits- und Datenschutzbehörden**.

37. **Um die Kohärenz zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union zu gewährleisten**, und im Einklang mit Artikel 28 des NIS-2-Vorschlags **empfiehlt der EDSB nachdrücklich**, in Artikel 12 „Auftrag und Aufgaben des CERT-EU" des Vorschlags eine Bestimmung aufzunehmen, wonach das **„CERT-EU bei der Bewältigung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten oder zu einer Verletzung der Vertraulichkeit der elektronischen Kommunikation führen, eng mit dem EDSB zusammenarbeitet"**.

38. In diesem Sinne ist der EDSB der Auffassung, dass das **CERT-EU den EDSB informieren muss, wenn es um die Behebung erheblicher Schwachstellen, erheblicher Sicherheitsvorfälle oder schwerer Angriffe geht, die zu Verletzungen des Schutzes personenbezogener Daten und/oder zur Verletzung der Vertraulichkeit der elektronischen Kommunikation führen können**. Eine entsprechende Verpflichtung sollte in Artikel 12 „Auftrag und Aufgaben des CERT-EU" des Vorschlags aufgenommen werden.

39. Darüber hinaus **empfiehlt** der EDSB, in Artikel 12 vorzusehen, dass der EDSB an den Maßnahmen des CERT-EU zur Sensibilisierung der Organe, Einrichtungen und sonstigen Stellen der Union im Bereich Cybersicherheit beteiligt wird, um das Zusammenspiel zwischen Verletzungen des Schutzes personenbezogener Daten und Cybersicherheitsvorfällen abzudecken.

40. Darüber hinaus **empfiehlt** der EDSB im Einklang mit Artikel 32 des NIS-2-Vorschlags, in Artikel 12 „Auftrag und Aufgaben des CERT-EU" des Vorschlags eine Bestimmung aufzunehmen, wonach das **CERT-EU den EDSB unverzüglich zu unterrichten hat, wenn ihm Hinweise darauf vorliegen, dass ein Verstoß der Organe, Einrichtungen und sonstigen Stellen der Union gegen die in dem Vorschlag festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten nach sich zieht**.

41. Der EDSB steht nicht auf der Liste der ständigen Teilnehmer des in Artikel 9 des Vorschlags definierten „Interinstitutionellen Cybersicherheitsbeirats" („IICB"). Wie bereits erwähnt, ist die Sicherheit der Verarbeitung personenbezogener Daten und damit auch die Cybersicherheit einer der Eckpfeiler des Datenschutzes. Darüber hinaus ist der EDSB

gemäß Artikel 57 Absatz 1 Buchstabe h EU-DSVO beauftragt, maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie. Dies schließt Entwicklungen im Bereich der Cybersicherheit ein; um also spezifische Datenschutzleitlinien im Zusammenhang mit Cybersicherheit herausgeben zu können, **empfiehlt der EDSB nachdrücklich, den Europäischen Datenschutzbeauftragten in Artikel 9 Absatz 3 als ständigen Teilnehmer am IICB mit einem Vertreter aufzunehmen.**

3.4. Informationsaustausch und CERT-EU-Dienste

42. Gemäß Artikel 12 erbringt das CERT-EU bestimmte Cybersicherheitsdienste, bei denen es als Auftragsverarbeiter für Cybersicherheitsinformationen fungiert, die personenbezogene Daten enthalten. Es muss von Anfang an sichergestellt sein, dass diese Datenverarbeitungstätigkeiten in vollem Einklang mit der EU-DSVO und der DSGVO stehen.

43. Artikel 16 Absatz 2 besagt: „Das CERT-EU kann spezifische Informationen über Sicherheitsvorfälle ohne Einwilligung des betroffenen Konstituenten an diese entsprechenden nationalen Stellen weitergeben, um die Aufdeckung ähnlicher Cyberberdrohungen oder Sicherheitsvorfälle zu erleichtern"; und weiter heißt es dort: „Das CERT-EU kann spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der Zielgruppe des Sicherheitsvorfalls hervorgeht, nur mit Einwilligung des betroffenen Konstituenten weitergeben".

44. Nach Artikel 19 kann das CERT-EU von den Organen, Einrichtungen und sonstigen Stellen der Union verlangen, ihm Informationen aus ihren IT-Systemverzeichnissen zu übermitteln, um das Management von Sicherheitslücken und die Bewältigung von Sicherheitsvorfällen zu koordinieren. Darüber hinaus sind die Organe, Einrichtungen und sonstigen Stellen der Union gehalten, dem CERT-EU auf Anfrage unverzüglich die digitalen Informationen zur Verfügung zu stellen, die bei der Nutzung der an den jeweiligen Sicherheitsvorfällen beteiligten Geräte erzeugt wurden.

45. Nach Auffassung des EDSB besteht eine hohe Wahrscheinlichkeit, dass die vorfallspezifischen Informationen sowie die digitalen Informationen, die bei der Nutzung von den an den jeweiligen Vorfällen beteiligten elektronischen Geräten erzeugt werden, personenbezogene Daten enthalten werden. Im Sinne der erforderlichen Rechtsklarheit, Rechtssicherheit und Vorhersehbarkeit empfiehlt der EDSB daher, die Kategorien personenbezogener Daten, die bei diesem Austausch verarbeitet werden sollen, den Zweck/die Zwecke der Verarbeitung, die Empfänger der Daten und die mögliche Datenübermittlung zu präzisieren. Nach Auffassung des EDSB sollten diese Elemente ausdrücklich in dem Vorschlag oder zumindest in einem delegierten Rechtsakt enthalten sein, der später von der Kommission erlassen wird. Der Vorschlag sollte einen solchen delegierten Rechtsakt vorsehen.

46. Darüber hinaus stellt der EDSB fest, dass der Begriff „Einwilligung" verwendet wird, den der Gesetzgeber bereits in Artikel 3 Absatz 15 EU-DSVO definiert hat. Da sich der Vorschlag im Zusammenhang mit Artikel 16 Absatz 2 auf EUIBA („Konstituenten") und nicht auf

betroffene Personen bezieht, schlägt der EDSB vor, anstelle von „Einwilligung“ den Begriff „Genehmigung“ zu verwenden.

47. In Artikel 17 Absatz 3 heißt es: „Das CERT-EU kann, mit Einwilligung des von einem Sicherheitsvorfall betroffenen Konstituenten, Informationen über diesen Sicherheitsvorfall an Partner weitergeben, die zu seiner Analyse beitragen können.“ Der EDSB erinnert daran, dass solche internationalen Datenübermittlungen in vollem Einklang mit Kapitel V der EU-DSVO stehen sollten. Der EDSB empfiehlt daher, in den Vorschlag einen Erwägungsgrund aufzunehmen, der sich auf das genannte Kapitel bezieht.

4. Schlussfolgerungen

48. Vor diesem Hintergrund spricht der EDSB folgende Hauptempfehlungen aus:

- Der EDSB empfiehlt, in einen Erwägungsgrund aufzunehmen, dass der Vorschlag auf dem NIS-2-Vorschlag aufbaut, und in den Erwägungsgründen 4 und 5 den Zusammenhang zwischen dem Vorschlag und der NIS-Richtlinie sowie dem NIS-2-Vorschlag näher zu erläutern. Darüber hinaus empfiehlt der EDSB, folgenden Wortlaut in den verfügenden Teil aufzunehmen: „Die Mindestsicherheitsanforderungen sollten mindestens den Mindestsicherheitsanforderungen der Einrichtungen der NIS-Richtlinie und des NIS-2-Vorschlags entsprechen oder darüber liegen.“

- Der EDSB empfiehlt nachdrücklich, im Vorschlag eine eindeutige Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch das CERT-EU und die Organe, Einrichtungen und sonstigen Stellen der Union zu schaffen und unter anderem insbesondere die Zwecke der Verarbeitung und die Kategorien personenbezogener Daten zu regeln. Darüber hinaus sollten die folgenden Elemente ausdrücklich festgelegt werden: a) Angabe des/der Verantwortlichen, des Auftragsverarbeiters oder gegebenenfalls der gemeinsam Verantwortlichen; b) Kategorien betroffener Personen; c) Aufbewahrungsfristen oder zumindest Kriterien für die Festlegung solcher Zeiträume. Nach Auffassung des EDSB sollten diese Elemente ausdrücklich in dem Vorschlag oder zumindest in einem delegierten Rechtsakt enthalten sein, der später von der Kommission erlassen wird. Der Vorschlag sollte einen solchen delegierten Rechtsakt vorsehen.

- Der EDSB empfiehlt nachdrücklich, „Verschlüsselung im Ruhezustand“, „Verschlüsselung während der Übertragung“ sowie „End-to-End-Verschlüsselung“ in die Liste der Mindestmaßnahmen im Bereich der Cybersicherheit in Anhang II des Vorschlags aufzunehmen.

- Der EDSB empfiehlt nachdrücklich, dass der Vorschlag eine spezifische Verpflichtung für den lokalen Cybersicherheitsbeauftragten im Sinne von Artikel 4 Absatz 5 vorsieht, mit dem gemäß Artikel 43 EU-DSVO benannten Datenschutzbeauftragten zusammenzuarbeiten, wenn es um sich überschneidende Tätigkeiten wie die Anwendung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf Cybersicherheitsmaßnahmen, die Auswahl von Cybersicherheitsmaßnahmen, bei denen personenbezogene Daten

betroffen sind, ein integriertes Risikomanagement und die integrierte Behandlung von Sicherheitsvorfällen geht.

- Der EDSB empfiehlt nachdrücklich, in Artikel 12 „Auftrag und Aufgaben des CERT-EU“ des Vorschlags eine Bestimmung aufzunehmen, wonach „das CERT-EU bei der Bewältigung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten oder zu einer Verletzung der Vertraulichkeit der elektronischen Kommunikation führen, eng mit dem EDSB zusammenarbeitet“.

- Der EDSB empfiehlt, eine Verpflichtung für das CERT-EU aufzunehmen, den EDSB zu informieren, wenn es um die Behebung erheblicher Schwachstellen, erheblicher Sicherheitsvorfälle oder schwerer Angriffe geht, die zu Verletzungen des Schutzes personenbezogener Daten und/oder zu einer Verletzung der Vertraulichkeit der elektronischen Kommunikation führen können.

- Der EDSB empfiehlt, in Artikel 12 vorzusehen, dass der EDSB an den Maßnahmen des CERT-EU zur Sensibilisierung der Organe, Einrichtungen und sonstigen Stellen der Union im Bereich Cybersicherheit beteiligt wird, um das Zusammenspiel zwischen Verletzungen des Schutzes personenbezogener Daten und Cybersicherheitsvorfällen abzudecken.

- Der EDSB empfiehlt, in Artikel 12 „Auftrag und Aufgaben des CERT-EU“ des Vorschlags eine Bestimmung aufzunehmen, wonach das CERT-EU den EDSB unverzüglich zu unterrichten hat, wenn ihm Hinweise darauf vorliegen, dass ein Verstoß der Organe, Einrichtungen und sonstigen Stellen der Union gegen die in dem Vorschlag festgelegten Pflichten eine Verletzung des Schutzes personenbezogener Daten nach sich zieht.

- Der EDSB empfiehlt nachdrücklich, dass der Europäische Datenschutzbeauftragte in Artikel 9 Absatz 3 als ständiger Teilnehmer am IICB mit einem Vertreter aufgenommen wird.

Brüssel, den 17. Mai 2022

Wojciech Rafał WIEWIÓROWSKI

[elektronisch unterzeichnet]

Endnoten

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] COM(2022) 122 final.
[3] COM(2022) 119 final.
[4] Die Cybersicherheitsstrategie der EU für die digitale Dekade – Gestaltung der digitalen Zukunft Europas (europa.eu), einschließlich einer gemeinsamen Mitteilung mit dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik (JOIN(2020)18).
[5] Siehe Kapitel I. EINLEITUNG der Strategie, S. 5.
[6] Gemeinsame Mitteilung der Europäische Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade".
[7] Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie.
[8] Die derzeitige Rolle des CERT-EU ergibt sich aus der Interinstitutionellen Vereinbarung 2018/C 12/01.
[9] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295/39 vom 21.11.2018).