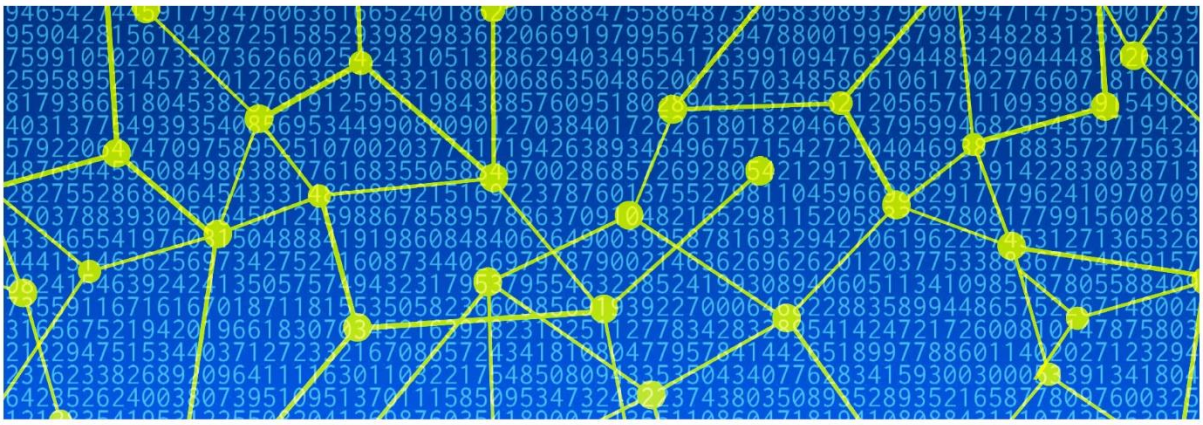

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 5/2021

zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie

EDPS

11. März 2021

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 Wiewiórowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.

Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 besagt: „Nach 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, konsultiert die Kommission den EDSB", und gemäß Artikel 57 Absatz 1 Buchstabe g muss der EDSB „von sich aus oder auf Anfrage alle Organe und Einrichtungen der Union bei legislativen und administrativen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten beraten".

Die vorliegende Stellungnahme wird vom EDSB innerhalb von acht Wochen nach Eingang des Konsultationsersuchens nach Artikel 42 Absatz 3 der Verordnung (EU) 2018/1725 abgegeben, und sie befasst sich mit den Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten des Vorschlags der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148.

Zusammenfassung

Am 16. Dezember 2020 nahm die Europäische Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (im Folgenden „Vorschlag“) an. Parallel dazu veröffentlichten die Europäische Kommission und der Hohe Vertreter der Union für Außen- und Sicherheitspolitik eine Gemeinsame Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade“ (im Folgenden „Strategie“).

Der EDSB unterstützt uneingeschränkt das übergeordnete Ziel der Strategie, mit der ein globales und offenes Internet mit starken Schutzvorkehrungen für die Risiken für die Sicherheit und die Grundrechte gewährleistet werden soll, wobei gleichzeitig der strategische Wert des Internets und seiner Verwaltung anerkannt und das Handeln der Union darin in einem Multi-Stakeholder-Modell ausgebaut wird.

Der EDSB begrüßt daher gleichermaßen das Ziel des Vorschlags, systemische und strukturelle Änderungen an der derzeitigen NIS-Richtlinie vorzunehmen, um ein breiteres Spektrum von Einrichtungen in der gesamten Union mit strengeren Sicherheitsmaßnahmen, einschließlich obligatorischen Risikomanagements Mindeststandards und einschlägigen Aufsichts- und Durchsetzungsbestimmungen, abzudecken. In diesem Zusammenhang hält es der EDSB für **erforderlich, die Organe, Einrichtungen und sonstigen Stellen der Union vollständig in den EU-weiten Gesamtrahmen für Cybersicherheit einzubeziehen**, um ein einheitliches Schutzniveau zu erreichen, **indem die Organe, Einrichtungen und sonstigen Stellen der Union ausdrücklich in den Anwendungsbereich des Vorschlags einbezogen werden**.

Der EDSB betont ferner, wie wichtig es ist, **die Perspektive des Schutzes der Privatsphäre und des Datenschutzes in die Cybersicherheitsmaßnahmen zu integrieren**, die sich aus dem Vorschlag oder aus anderen Cybersicherheitsinitiativen der Strategie ergeben, um einen ganzheitlichen Ansatz zu gewährleisten und Synergien beim Management der Cybersicherheit und beim Schutz der von ihnen verarbeiteten personenbezogenen Informationen zu ermöglichen. Ebenso wichtig ist, dass jede etwaige Einschränkung des Rechts auf Schutz personenbezogener Daten und der Privatsphäre, die sich aus solchen Maßnahmen ergibt, die in Artikel 52 der Charta der Grundrechte der Europäischen Union festgelegten Kriterien erfüllt und insbesondere durch legislative Maßnahmen erreicht wird und sowohl notwendig als auch verhältnismäßig ist.

Der EDSB begrüßt die Tatsache, dass **der Vorschlag nicht versucht, die Anwendung der bestehenden EU-Rechtsvorschriften über die Verarbeitung personenbezogener Daten** zu beeinträchtigen, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, denen die Überwachung der Einhaltung dieser Vorschriften obliegt. Das bedeutet, dass alle Cybersicherheitssysteme und -dienste, die an der Prävention und Erkennung von Cyberbedrohungen und der Reaktion darauf beteiligt sind, mit dem geltenden Rahmen für den Schutz der Privatsphäre und den Datenschutz im Einklang stehen sollten. In diesem Zusammenhang hält es der EDSB für wichtig und notwendig, für die Zwecke des Vorschlags eine klare und eindeutige Definition des Begriffs „Cybersicherheit“ festzulegen.

Der EDSB formuliert spezifische Empfehlungen, um sicherzustellen, dass der Vorschlag **die bestehenden Rechtsvorschriften der Union zum Schutz personenbezogener Daten**, insbesondere die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation,

korrekt und wirksam **ergänzt**, indem er erforderlichenfalls auch den EDSB und den Europäischen Datenschutzausschuss einbezieht und klare Mechanismen für die Zusammenarbeit zwischen den zuständigen Behörden aus den verschiedenen Regelungsbereichen schafft.

Darüber hinaus sollten in den Bestimmungen über die Verwaltung von **Registern von Internet-Domänennamen der obersten Stufe** der Anwendungsbereich und die rechtlichen Bedingungen im Gesetz eindeutig festgelegt werden. Das Konzept der proaktiven Überprüfungen auf Schwachstellen von Netz- und Informationssystemen durch die CSIRT erfordert ebenfalls weitere Klarstellungen bezüglich des Umfangs und der Arten der verarbeiteten personenbezogenen Daten. Hingewiesen wird auf die Risiken für mögliche nicht konforme Datenübermittlungen im Zusammenhang mit der Auslagerung von Cybersicherheitsdiensten oder der Beschaffung von Cybersicherheitsprodukten und ihrer Lieferkette.

Der EDSB **begrüßt die Forderung nach der Förderung der Verwendung von Verschlüsselung**, insbesondere der End-zu-End-Verschlüsselung, und bekräftigt seinen Standpunkt zur Verschlüsselung als kritische und unersetzliche Technologie für einen wirksamen Datenschutz und Schutz der Privatsphäre, deren Umgehung den Mechanismus aufgrund seiner möglichen unrechtmäßigen Nutzung und des Verlusts des Vertrauens in Sicherheitskontrollen jeglicher Schutzfähigkeit beraubt. Zu diesem Zweck sollte klargestellt werden, **dass keine Bestimmung des Vorschlags als Befürwortung einer Schwächung der End-zu-End-Verschlüsselung** durch „Hintertürchen“ oder ähnliche Lösungen ausgelegt werden sollte.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[1],

gestützt auf die Verordnung (EG) 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 und zum freien Datenverkehr[2], insbesondere auf Artikel 42 Absatz 1, Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c,

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[3] –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1. Am 16. Dezember 2020 nahm die Europäische Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (im Folgenden „Vorschlag“) an.[4]

2. Parallel dazu veröffentlichten die Europäische Kommission und der Hohe Vertreter der Union für Außen- und Sicherheitspolitik eine Gemeinsame Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade“ (im Folgenden „Strategie“).[5]

3. Die Strategie zielt darauf ab, 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 und die Grundrechte und Grundfreiheiten der Menschen in Europa zu begegnen.[6]

4. Die Strategie enthält Vorschläge für Regulierung, Investitionen und Politikvorgaben in drei Handlungsbereichen der EU: 1) Resilienz, technologische Souveränität und Führungsrolle, 2) Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion und 3) Förderung eines globalen und offenen Cyberraums.

5. Der Vorschlag ist eine der Regulierungsinitiativen der Strategie, und zwar insbesondere im Bereich Resilienz, technologische Souveränität und Führungsrolle.

6. Der Begründung zufolge zielt der Vorschlag darauf ab, den bestehenden Rechtsrahmen, d. h. die Richtlinie (EU) 2016/1148 („NIS-Richtlinie"), zu modernisieren.[7] Der Vorschlag soll auf der geltenden NIS-Richtlinie aufbauen und diese aufheben, die die erste EU-weite Rechtsvorschrift zur Cybersicherheit war und rechtliche Maßnahmen vorsieht, um das allgemeine Cybersicherheitsniveau in der Union anzuheben. Der Vorschlag trägt der zunehmenden Digitalisierung des Binnenmarkts in den letzten Jahren und einer sich verändernden Bedrohungslage im Bereich der Cybersicherheit Rechnung, die sich seit Beginn der COVID-19-Krise verschärft hat. Der Vorschlag zielt darauf ab, mehrere festgestellte Mängel der NIS-Richtlinie zu beheben, und soll die Resilienz all jener öffentlichen und privaten Sektoren, die eine wichtige Funktion für Wirtschaft und Gesellschaft erfüllen, erhöhen.

7. Zu den wichtigsten Elementen des Vorschlags gehören:

   (i) Die Ausweitung des Anwendungsbereichs der derzeitigen NIS-Richtlinie durch die Aufnahme neuer Sektoren aufgrund ihrer Kritikalität für Wirtschaft und Gesellschaft;
   (ii) strengere Sicherheitsanforderungen für erfasste Unternehmen und Einrichtungen durch Einführung eines Risikomanagementkonzepts, das eine Mindestliste der grundlegenden Sicherheitselemente enthält, die anzuwenden sind;
   (iii) Verbesserung der Sicherheit von Lieferketten und Lieferantenbeziehungen, indem einzelne Unternehmen verpflichtet werden, Cybersicherheitsrisiken in Lieferketten und Lieferantenbeziehungen anzugehen;
   (iv) Intensivierung der Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und mit den Organen, Einrichtungen und sonstigen Stellen der Union bei Tätigkeiten im Zusammenhang mit der Cybersicherheit, einschließlich des Cyber-Krisenmanagements.

8. Am 14. Januar 2021 ging beim EDSB ein Ersuchen der Europäischen Kommission um formelle Konsultation zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148" ein.

2. ALLGEMEINE BEMERKUNGEN

2.1. Zur Cybersicherheitsstrategie

9. Der EDSB begrüßt die Cybersicherheitsstrategie und unterstützt uneingeschränkt ihr Ziel, ein globales und offenes Internet mit starken Schutzvorkehrungen zu gewährleisten, um den Risiken für die Sicherheit und die Grundrechte zu begegnen, wobei gleichzeitig der strategische Wert des Internets und seiner Verwaltung anerkannt und das Handeln der Union darin in einem Multi-Stakeholder-Modell ausgebaut wird.

10. Nach Artikel 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 (DSGVO)[8] 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. Beide Bestimmungen machen deutlich, dass Sicherheit für die Einhaltung des EU-Datenschutzrechts unerlässlich ist. Aus diesem Grund ist auch der EDSB der Auffassung, dass die Verbesserung der Cybersicherheit für die Wahrung der Grundrechte und Grundfreiheiten, einschließlich des Rechts auf Privatsphäre und des Schutzes personenbezogener Daten, von wesentlicher Bedeutung ist, und unterstützt nachdrücklich den Vorschlag für ein umfassendes Paket einschlägiger wirksamer technischer und organisatorischer Maßnahmen.

11. Der EDSB weist jedoch darauf hin, 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[9] und den Wesensgehalt des Rechts achten müssen.

12. Sicherheitsvorschriften, Sicherheitskonzepte und Sicherheitsstandards bilden das Rückgrat eines ordnungsgemäßen Cybersicherheits- und Informationssicherheitsmanagements. Aus diesem Grund begrüßt der EDSB insbesondere die Absicht der Strategie, Folgendes festzulegen:
    - Sicherheitsvorschriften für die Cybersicherheit sowie für die Informationssicherheit der Organe, Einrichtungen und sonstigen Stellen der Union;
    - Sicherheitsvorschriften für die Cybersicherheit aller vernetzten Produkte (IoT) und zugehörigen Dienste;
    - Sicherheitsstandards für die Sicherheit von 5G-Netzen und Mobilfunknetzen der künftigen Generation mit besonderem Schwerpunkt auf der Sicherheit der Lieferkette.

13. Der EDSB unterstützt uneingeschränkt die Initiativen der Strategie im Bereich „technologische Souveränität und Führungsrolle“. In seiner Strategie für den Zeitraum 2020-2024[10] brachte der EDSB seine nachdrückliche Unterstützung für politische Initiativen zur Förderung der „digitalen Souveränität“ zum Ausdruck, bei denen in Europa erzeugte Daten in Werte für europäische Unternehmen und Einzelpersonen umgewandelt und im Einklang mit den europäischen Werten verarbeitet werden. Der EDSB begrüßt daher insbesondere die folgenden Initiativen:
    - den Aufbau eines Netzes von Sicherheitseinsatzzentren in der gesamten EU;
    - die Initiative zum Aufbau einer sicheren Quantenkommunikationsinfrastruktur (QCI), die mit europäischer Technik geschaffen wird;
    - den Aufbau eines öffentlichen europäischen DNS-Auflösungsdienstes;
    - die Einrichtung des Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes der Koordinierungszentren (CCCN), das die Entwicklung der technologischen Souveränität der EU unterstützen und die bei den wichtigsten Technologien bestehende Abhängigkeit von anderen Teilen der Welt verringern wird.

14. Der EDSB ist sich des Potenzials der künstlichen Intelligenz für die Entwicklung fortgeschrittener Cybersicherheitsfähigkeiten für die **Erkennung, Analyse, Eindämmung und Reaktion** auf Cyberbedrohungen in einer kontinuierlich erweiterten digitalen Landschaft **in Echtzeit** bewusst. Diese Technologien erfordern jedoch in der Regel die Verarbeitung großer Mengen personenbezogener Daten (z. B. Protokolldaten der Nutzer)

und gehen mit eigenen Risiken einher, die identifiziert und gemindert werden müssen (z. B. mangelnde Transparenz oder Voreingenommenheit). 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 25 DSGVO**, die dazu beitragen werden, geeignete Garantien wie Pseudonymisierung, Verschlüsselung, Richtigkeit der Daten, Datenminimierung bei der Gestaltung und Nutzung dieser Technologien und Systeme zu integrieren.

15. Während die Sicherheit von Informationen, die, wie es im Vorschlag heißt, von kritischen und wichtigen Organisationen und Infrastrukturen verarbeitet werden, von größter Bedeutung für die Wirtschaft und Gesellschaft in der EU ist, wird der Schutz der Privatsphäre und personenbezogener Daten auch weitgehend von kleinen und mittleren Unternehmen (KMU), die digitale Dienste anbieten, getragen und erfordert ein angemessenes Bewusstsein und angemessene Kompetenzen für die Cybersicherheit beim Einzelnen. **Daher begrüßt der EDSB den Plan für eine breitgefächerte Einführung von Cybersicherheitstechnologien durch gezielte Unterstützung von KMU im Rahmen der Zentren für digitale Innovation und anderer Instrumente** sowie Pläne für eine intensivere Aufklärung von Menschen, insbesondere von Kindern und Jugendlichen, und von Organisationen, vor allem KMU, durch den überarbeiteten Aktionsplan für digitale Bildung.

16. Der EDSB ist der Ansicht, dass sowohl der Gesetzgeber als auch die Mitgliedstaaten und die EU-Organe der Rolle der Cybersicherheit beim Schutz der Privatsphäre und personenbezogener Daten Rechnung tragen sollten, indem sie diese „Dimension" in allen oben genannten politischen Maßnahmen berücksichtigen, insbesondere die Notwendigkeit, natürliche Personen und ihre Grundrechte zu schützen und dieses Gut neben anderen Arten von Gütern in ihrem Zuständigkeitsbereich zu schützen. **Die Einbeziehung der Perspektive des Schutzes der Privatsphäre und des Datenschutzes in das traditionelle Cybersicherheitsmanagement wird einen ganzheitlichen Ansatz gewährleisten und Synergien zwischen öffentlichen und privaten Organisationen ermöglichen, wenn es darum geht, die Cybersicherheit zu verwalten und die von ihnen verarbeiteten Informationen ohne sinnlose Mehrarbeit zu schützen.**

17. **Der EDSB begrüßt, dass ín der Strategie sowohl die Organe als auch die Einrichtungen und sonstigen Stellen der Union (EUI) als Organisationen betrachtet werden, die gemeinsam mit den Einrichtungen und Akteuren der Mitgliedstaaten im Rahmen eines EU-weiten koordinierten Cybersicherheitskonzepts verteidigt werden.** Dies gilt insbesondere im Hinblick auf die Einrichtung einer gemeinsamen Cyberstelle (JCU), deren Ziel es den Plänen nach sein soll, die Koordinierung zwischen allen Akteuren zu verbessern und zu beschleunigen und es der EU zu ermöglichen, sich großen Cybervorfällen und -krisen zu stellen und darauf zu reagieren. In der Strategie heißt es: „*Im Rahmen ihrer Beiträge zur gemeinsamen Cyberstelle sind die EU-Akteure (die Kommission und die Einrichtungen und sonstigen Stellen der EU) daher bereit, ihre Ressourcen und Fähigkeiten erheblich zu steigern, um besser vorbereitet und widerstandsfähiger zu sein*". **Der EDSB empfiehlt den beiden gesetzgebenden Organen, zu prüfen und zu planen, dass diese Ressourcen von den EUI genutzt werden**, um ihre Cybersicherheitskapazitäten zu stärken, und zwar auch in einer Weise, die den Werten der EU uneingeschränkt Rechnung trägt.

18. Wie bereits in den Anmerkungen zum allgemeineren Kontext der Strategie erwähnt, empfehlen wir, dass bei den Maßnahmen und der entsprechenden Aufstockung der Ressourcen die Aspekte der Privatsphäre und des Datenschutzes der Cybersicherheit berücksichtigt werden, indem auf Strategien, Verfahren und Instrumente gesetzt wird, bei denen die Perspektive der Privatsphäre und des Datenschutzes in das herkömmliche Cybersicherheitsmanagement integriert ist und bei der Verarbeitung personenbezogener Daten bei Tätigkeiten im Bereich der Cybersicherheit wirksame Datenschutzgarantien berücksichtigt werden.

2.2. Zum Vorschlag

19. Der EDSB begrüßt das Ziel des Vorschlags, systemische und strukturelle Änderungen an der derzeitigen NIS-Richtlinie vorzunehmen, um ein breiteres Spektrum von Einrichtungen in der gesamten Union mit strengeren Sicherheitsmaßnahmen, einschließlich Mindeststandards und einschlägige Aufsichts- und Durchsetzungsbestimmungen, und durch Förderung der Zusammenarbeit und gemeinsame Zuständigkeiten und Rechenschaftspflicht abzudecken.

20. Der EDSB geht davon aus, dass sich die vorgeschlagenen Änderungen positiv auf die Sicherheit personenbezogener Daten und der elektronischen Kommunikation auswirken werden, und zwar sowohl durch die Verbesserung der Cybersicherheitsverfahren der Einrichtungen, die direkt unter den Vorschlag fallen, als auch durch die Verbesserung der Sicherheit des Internets im Allgemeinen.

21. Der EDSB begrüßt die zahlreichen Verweise auf den Schutz der Grundrechte, einschließlich des Rechts auf Datenschutz und Privatsphäre, in verschiedenen Teilen des Vorschlags.

2.3. Zum Anwendungsbereich der Strategie und des Vorschlags auf die Organe, Einrichtungen und sonstigen Stellen der Union

22. In der Strategie werden spezifische Maßnahmen vorgeschlagen, die darauf abzielen, die Informationssicherheit von EU-Einrichtungen zu verbessern und sie unter den verschiedenen EU-Einrichtungen zu harmonisieren. Diese Maßnahmen umfassen Folgendes:

    a) zwei Legislativvorschläge für gemeinsame verbindliche Vorschriften für Informationssicherheit und für gemeinsame verbindliche Vorschriften zur Cybersicherheit für alle EU-Einrichtungen im Jahr 2021;

    b) höhere Investitionen, um ein hohes Maß an „Cyberreife“ zu erreichen;

    c) ein gestärktes CERT-EU mit einem verbesserten Finanzierungsmechanismus.

23. Der EDSB schließt sich der Schlussfolgerung der Kommission in der Strategie an, dass die Fähigkeiten der einzelnen EU-Einrichtungen, Cyberangriffe abzuwehren und böswillige Cyberaktivitäten zu erkennen und darauf zu reagieren, sehr unterschiedlich entwickelt sind. Wir nehmen ferner zur Kenntnis, dass EU-Einrichtungen wie ENISA und die Kommission an der Gewährleistung eines hohen Cybersicherheitsniveaus in den Mitgliedstaaten beteiligt sind.

24. Der EDSB nimmt jedoch zur Kenntnis, dass sich die Bestimmungen der Vorschläge nur an die Mitgliedstaaten der Union wenden. Angesichts der anerkannten Notwendigkeit, das Gesamtniveau der Cybersicherheit durch **kohärente und einheitliche Vorschriften** zu verbessern, **empfiehlt** der EDSB **den gesetzgebenden Organen, den Bedürfnissen und Rollen der EU-Einrichtungen Rechnung zu tragen, damit EU-Einrichtungen in diesen EU-weiten Gesamtrahmen für Cybersicherheit integriert werden können**, da sie das gleiche hohe Schutzniveau genießen wie die Einrichtungen in den Mitgliedstaaten.

25. Zu diesem Zweck **schlägt der EDSB vor, die Organe, Einrichtungen und sonstigen Stellen der Union ausdrücklich in den Anwendungsbereich des Vorschlags aufzunehmen**. Alternativ empfiehlt der EDSB den Mitgesetzgebern, in den Wortlaut des Vorschlags eine ausdrückliche Verpflichtung für die Kommission aufzunehmen, noch im Verlauf des Jahres 2021 gesonderte Legislativvorschläge für EU-Einrichtungen vorzulegen, um eine realisierbare Verbindung zwischen dem Vorschlag selbst und den künftigen Legislativmaßnahmen auf Ebene der EU-Einrichtungen herzustellen, um kohärente und einheitliche Vorschriften für die Mitgliedstaaten und die EU-Einrichtungen zu erreichen.

3. SPEZIFISCHE EMPFEHLUNGEN

26. Der verbleibende Teil dieser Stellungnahme enthält spezifische Empfehlungen, mit denen sichergestellt werden soll, dass der Vorschlag die bestehenden Rechtsvorschriften der Union zum Schutz personenbezogener Daten, insbesondere die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation[11], wirksam ergänzt und den Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen verbessert.

3.1. Verhältnis zu den bestehenden Rechtsvorschriften der Union zum Schutz personenbezogener Daten

27. Der EDSB stellt fest, dass in dem Vorschlag an verschiedenen Stellen[12] klargestellt wird, dass er die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation „unberührt lässt“, jedoch nur in Bezug auf spezifische Kontexte, und mitunter wird nur eines der beiden Instrumente genannt.

28. Der EDSB stellt fest, dass die von dem Vorschlag erfassten Stellen, um ihm nachzukommen, bestimmte Cybersicherheitskontrollen einführen müssen, die höchstwahrscheinlich die Verarbeitung personenbezogener Daten und elektronischer Kommunikationsdaten, einschließlich Verkehrsdaten, umfassen werden.

29. Der EDSB ist daher der Auffassung, dass die Ausweitung des Anwendungsbereichs des Vorschlags auf ein breiteres Spektrum von Tätigkeiten zu einer verstärkten Verarbeitung personenbezogener Daten für Cybersicherheitszwecke führen wird. Des Weiteren stellt der EDSB fest, dass der Vorschlag gemäß Artikel 2 Absatz 2 auch für „öffentliche elektronische Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste“ gilt, die auch unter die Datenschutzrichtlinie für elektronische Kommunikation fallen. Das bedeutet, dass sowohl den Anforderungen der DSGVO als auch der Datenschutzrichtlinie für elektronische Kommunikation Rechnung getragen werden muss.

30. Der EDSB stellt 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 führt zu Verstößen gegen die DSGVO, insbesondere in Bezug auf Grundsätze wie Zweckbindung, Speicherbegrenzung, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie Verpflichtungen für konforme Datenübermittlungen. Nach Auffassung des EDSB muss deutlich gemacht werden, dass alle Cybersicherheitssysteme und -dienste, die an der Prävention und Erkennung von Cyberbedrohungen und der Reaktion darauf beteiligt sind, mit dem geltenden Datenschutzrahmen im Einklang stehen und entsprechende technische und organisatorische Sicherheitsvorkehrungen treffen sollten, um über diese Einhaltung auch Rechenschaft ablegen zu können.

31. Der EDSB hält es daher für notwendig, in Artikel 2 klarzustellen, dass die **Rechtsvorschriften der Union zum Schutz personenbezogener Daten**, insbesondere die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation, **für alle Verarbeitungen personenbezogener Daten gelten, die in den Anwendungsbereich des Vorschlags fallen** (und nicht nur innerhalb bestimmter Kontexte). In einem entsprechenden Erwägungsgrund sollte ferner klargestellt werden, dass der Vorschlag nicht versucht, die Anwendung der bestehenden EU-Rechte für die Verarbeitung personenbezogener Daten einschließlich der Aufgaben und Befugnisse der für die Überwachung der Einhaltung dieser Instrumente zuständigen Aufsichtsbehörden zu beeinträchtigen.

3.2. Definition des Begriffs „Cybersicherheit“

32. Der EDSB stellt fest, dass der zentrale Begriff des Vorschlags „Cybersicherheit“ ist (auch im Titel des Vorschlags), während in der derzeitigen NIS-Richtlinie der zentrale Begriff „Sicherheit von Netz- und Informationssystemen“ lautet. Allerdings wird im Vorschlag neben dem Begriff „Cybersicherheit“ auch weiterhin der Begriff „Sicherheit von Netz- und Informationssystemen“ verwendet. Allerdings werden diese Begriffe im Textverlauf nicht einheitlich verwendet.

33. Im Vorschlag wird der Begriff „Cybersicherheit“ in Artikel 4 Absatz 3 definiert, der jedoch auf Artikel 2 Absatz 1 der Verordnung (EU) 2019/881[13] verweist, wo es heißt, „Cybersicherheit“ „*bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen*“. Der Begriff „Cyberbedrohung“ nach Artikel 2 Absatz 8 der Verordnung (EU) 2019/881 bezeichnet „*einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte*“.

34. Gemäß Artikel 4 Absatz 2 des Vorschlags[14] bezeichnet der Begriff „Sicherheit von Netz- und Informationssystemen“ „*die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder*

verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen."

35. Nach Ansicht des EDSB berücksichtigt der Begriff „Cybersicherheit", wie er in der Verordnung (EU) 2019/881 definiert ist und auch im Vorschlag verwendet wird, auch nachteilige Auswirkungen auf „*... Nutzer solcher Systeme und andere Personen*". Diese Definition ermöglicht es, dem Umgang mit Risiken für die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten über Netz- und Informationssysteme Rechnung zu tragen und beinhaltet einen integrierten Ansatz.

36. Gleichzeitig halten wir fest, dass der Begriff „Sicherheit von Netz- und Informationssystemen" diesen Aspekt nicht einschließt, da *er sich nicht ausdrücklich auf den Schutz natürlicher Personen bezieht.* Dies ist insofern kein Problem, als der Begriff nur verwendet wird, um die Fokussierung auf die Netz- und Informationssysteminfrastruktur als solche zu betonen und den primären Schutzbedarf dieser Güter zu betonen, der dann für den Schutz anderer Güter, einschließlich natürlicher Personen, ebenfalls gilt. Der EDSB weist jedoch darauf hin, dass die beiden Begriffe in dem Vorschlag fast austauschbar verwendet werden[15], was möglicherweise unbeabsichtigte praktische Folgen für die Notwendigkeit hat, dem Schutz natürlicher Personen Rechnung zu tragen.

37. Der EDSB fordert daher die Mitgesetzgeber auf, diese Frage zu klären. Der EDSB schlägt vor, angesichts des breiteren Anwendungsbereichs generell den Begriff „Cybersicherheit" zu verwenden und den Begriff „Sicherheit von Netz- und Informationssystemen" nur dann heranzuziehen, wenn der Kontext dies zulässt (z. B. ein rein technischer Kontext, in dem Auswirkungen auch auf die Nutzer von Systemen und andere Personen nicht berücksichtigt werden).

3.3. Domänennamen und Registrierungsdaten („WHOIS-Daten")

38. Der EDSB begrüßt Erwägungsgrund 59 des Vorschlags, dem zufolge in Fällen, in denen die Verarbeitung von „WHOIS-Daten" auch personenbezogene Daten umfasst, diese Verarbeitung im Einklang mit dem Datenschutzrecht der Union erfolgen muss. In Erwägungsgrund 60 wird zudem bestätigt, dass der Zugang zuständiger Behörden zu diesen Daten, soweit personenbezogene Daten betroffen sind, mit dem EU-Datenschutzrecht im Einklang stehen sollte. Wie bereits ausgeführt (siehe Abschnitt 3.1), empfiehlt der EDSB nachdrücklich, (in Artikel 2) eine allgemeine materiellrechtliche Bestimmung über die Anwendung des Datenschutzrechts der Union aufzunehmen und sie nicht an mehreren Stellen zu erwähnen..

39. Artikel 23 Absatz 2 des Vorschlags spricht von „*einschlägigen Angaben (...), anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können*". Der EDSB empfiehlt eine **klare Definition dessen, was unter „einschlägigen Angaben"** für die Zwecke dieser Bestimmung, einschließlich personenbezogener Daten, **zu verstehen ist**, und dabei den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit Rechnung zu tragen. Dies wäre der Rechtssicherheit förderlich und würde einen einheitlichen Ansatz in den 27 Mitgliedstaaten der EU gewährleisten.

40. Gemäß Artikel 23 Absatz 4 des Vorschlags müssen die Mitgliedstaaten außerdem sicherstellen, dass die Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich die nicht personenbezogenen Domänenregistrierungsdaten veröffentlichen. Der EDSB empfiehlt ferner, genauer zu klären, **welche Kategorien von Domänenregistrierungsdaten** (die keine personenbezogenen Daten darstellen) **veröffentlicht werden sollten**.

41. In Erwägungsgrund 14 der DSGVO heißt es: „*Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der der juristischen Person*". Der EDSB erinnert daran, dass zwar die Kontaktdaten einer juristischen Person nicht in den Anwendungsbereich der DSGVO fallen, sofern sie keine natürliche Person identifizieren, die Kontaktdaten natürlicher Personen jedoch sehr wohl in den Anwendungsbereich der DSGVO fallen.[16]

42. In Artikel 4 Absatz 1 DSGVO werden personenbezogene Daten definiert als „alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Daher können – wie vom EuGH klargestellt – auch die Daten juristischer Personen in einigen Fällen als personenbezogene Daten betrachtet werden.[17] In diesen Fällen ist entscheidend, ob sich die Informationen auf eine „identifizierbare" natürliche Person „beziehen".

43. Gemäß Artikel 23 Absatz 5 des Vorschlags stellen die Mitgliedstaaten sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. In dem Vorschlag wird weder definiert, was unter „rechtmäßigen und hinreichend begründeten Anträgen" zu verstehen ist, noch werden „berechtigte Zugangsnachfrager" definiert oder Zwecke für einen solchen Zugang festgelegt. Der Vorschlag enthält auch kein objektives Kriterium für die Festlegung der Grenzen für den Zugang „berechtigter Zugangsnachfrager" zu den Daten und für ihre anschließende Nutzung.

44. Artikel 23 Absatz 5 des Vorschlags verpflichtet die Mitgliedstaaten zu einem Eingriff in das durch Artikel 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten, da er die Verarbeitung personenbezogener Daten vorsieht.[18]

45. Im Einklang mit Artikel 52 Absatz 1 der Charta hat der EuGH wiederholt klargestellt, dass die Rechtsgrundlage, die den Eingriff zulässt, selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts bestimmen muss.[19] Gemäß dem Grundsatz der Verhältnismäßigkeit müssen sich Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken.[20] Um dem

Erfordernis der Verhältnismäßigkeit zu genügen, muss die den Eingriff vorsehende Regelung **klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen**, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. „[Die Regelung] muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden.[21]

46. In Anbetracht dieser Anforderungen **betont der EDSB, dass der Wortlaut des Vorschlags daher klarstellen muss, welche (öffentlichen oder privaten) Einrichtungen *„berechtigte Zugangsnachfrager“* sein könnten.** So sollte beispielsweise präzisiert werden, ob der Zugang auf die in Erwägungsgrund 60 des Vorschlags genannten Einrichtungen beschränkt werden soll, oder ob auch andere Kategorien von Empfängern Zugang erhalten können. Der EDSB macht geltend, dass in der Praxis auch Einrichtungen außerhalb des EWR Zugang zu bestimmten Registrierungsdaten für Domänennamen beantragen könnten. Aus diesem Grund fordert der EDSB die Gesetzgeber auf, in diesem Vorschlag klarzustellen, ob die personenbezogenen Daten im Besitz der TLD-Register und der Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auch für Einrichtungen außerhalb des EWR zugänglich sein sollten. Sollte dies der Fall sein, sollte der Vorschlag die Bedingungen, Beschränkungen und Verfahren für einen solchen Zugang eindeutig festlegen, wobei gegebenenfalls auch die Anforderungen des Artikels 49 Absatz 2 DSGVO zu berücksichtigen wären.

47. In diesem Sinne empfiehlt der EDSB auch, weiter zu präzisieren, **was ein *„rechtmäßiger und hinreichend begründeter“* Antrag ist**, auf dessen Grundlage und zu welchen Bedingungen der Zugang gewährt wird.

3.4. „Proaktive Überprüfung von Netz- und Informationssystemen auf Schwachstellen“ durch CSIRTs

48. Der EDSB stellt fest, dass in Artikel 10 Absatz 2 Buchstabe e des Vorschlags den CSIRTs die Aufgabe übertragen wird, auf Ersuchen einer (wesentlichen oder wichtigen) Einrichtung eine „*proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen*“ durchzuführen. Nach Auffassung des EDSB bezieht sich dies nicht nur auf die Überprüfung von Netzen, sondern auch auf die Überprüfung von Informationssystemen im Allgemeinen (Anwendungen, Server und Datenbanken).

49. In Erwägungsgrund 25 heißt es: „*In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen*“.

50. Der EDSB hält fest, dass in Erwägungsgrund 69 die Tätigkeiten der CSIRTs weiter präzisiert und deren Zweck (d. h. „Gewährleistung der Netz- und Informationssicherheit durch Einrichtungen“) und ihr Umfang (d. h. „Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools) sowie die Arten möglicherweise betroffener personenbezogener Daten (d. h. „IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen) allgemein angegeben werden.

51. Nach Auffassung des EDSB umreißt der Vorschlag nicht ausreichend die Art der Verarbeitung personenbezogener Daten im Rahmen der proaktiven Überprüfung auf Schwachstellen. Angesichts des Wortlauts von Erwägungsgrund 69 („können erfordern“) geht der EDSB davon aus, dass Artikel 10 Absatz 2 Buchstabe e nicht darauf abzielt, eine systematische Erhebung und Analyse personenbezogener Daten und/oder elektronischer Kommunikationsdaten durch CSIRTs zu ermöglichen. Im Interesse der Rechtssicherheit empfiehlt der EDSB den Mitgesetzgebern, **die Arten der proaktiven Überprüfung auf Schwachstellen, zu deren Durchführung die CSIRTs aufgefordert werden können, genauer zu definieren** und **die wichtigsten Kategorien betroffener personenbezogener Daten** im Wortlaut des Vorschlags **zu benennen**.

3.5. Auslagerung und Lieferkette

52. Die Erwägungsgründe 42 und 44 des Vorschlags implizieren, dass für wesentliche und wichtige Einrichtungen die Möglichkeit besteht, Teile oder die Gesamtheit ihrer Cybersicherheitsaktivitäten an externe Diensteanbieter auszulagern, wie etwa die „Anbieter verwalteter Sicherheitsdienste (MSSP)“.

53. Der EDSB erinnert daran, dass die Auslagerung solcher Tätigkeiten durch den Verantwortlichen in vollem Einklang mit der DSGVO erfolgen muss. Insbesondere unterliegt gemäß Artikel 28 DSGVO die Verarbeitung durch einen Auftragsverarbeiter einem Vertrag oder einem anderen Rechtsakt nach dem Unionsrecht oder dem Recht der Mitgliedstaaten. Diesbezüglich erinnert der EDSB daran, dass Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen Kapitel V und der einschlägigen Rechtsprechung des Gerichtshofs[22] entsprechen müssen.

54. Der EDSB begrüßt die Maßnahmen zur Minderung von Risiken aufgrund technischer und gegebenenfalls nichttechnischer Faktoren der Lieferkette durch koordinierte (sektorale) Risikobewertungen der Lieferkette.[23] Der EDSB begrüßt ferner, dass in dem Vorschlag bei den Kriterien zur Bestimmung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, die Relevanz bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte, die unter anderem personenbezogene Daten verarbeiten, genannt wird.

55. Der EDSB betont, dass unter den spezifischen Faktoren, die bei der Bewertung der Lieferketten für Technologien und Systeme, die personenbezogene Daten verarbeiten, zu berücksichtigen sind, **besonderes Augenmerk auf die Merkmale gerichtet werden sollte, die die wirksame Umsetzung des Grundsatzes des Datenschutzes durch**

Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ermöglichen. Dies wäre ein Beitrag zur Einhaltung von Artikel 25 DSGVO und zum wirksamen Schutz der Kommunikation und der Endeinrichtungen in der Datenschutzrichtlinie für elektronische Kommunikation.

56. Darüber hinaus ist der EDSB der Auffassung, dass bei der Bewertung der Risiken für die Lieferkette der Schwerpunkt auf **IKT-Dienste, -Systeme oder -Produkte gelegt werden sollte, für die im Herkunftsland besondere Anforderungen gelten, die ein Hindernis für die Einhaltung der EU-Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz darstellen könnten.**

57. Der EDSB empfiehlt ferner, **den durch Artikel 68 DSGVO eingesetzten Europäischen Datenschutzausschuss (EDSA)** bei der Festlegung dieser Kriterien und erforderlichenfalls bei der koordinierten sektoralen Risikobewertung gemäß Erwägungsgrund 46 **zu konsultieren**.

58. Der EDSB nutzt auch die Gelegenheit für die Empfehlung, in einem Erwägungsgrund darauf hinzuweisen, dass **quelloffene Cybersicherheitsprodukte** (Software und Hardware), einschließlich der Verschlüsselung offener Quellen, die nötige Transparenz bieten könnten, um spezifische Risiken in der Lieferkette zu mindern.

3.6. Verschlüsselung

59. Der EDSB begrüßt die Aufnahme von Verschlüsselung und Kryptografie in die Liste der Mindestgarantien für die Cybersicherheit in Artikel 18 des Vorschlags. Darüber hinaus begrüßt der EDSB auch die Verweise auf Verschlüsselung in der Strategie.[24]

60. Der EDSB unterstützt uneingeschränkt die Aussage in Erwägungsgrund 54 des Vorschlags zur Förderung und sogar zur verpflichtenden Nutzung der End-zu-End-Verschlüsselung durch die Anbieter elektronischer Kommunikationsdienste.

61. In Erwägungsgrund 54 heißt es jedoch auch, dass die Nutzung der End-zu-End-Verschlüsselung mit den Befugnissen der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, „in Einklang gebracht werden“ sollte. Insbesondere heißt es dort: „*Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten*“.

62. Der EDSB weist erneut darauf hin, dass die Verschlüsselung laut der Erklärung der Artikel 29-Datenschutzgruppe[25] eine kritische und unersetzliche Technologie für einen wirksamen Datenschutz und einen wirksamen Schutz der Privatsphäre ist. **Für die Minderung hoher Risiken für die Rechte und Freiheiten des Einzelnen muss eine starke Verschlüsselung zur Verfügung stehen.** Als Beispiel für die Notwendigkeit einer starken Verschlüsselung verweist der EDSB auf die jüngsten Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten[26], die bestimmte Anwendungsfälle enthalten, in denen eine starke Verschlüsselung zur Minderung von

Risiken im Zusammenhang mit nicht konformen Datenübermittlungen eingesetzt werden kann.

63. Jede Schwächung oder Umgehung der Verschlüsselung (z. B. Verwendung obligatorischer Hintertüren, obligatorischer Schlüsselhinterlegung und versteckter Kommunikationskanäle) würde aufgrund ihrer möglichen unrechtmäßigen Nutzung und des Verlusts des Vertrauens in Sicherheitskontrollen den Mechanismus seiner wirksamen Schutzfähigkeit gänzlich berauben. Sie würde somit unweigerlich den Schutz der Grundrechte auf den Schutz personenbezogener Daten und der Privatsphäre beeinträchtigen, da sie generell erhebliche Risiken für Wirtschaft und Gesellschaft darstellen würde. Selbst wenn keine starke Verschlüsselung verwendet wird, obwohl noch verfügbar, **sollte eine nicht autorisierte Entschlüsselung oder ein Reverse Engineering von Verschlüsselungscodes oder die Überwachung elektronischer Kommunikation außerhalb eindeutiger rechtlicher Befugnisse verboten werden.**

64. Der EDSB geht zwar davon aus, dass die Strafverfolgung die Mittel zur Bekämpfung von Straftaten im Internet erfordert, doch muss jede Maßnahme, die in die Vertraulichkeit der Kommunikation eingreift, dem Erfordernis der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit genügen, und zwar auf der Grundlage fundierter Beweise. Verschlüsselung erschwert zwar die Erhebung von Massendaten und die Massenüberwachung, ist aber kein begrenzender Faktor für gezieltere und spezifischere Maßnahmen. **Der EDSB empfiehlt daher, in Erwägungsgrund 54 klarzustellen, dass keine Bestimmung des Vorschlags als Befürwortung einer Schwächung der End-zu-End-Verschlüsselung durch „Hintertürchen“ oder ähnliche Lösungen ausgelegt werden sollte.**

3.7. Risikomanagementmaßnahmen im Bereich der Cybersicherheit

65. Der EDSB begrüßt Artikel 18, dem zufolge die Mitgliedstaaten sicherstellen, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen sowie die in Artikel 18 Absatz 2 vorgesehenen Mindestmaßnahmen zu bewältigen.

66. Der EDSB erinnert daran, dass das Management von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gemäß Artikel 32 DSGVO eine Verpflichtung für alle Verantwortlichen (und nicht nur für wesentliche und wichtige Einrichtungen) darstellt. Während die Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit in Artikel 18 des Vorschlags darauf abzielen, Netz- und Informationssysteme der Organisation (und die darin enthaltenen Daten) zu schützen, zielt Artikel 32 DSGVO 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 beiden Tätigkeiten geschützt werden sollen, was unter bestimmten Umständen zu unterschiedlichen Schlussfolgerungen führen könnte. Zugleich kann das Verfahren für das Risikomanagement im Bereich der Cybersicherheit dazu beitragen, die Auswirkungen von Schwachstellen bei der Sicherheit personenbezogener Daten auf den Datenschutz zu bewerten. Wie bereits erwähnt, empfiehlt der EDSB in Bezug auf die weiter gefasste Maßnahme der Strategie die **Einbeziehung der Aspekte Schutz der Privatsphäre und Datenschutz in das Risikomanagement im Bereich der Cybersicherheit**, um einen

ganzheitlichen Ansatz zu gewährleisten und öffentliche und private Organisationen bei der Verwaltung der Cybersicherheit und beim Schutz der von ihnen verarbeiteten Informationen ohne unnötige Mehrarbeit Synergien zu ermöglichen.

67. **Der EDSB schlägt vor, diese Überlegungen sowohl in die Erwägungsgründe als auch in den verfügenden Teil des Vorschlags einfließen zu lassen**, damit etwaige künftige Durchführungsrechtsakte der Kommission, Leitlinien der ENISA zur Cybersicherheit auf EU-Ebene sowie ihre Arbeit an europäischen Systemen für die Cybersicherheitszertifizierung (siehe Artikel 21 des Vorschlags) und die Arbeit der Normungsgremien der EU (siehe Artikel 22) diese Aspekte berücksichtigen und somit das Management der Risiken für natürliche Personen und ihre Grundrechte, die sich aus Bedrohungen für die Cybersicherheit ergeben, berücksichtigen könnten.

68. Angesichts der engen Verbindungen zwischen Cybersicherheitsmanagement und Schutz personenbezogener Daten schlägt der EDSB außerdem vor, **die ENISA zur Konsultation des EDSA** bei der Ausarbeitung einschlägiger Leitlinien **zu verpflichten**. Diese Rechtsakte und Leitlinien können auch für Organisationen nützlich sein, die nicht in den Anwendungsbereich der Richtlinie fallen, könnten aber dennoch ähnliche Vorteile bieten und die Erfüllung der Verpflichtungen nach der DSGVO in Bezug auf die Sicherheit personenbezogener Daten fördern.

3.8. Verletzungen des Schutzes personenbezogener Daten

69. Gemäß Artikel 20 Absatz 2 des Vorschlags stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT unverzüglich jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können. In Artikel 20 Absatz 3 ist festgelegt, wann ein Sicherheitsvorfall als „erheblich“ gilt. Eine Möglichkeit ist, dass der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder potenziell schädigen könnte.

70. Der EDSB begrüßt Artikel 20 Absatz 3 Buchstabe b des Vorschlags, der nicht nur Auswirkungen auf die Organisation, sondern auch auf möglicherweise betroffene natürliche Personen berücksichtigt. Der EDSB stellt aber auch fest, dass die Definition in Artikel 20 Absatz 3 Buchstabe b bestimmte „Verletzungen des Schutzes personenbezogener Daten“ im Sinne von Artikel 4 Absatz 12 DSGVO umfassen würde. Offenbar können sich die entsprechenden Meldepflichten in bestimmten Fällen auch mit der Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständigen Behörden gemäß Artikel 33 DSGVO überschneiden. Allerdings unterscheiden sich die Definitionen der Umstände, unter denen die Verpflichtung besteht, die festgelegten maximalen Fristen sowie die zuständigen Behörden, an die Meldung zu erstatten ist. Analoge Meldepflichten gegenüber den zuständigen Behörden sind auch in der Datenschutzrichtlinie für elektronische Kommunikation festgelegt, die derzeit überarbeitet wird.

71. Der EDSB begrüßt Artikel 28 Absatz 2, dem zufolge die nach dem Vorschlag zuständigen Behörden bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den Datenschutzbehörden zusammenarbeiten, wodurch Synergien zwischen den Rechtsinstrumenten entstehen. Der EDSB begrüßt ferner

die Verpflichtung der zuständigen Behörden gemäß Artikel 32 Absatz 1, die für den Datenschutz zuständigen Behörden zu informieren, wenn ihnen Hinweise darauf vorliegen, dass die Verletzung der in den Artikeln 18 und 20 festgelegten Pflichten durch eine wesentliche oder wichtige Einrichtung zu einer Verletzung des Schutzes personenbezogener Daten führt, die nach Artikel 33 DSGVO zu melden ist.

72. Der EDSB stellt fest, dass die zuständigen Behörden dieser Verpflichtung zur Meldung an die nach der DSGVO zuständigen Behörden „innerhalb einer angemessenen Frist" nachzukommen haben. Der EDSB hält fest, dass diese Verpflichtung unbeschadet der Meldepflicht für Verantwortliche gemäß Artikel 33 DSGVO gilt, die „unverzüglich" und „binnen 72 Stunden", nachdem sie Kenntnis von der Verletzung des Schutzes personenbezogener Daten erhalten haben, diese zu melden haben. Damit die Datenschutzbehörden ihre Aufgaben wirksam wahrnehmen können, **schlägt der EDSB vor, den Wortlaut des Vorschlags „innerhalb einer angemessenen Frist" in „unverzüglich" zu ändern**.

3.9. Kooperationsgruppe

73. Mit Artikel 12 des Vorschlags wird zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten bei der Anwendung der Richtlinie eine Kooperationsgruppe eingesetzt. Unter Berücksichtigung der Aufgabe dieser Gruppe und einer möglichen Verknüpfung mit dem Datenschutzrahmen **empfiehlt der EDSB, einen Vertreter des EDSA als Mitglied in die Kooperationsgruppe aufzunehmen**.

3.10. Gerichtliche Zuständigkeit und Territorialität

Der EDSB stellt fest, dass der in Artikel 24 Absatz 2 des Vorschlags verwendete Begriff „Hauptniederlassung"[27] anders definiert ist als in Artikel 4 Absatz 16 DSGVO.

74. Im Bereich der DSGVO ist das Konzept der „Hauptniederlassung" besonders wichtig in Fällen, in denen es um die grenzüberschreitende Verarbeitung personenbezogener Daten geht. Artikel 56 Absatz 1 DSGVO enthält eine übergeordnete Vorschrift, der zufolge die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung ist.[28] Daher empfiehlt der EDSB, im verfügenden Teil **klarzustellen, dass der Vorschlag die Zuständigkeiten der Datenschutzaufsichtsbehörden gemäß der DSGVO unberührt lässt** (siehe weiter oben Abschnitt 3.8).

75. Der EDSB bekräftigt seine Unterstützung für Artikel 28 Absatz 2 des Vorschlags, wonach die zuständigen Behörden bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den Datenschutzbehörden zusammenarbeiten (siehe weiter oben Ziffer 67).

76. Gleichzeitig betont der EDSB, dass in dem Vorschlag **eine umfassendere Rechtsgrundlage für die Zusammenarbeit und den Austausch einschlägiger Informationen** zwischen den zuständigen Behörden im Rahmen des Vorschlags und anderen einschlägigen Aufsichtsbehörden geschaffen werden muss, die jeweils innerhalb

ihres jeweiligen Zuständigkeitsbereichs handeln. Insbesondere empfiehlt der EDSB, klar zum Ausdruck zu bringen, dass zuständige Behörden nach dem Vorschlag auch in der Lage sein sollten, den zuständigen Aufsichtsbehörden nach der Verordnung (EU) 2016/679 auf Anfrage oder auf eigene Initiative alle im Zusammenhang von Prüfungen und Untersuchungen erhaltenen Informationen bereitzustellen, die sich auf die Verarbeitung personenbezogener Daten beziehen, und zu diesem Zweck eine eindeutige Rechtsgrundlage vorzugeben.

4. SCHLUSSFOLGERUNGEN

77. Vor diesem Hintergrund spricht der EDSB folgende Empfehlungen aus:

Zur Cybersicherheitsstrategie

- Es sollte berücksichtigt werden, dass der erste Schritt zur Minderung von Risiken für den Datenschutz und den Schutz der Privatsphäre in der Anwendung der Anforderungen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO besteht, was dazu beitragen wird, geeignete Garantien wie Pseudonymisierung, Verschlüsselung, Richtigkeit der Daten, Datenminimierung bei der Gestaltung und Nutzung dieser Technologien und Systeme zu integrieren;

- es sollte berücksichtigt werden, dass der Einbeziehung der Perspektive des Schutzes der Privatsphäre und des Datenschutzes in Maßnahmen und Standards im Bereich der Cybersicherheit sowie in das traditionelle Cybersicherheitsmanagement große Bedeutung zukommt, um einen ganzheitlichen Ansatz zu gewährleisten und Synergien zwischen öffentlichen und privaten Organisationen zu ermöglichen, wenn es darum geht, die Cybersicherheit zu verwalten und die von ihnen verarbeiteten Informationen ohne sinnlose Mehrarbeit zu schützen;

- es sollte erwogen und geplant werden, die Cybersicherheitskapazität von durch EU-Institutionen genutzten Ressourcen zu stärken, und zwar auch in einer Weise, die den Werten der EU uneingeschränkt Rechnung trägt;

- es sollte der Dimension des Schutzes der Privatsphäre und des Datenschutzes der Cybersicherheit Rechnung getragen werden, indem auf Strategien, Verfahren und Instrumente gesetzt wird, bei denen die Perspektive des Schutzes der Privatsphäre und des Datenschutzes in das herkömmliche Cybersicherheitsmanagement integriert ist und bei der Verarbeitung personenbezogener Daten bei Tätigkeiten im Bereich der Cybersicherheit wirksame Datenschutzgarantien integriert sind;

Zum Anwendungsbereich der Strategie und des Vorschlags auf die Organe, Einrichtungen und sonstigen Stellen der Union:

- Es sollte den Bedürfnissen und der Rolle der EU-Institutionen Rechnung getragen werden, damit die EU-Institutionen in diesen EU-weiten Gesamtrahmen für Cybersicherheit als Einrichtungen integriert werden, die das gleiche hohe Schutzniveau genießen wie Einrichtungen in den Mitgliedstaaten;

- es sollten die Organe, Einrichtungen und sonstigen Stellen der Union ausdrücklich in den Anwendungsbereich des Vorschlags aufgenommen werden.

Zum Verhältnis zu den bestehenden Rechtsvorschriften der Union über den Schutz personenbezogener Daten:

- In Artikel 2 des Vorschlags sollte klargestellt werden, dass die Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation, für jede Verarbeitung personenbezogener Daten gelten, die in den Anwendungsbereich des Vorschlags fällt (und nicht nur in bestimmten Kontexten);

- ferner sollte in einem entsprechenden Erwägungsgrund klargestellt werden, dass der Vorschlag nicht versucht, die Anwendung der bestehenden EU-Rechtsvorschriften für die Verarbeitung personenbezogener Daten einschließlich der Aufgaben und Befugnisse der für die Überwachung der Einhaltung dieser Instrumente zuständigen Aufsichtsbehörden zu beeinträchtigen.

Zur Definition des Begriffs „Cybersicherheit“:

- Es sollte auf die unterschiedliche Verwendung der Begriffe „Cybersicherheit“ und „Sicherheit von Netz- und Informationssystemen“ eingegangen und klar gemacht werden, dass der Begriff „Cybersicherheit“ generell und der Begriff „Sicherheit von Netz- und Informationssystemen“ nur dann zu verwenden ist, wenn der Kontext (z. B. ein rein technischer Kontext, ohne die Auswirkungen auf die Nutzer von Systemen und andere Personen zu berücksichtigen) dies zulässt.

Zu Domänennamen und Registrierungsdaten („WHOIS-Daten“):

- Es sollte klar zum Ausdruck gebracht werden, was unter „einschlägigen Angaben“ für Zwecke der Identifizierung und Kontaktierung der Inhaber von Domänennamen und der Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, zu verstehen ist;

- es sollte genauer geklärt werden, welche Kategorien von Domänenregistrierungsdaten (die keine personenbezogenen Daten darstellen) veröffentlicht werden sollten;

- es sollte weiter geklärt werden, welche (öffentlichen oder privaten) Einrichtungen „*berechtigte Zugangsnachfrager*“ sein können;

- es sollte klargestellt werden, ob die personenbezogenen Daten im Besitz der TLD-Register und der Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auch für Einrichtungen außerhalb des EWR zugänglich sein sollten, und falls dies der Fall wäre, sollten die Bedingungen, Beschränkungen und Verfahren für diesen Zugang eindeutig festgelegt werden, wobei gegebenenfalls auch die Anforderungen von Artikel 49 Absatz 2 DSGVO zu berücksichtigen sind;

- es sollte näher präzisiert werden, was ein „*rechtmäßiger und hinreichend begründeter*“ Antrag ist, auf dessen Grundlage und zu welchen Bedingungen der Zugang gewährt wird.

Zur „proaktiven Überprüfung von Netz- und Informationssystemen auf Schwachstellen“ durch CSIRTs:

- Es sollten die Arten der Schwachstellenscans, zu deren Durchführung die CSIRTs aufgefordert werden können, genauer definiert und die wichtigsten Kategorien betroffener personenbezogener Daten im Wortlaut des Vorschlags benannt werden.

Zur Auslagerung und zu Lieferketten:

- Bei der Bewertung der Lieferketten für Technologien und Systeme, die personenbezogene Daten verarbeiten, sollten die Merkmale berücksichtigt werden, die die wirksame Umsetzung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ermöglichen;

- bei der Bewertung der Lieferkettenrisiken von IKT-Diensten, -Systemen oder -Produkten sollten besondere Anforderungen im Herkunftsland berücksichtigt werden, die ein Hindernis für die Einhaltung der EU-Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz darstellen könnten;

- es sollte in den verfügenden Teil und erforderlichenfalls in die koordinierte sektorale Risikobewertung gemäß Erwägungsgrund 46 die obligatorische Konsultation des EDSA bei der Festlegung der oben genannten Merkmale aufgenommen werden;

- es sollte in einem Erwägungsgrund darauf hingewiesen werden, dass **quelloffene Cybersicherheitsprodukte** (Software und Hardware), einschließlich der Verschlüsselung offener Quellen, die nötige Transparenz bieten könnten, um spezifische Risiken in der Lieferkette zu mindern.

Zur Verschlüsselung:

- Es sollte in Erwägungsgrund 54 klargestellt werden, dass keine Bestimmung des Vorschlags als Befürwortung einer Schwächung der End-zu-End-Verschlüsselung durch „Hintertürchen“ oder ähnliche Lösungen ausgelegt werden sollte.

Zu Risikomanagementmaßnahmen im Bereich der Cybersicherheit:

- Es sollte sowohl in die Erwägungsgründe als auch in den verfügenden Teil des Vorschlags der Gedanke aufgenommen werden, dass die Einbeziehung der Perspektive Schutz der Privatsphäre und Datenschutz in das traditionelle Risikomanagement im Bereich der Cybersicherheit einen ganzheitlichen Ansatz gewährleistet und öffentlichen und privaten Organisationen bei der Verwaltung der Cybersicherheit und beim Schutz der von ihnen verarbeiteten Informationen ohne unnötige Mehrarbeit Synergien ermöglicht;

- es sollte in den verfügenden Teil eine Verpflichtung für die ENISA aufgenommen werden, den EDSA bei der Ausarbeitung einschlägiger Leitlinien zu konsultieren.

Zu Verletzungen des Schutzes personenbezogener Daten:

- Es sollte die Formulierung „innerhalb einer angemessenen Frist“ in Artikel 32 Absatz 1 in „unverzüglich“ geändert werden;

Zur Kooperationsgruppe:

- Es sollte in den verfügenden Teil die Mitgliedschaft des EDSA in der Kooperationsgruppe unter Berücksichtigung des Zusammenhangs zwischen der Aufgabe dieser Gruppe und dem Datenschutzrahmen aufgenommen werden.

Zu Zuständigkeit und Territorialität:

- Es sollte im verfügenden Teil klargestellt werden, dass der Vorschlag die Zuständigkeiten der Datenschutzaufsichtsbehörden gemäß der DSGVO unberührt lässt;

- es sollte eine umfassenden Rechtsgrundlage für die Zusammenarbeit und den Informationsaustausch zwischen zuständigen Behörden und Aufsichtsbehörden geschaffen werden, die im Rahmen ihrer jeweiligen Zuständigkeiten tätig werden;

- es sollte klargestellt werden, dass nach dem Vorschlag zuständige Behörden auch in der Lage sein sollten, den zuständigen Aufsichtsbehörden nach der Verordnung (EU) 2016/679 auf Anfrage oder auf eigene Initiative alle im Zusammenhang von Prüfungen und Untersuchungen erhaltenen Informationen bereitzustellen, die sich auf die Verarbeitung personenbezogener Daten beziehen und zu diesem Zweck eine eindeutige Rechtsgrundlage vorzugeben.

Brüssel, 11. März 2021

[elektronisch unterzeichnet]
Wojciech Rafał WIEWIÓROWSKI

Endnoten

[1] ABl. L 119 vom 4.5.2016, S. 1.
[2] ABl. L 295 vom 21.11.2018, S. 39.

[4] 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.
[5] Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final.
[6] Siehe Kapitel I. EINLEITUNG, S. 5 der Strategie.
[7] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1.
[8] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).
[9] Für weitere Einzelheiten siehe: Leitlinien des EDSB für die „Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken“, 19. Dezember 2019, (https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en) sowie das Dokument des EDSB „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken“, 11. April 2017 (https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en).
[10] EDSB, „Eine sicherere digitale Zukunft gestalten: eine neue Strategie für ein neues Jahrzehnt“, 30. Juni 2020 (https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en).
[11] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.
[12] Erwägungsgrund 25 des Vorschlags verweist mit Blick auf die proaktive Überprüfung von Netz- und Informationssystemen auf Schwachstellen nur auf die Verordnung (EU) 2016/679; Erwägungsgrund 48 bezieht sich im Zusammenhang mit den Meldepflichten sowohl auf die Verordnung (EU) 2016/679 als auch auf die Richtlinie 2002/58/EG; Erwägungsgrund 56 erwähnt sowohl die Verordnung (EU) 2016/679 als auch die Richtlinie 2002/58/EG mit Blick auf Meldepflichten nach verschiedenen Regelungen; Erwägungsgrund 58 verweist lediglich auf die Richtlinie 2002/58/EG im Hinblick auf die Gefährdung personenbezogener Daten bei Sicherheitszwischenfällen (obwohl dort auch ein Verweis auf die Verordnung (EU) 2016/679 angebracht wäre); Artikel 26 verweist auf die Verordnung (EU) 2016/679 bezüglich des Austauschs von Cybersicherheitsinformationen zwischen Mitgliedstaaten, und Artikel 32 bezieht sich bei Verstößen, die eine Verletzung des Schutzes personenbezogener Daten zur Folge haben, auf die Verordnung (EU) 2016/679.
[13] 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.
[14] Dieselbe Definition findet sich in der geltenden NIS-Richtlinie.
[15] So heißt es beispielsweise in Artikel 4 Absatz 4 des Vorschlags: „Der Begriff „*nationale Cybersicherheitsstrategie“ bezeichnet einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in diesem Mitgliedstaat*;“
[16] https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf (S. 4).
[17] Siehe Gerichtshof der Europäischen Union in den verbundenen Rechtssachen C-92/09 Volker und Markus Schecke GbR gegen Land Hessen und C-93/09 Eifert gegen Land Hessen und Bundesanstalt für Landwirtschaft und Ernährung; hier befand der Gerichtshof in Rn. 53, dass sich juristische Personen auf den durch die Art. 7 und 8 der Charta verliehenen Schutz nur berufen können, soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt.
[18] Artikel 52 Absatz 1 der Charta besagt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen

werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“.

[19] Vgl. hierzu Gerichtshof der Europäischen Union, Urteil vom 17. Dezember 2015, WebMindLicenses, C-419/14, EU:C:2015:832, Rn. 81.

[20] Gerichtshof der Europäischen Union, Urteile vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn, 56; vom 8. April 2014, Digital Rights Ireland und andere, C-293/12 und C-594/12, EU:C:2014:238, Rn. 51 und 52; vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92; und vom 21. Dezember 2016, Tele2 Sverige und Watson und andere, C-203/15 und C-698/15, EU:C:2016:970, Rn. 96 und 103.

[21] Vgl. Gerichtshof der Europäischen Union, Gutachten 1/15 des Gerichtshofs vom 26. Juli 2017, Rn. 140 und 141.

[22] Urteil des Gerichtshofs der Europäischen Union (EuGH) in der Rechtssache C-311/18 (Schrems II) (http://curia.europa.eu/juris/liste.jsf?num=C-311/18#).

[23] Erwägungsgrund 46 und Artikel 19 des Vorschlags.

[24] Diese Verweise beziehen sich auf i) zum einen die Einbeziehung der Verschlüsselung in die für die Strategie wichtigen Technologien, für die die EU die Kontrolle ihrer Lieferkette sicherstellen muss (S. 1), und zum anderen die Einbeziehung der Verschlüsselung in die Technologien, die die EU weiterentwickeln sollte (S. 18); ii) die Aussage in Abschnitt 2.4 der Strategie, der zufolge die Verschlüsselung als eine der drei Schlüsseltechnologien gilt, mit denen die Cybersicherheit integriert werden muss; und die Absicht, im Zusammenhang mit dem Aufbau einer sicheren Quantenkommunikationsinfrastruktur (QCI) für Europa „neue und sicherere Verschlüsselungsformen zu entwickeln, um sich so gegen Cyberangriffe zu schützen“, die ein hohes Maß an Vertraulichkeit bieten wird.

[25] Erklärung der Artikel 29-Datenschutzgruppe zu Verschlüsselung und ihrer Auswirkung auf den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogene Daten in der EU, Brüssel, 11. April 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

[26] EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

[27] Laut Artikel 24 Absatz 2 des Vorschlags wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Artikel 24 Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden.

[28] Vgl. die Stellungnahme 8/2019 des EDSA zur Zuständigkeit einer Aufsichtsbehörde im Falle einer Veränderung von Umständen, die die Hauptniederlassung oder die einzige Niederlassung betrifft, angenommen am 12. Juli 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishment_de.pdf.