EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17. Mai 2022

Stellungnahme 7/2022

zu dem Vorschlag für eine Verordnung über die Informationssicherheit 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 bezieht sich auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Informationssicherheit 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. Der EDSB hat sich in seinen nachstehenden Bemerkungen auf die Bestimmungen des Vorschlags beschränkt, die unter dem Blickwinkel des Datenschutzes besonders relevant sind.

Zusammenfassung

Am 22. März 2022 nahm die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union („Vorschlag“) an.

Der EDSB begrüßt das Ziel des Vorschlags, die Sicherheit der von den Organen und Einrichtungen der Union bearbeiteten Informationen zu verbessern, indem in einem spezifischen Rechtsinstrument gemeinsame Vorschriften für die Informationssicherheit festgelegt und eine kohärente Kultur der Informationssicherheit gefördert werden.

Der EDSB stellt fest, dass die Sicherheit personenbezogener Daten, wie sie in der EU-DSVO vorgeschrieben ist, einen Anwendungsbereich hat, der sich nur teilweise mit dem Anwendungsbereich der Informationssicherheit gemäß dem Vorschlag überschneidet. Letzterer hebt vor allem auf die Vertraulichkeit von Informationen ab, während die EU-DSVO auch Integrität und Verfügbarkeit gewährleistet. Darüber hinaus befassen sich die in der EU-DSVO enthaltenen Bestimmungen über die Sicherheit personenbezogener Daten speziell mit den Risiken für die Rechte und Freiheiten natürlicher Personen.

Gemäß dem Vorschlag sind die Organe und Einrichtungen der Union gehalten, Maßnahmen zur Informationssicherheit zu ergreifen, was unweigerlich die Verarbeitung personenbezogener Daten und elektronischer Kommunikationsdaten, einschließlich Verkehrsdaten, mit sich bringen wird. Nach Auffassung des EDSB muss deutlich gemacht werden, dass alle Informationssicherheitsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten mit dem geltenden Rechtsrahmen für Datenschutz und Privatsphäre im Einklang stehen sollten und dass die Organe und Einrichtungen der Union einschlägige technische und organisatorische Maßnahmen ergreifen sollten, um diesen Einklang in verantwortlicher Weise sicherzustellen.

Um Rechtssicherheit und Vorhersehbarkeit zu erreichen und die Einhaltung der EU-DSVO zu gewährleisten, empfiehlt der EDSB nachdrücklich, in dem Vorschlag oder zumindest in einem delegierten Rechtsakt, der später von der Kommission zu erlassen ist, die Verarbeitung personenbezogener Daten, die für die Zwecke dieser Verordnung zulässig ist, klar zu regeln. Der EDSB weist ferner darauf hin, dass die Einhaltung der EU-DSVO-Vorschriften für die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen sichergestellt sein muss. Darüber hinaus empfiehlt der EDSB, in einem Erwägungsgrund zu erläutern, dass alle Bestimmungen der EU-DSVO gelten, einschließlich der Vorschriften über internationale Übermittlungen.

Der EDSB unterstreicht die Bedeutung der Integration der Perspektive „Datenschutz und Schutz der Privatsphäre“ in das Management der Informationssicherheit, damit positive Synergien zwischen dem Vorschlag und den Rechtsvorschriften über Datenschutz und Schutz der Privatsphäre erzielt werden, und er formuliert konkrete Empfehlungen dazu, wie sich solche Synergien erreichen lassen, nämlich unter anderem durch eine spezifische Verpflichtung für die für Informationssicherheit verantwortlichen EU-Beamten, eng mit den gemäß Artikel 43 EU-DSVO

ernannten Datenschutzbeauftragten zusammenzuarbeiten; gegebenenfalls die Aufnahme der End-to-End-Verschlüsselung der Daten in die Liste der gemäß dem Vorschlag mindestens zu ergreifenden Sicherheitsmaßnahmen, insbesondere für den Fall vertraulicher, aber nicht als Verschlusssache eingestufter Informationen; und die Förderung eines integrierten Risikomanagements für die Informationssicherheit und eines integriertes Verfahrens für den Umgang mit Zwischenfällen, das bei Meldungen über Verletzungen des Schutzes personenbezogener Daten sowohl den Verpflichtungen im Bereich der Informationssicherheit als auch denen im Bereich des Datenschutzes gerecht wird.

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 des Europäischen Parlaments und des Rates über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union[2] (im Folgenden „Vorschlag“) an.

2. Am selben Tag nahm die Europäische Kommission einen weiteren Vorschlag für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union[3] (im Folgenden „Cybersicherheitsvorschlag“) an.

3. Beide Vorschläge waren in der am 16. Dezember 2020 vorgelegten Cybersicherheitsstrategie der EU für die digitale Dekade[4] (im Folgenden „Strategie“) vorgesehen. Oberstes Ziel der Strategie war 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 und die Grundrechte und Grundfreiheiten der Menschen in Europa zu begegnen.[5]

4. Der Vorschlag ist eine der Regulierungsinitiativen der Strategie, insbesondere im Bereich der Cybersicherheit der Organe, Einrichtungen und sonstigen Stellen der EU („Organe und Einrichtungen der Union“). Gemäß der Strategie verfolgt der Vorschlag zwei Ziele:

   - Erleichterung der **Interoperabilität von Systemen für die Behandlung von Verschlusssachen**, die eine reibungslose Informationsübermittlung zwischen den verschiedenen Einrichtungen ermöglicht, und

   - Ermöglichung eines **interinstitutionellen Ansatzes für den Umgang mit EU-Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen**, der dann auch als Modell für die Interoperabilität zwischen den Mitgliedstaaten dienen könnte, wobei die EU auch ihre Fähigkeit, mit den einschlägigen Partnern sicher zu kommunizieren, weiterentwickeln und dabei so weit wie möglich auf bestehenden Vereinbarungen und Verfahren aufbauen sollte.

5. Der EDSB stellt fest, dass der Gegenstand des vorliegenden Vorschlags auch in direktem Zusammenhang 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 2.0-Vorschlag“) steht. Der EDSB erinnert an seine Stellungnahme 5/2021 zur Cybersicherheitsstrategie[6] und zur NIS 2.0-Richtlinie („NIS 2.0-Stellungnahme“)[7]. Daher wird in der vorliegenden Stellungnahme auf die NIS 2.0-Stellungnahme verwiesen.

6. Der Begründung des Vorschlags zufolge ist die europäische Verwaltung in allen ihren Tätigkeitsbereichen aufgrund der ständig wachsenden Menge an vertraulichen, nicht als Verschlusssache eingestuften und als EU-Verschlusssache eingestuften Informationen („EU-VS“), die die Organe und Einrichtungen der Union untereinander austauschen müssen, und angesichts der dramatischen Entwicklung der Bedrohungslage Angriffen ausgesetzt. Die von den Organen und Einrichtungen der Union bearbeiteten Informationen sind ein sehr attraktives Ziel für die Angreifer und müssen angemessen geschützt werden.

7. Aus der Begründung geht hervor, dass der Vorschlag

   - harmonisierte und umfassende **Kategorien von Informationen** sowie **gemeinsame Regeln für den Umgang** mit Informationen für alle Organe und Einrichtungen der Union festlegen soll,

   - ein effizientes **System der Zusammenarbeit im Bereich der Informationssicherheit** zwischen den Organen und Einrichtungen der Union einrichten soll, das eine kohärente Kultur der Informationssicherheit in der gesamten europäischen Verwaltung fördern kann,

   - die **Strategien zur Informationssicherheit** auf allen Ebenen der Klassifizierung/Kategorisierung für alle Organe und Einrichtungen der Union unter Berücksichtigung des digitalen Wandels und der Entwicklung der Telearbeit als strukturelle Praxis **modernisieren** soll.

8. Am 22. März 2022 konsultierte die Kommission den EDSB gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 („EU-DSVO“)[8]. Die Anmerkungen und Empfehlungen in dieser Stellungnahme beschränken sich auf diejenigen Bestimmungen des Vorschlags, die für den Datenschutz am relevantesten sind.

2. Allgemeine Anmerkungen

9. Der EDSB erinnert daran, dass die Informationssicherheit, um die es in dem Vorschlag geht, von Anfang an Teil der Datenschutzvorschriften ist. Nach Artikel 4 Absatz 1 Buchstabe f EU-DSVO **ist die Sicherheit einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten**. 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**. Aus diesem Grund wird in dieser Stellungnahme zum einen der Frage nachgegangen, ob mit dem Vorschlag ein wirksames Informationssicherheitsmanagementsystem geschaffen wird oder ob er wirksame

Maßnahmen zur Erhöhung der Sicherheit von Informationen, einschließlich personenbezogener Daten, enthält.

10. Zum anderen erhöhen die Maßnahmen zur Informationssicherheit nicht nur die Sicherheit personenbezogener Daten und tragen nicht nur zum Schutz personenbezogener Daten bei, sondern können auch in die Rechte und Freiheiten der betroffenen Personen eingreifen, insbesondere in die Grundrechte auf Schutz personenbezogener Daten und auf Privatsphäre in der elektronischen Kommunikation. Daher wird in dieser Stellungnahme auch geprüft, ob der Vorschlag Maßnahmen vorsieht, die unter anderem **auf einer gültigen Rechtsgrundlage beruhen, spezifische und begrenzte Zwecke verfolgen und angemessen, notwendig und verhältnismäßig sind**.

11. Der EDSB nimmt zur Kenntnis, dass der Gegenstand des Vorschlags eine andere Perspektive hat als die Vorschläge zu NIS 2.0 und zur Cybersicherheit. Wir gehen davon aus, dass im Mittelpunkt der Cybersicherheit der Schutz von Netz- und Informationssystemen, der Schutz der Nutzer solcher Systeme und anderer von Cyberbedrohungen betroffener Personen steht, während **der Vorschlag sich mit Informationssicherheit in jeder Form befasst und nicht nur mit der Sicherheit von Informationen, die von IT-Systemen verarbeitet werden, die von Cyberbedrohungen betroffen sind**.

12. Der EDSB möchte betonen, dass für den NIS 2.0-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 zwar von Bedeutung ist, dass aber für den vorliegenden Vorschlag, in dem Vorschriften für Organe und Einrichtungen der Union festgelegt werden, **die EU-DSVO gilt und eine ebenso wichtige Rolle spielt**.

13. Der EDSB **begrüßt** das Ziel des Vorschlags, **die Sicherheit der von den Organen und Einrichtungen der Union bearbeiteten Informationen zu verbessern**, indem in einem spezifischen Rechtsinstrument gemeinsame Vorschriften für die Informationssicherheit festgelegt und eine kohärente Kultur der Informationssicherheit gefördert werden.

3. Spezifische Anmerkungen

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

14. Nach Artikel 3 Buchstabe b des Vorschlags bedeutet „Informationssicherheit“ die Gewährleistung der Authentizität, Verfügbarkeit, Vertraulichkeit, Integrität und Beweisbarkeit von Informationen. Der EDSB **stellt** jedoch **fest**, dass nach Artikel 2 Absatz 2 Informationen nur im Hinblick auf die **Vertraulichkeit** als Verschlusssache eingestuft werden und dass nach Artikel 2 Absatz 3 die Vertraulichkeitsstufen „den Schaden widerspiegeln, der für die legitimen privaten und öffentlichen Interessen der Union, der Organe und Einrichtungen der Union, der Mitgliedstaaten oder anderer Interessenträger durch eine unbefugte Offenlegung entstehen kann“. Auch im Rahmen des in Artikel 5 beschriebenen Informationssicherheitsrisiko-Managementprozesses liegt der Schwerpunkt

auf der Vertraulichkeit, denn dort wird nur die Vertraulichkeitsstufe von Informationen berücksichtigt.

15. Folglich weist der EDSB darauf hin, dass **die Sicherheit personenbezogener Daten**, wie sie in der EU-DSVO vorgeschrieben ist, **einen Anwendungsbereich hat, der sich nur teilweise mit dem Anwendungsbereich der Informationssicherheit gemäß dem Vorschlag überschneidet**. Gemäß Artikel 4 Absatz 1 Buchstabe f EU-DSVO ist die **Integrität und Vertraulichkeit** personenbezogener Daten zu gewährleisten, während gemäß Artikel 33 EU-DSVO die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen ist, indem gegen die **Risiken für die Rechte und Freiheiten natürlicher Personen** vorgegangen wird.

16. Wie jedoch bereits in der NIS 2.0-Stellungnahme ausgeführt[1], kann die Verfolgung der Ziele der Cybersicherheit zur Anwendung von Maßnahmen führen, 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.

17. Der Vorschlag sieht vor, dass die Organe und Einrichtungen der Union Maßnahmen zur Informationssicherheit anwenden, entweder als verbindliche Maßnahmen oder als Maßnahmen, die unter Berücksichtigung bestimmter Kriterien aus einem Risikomanagementprozess ausgewählt werden. In der Praxis werden einige dieser Maßnahmen unweigerlich **die Verarbeitung personenbezogener Daten und elektronischer Kommunikationsdaten, einschließlich Verkehrsdaten, umfassen**. Der Vorschlag enthält bereits einige verbindliche Maßnahmen, die die Verarbeitung personenbezogener Daten voraussetzen:

    - Artikel 11 Absatz 2: „Identifizierung“ und „Authentifizierung“;
    - Artikel 11 Absatz 3: „geeignete Sicherheitsprotokolle“;
    - Artikel 17 Absatz 1 Buchstabe a: „starke Authentisierung“;
    - Artikel 17 Absatz 1 Buchstabe f: „Maßnahmen zur Verhinderung und Erkennung von unbefugter Weitergabe von Daten“.

18. Der EDSB hält fest, dass Organisationen, die als Verantwortliche und Auftragsverarbeiter fungieren, nicht immer erkennen, dass die in Informationssicherheitssystemen und -diensten verarbeiteten Daten personenbezogene Daten darstellen können (z. B. IP-Adressen, Gerätekennungen, Netzwerkprotokolldateien, Protokolldateien für Zugangskontrollen usw.). Dies könnte gewisse Risiken bezüglich der Nicht-Einhaltung der Grundsätze des Datenschutzes und des Schutzes der Privatsphäre mit sich bringen, wie z. B. Rechtmäßigkeit der Verarbeitung, Datenminimierung, Zweckbindung,

[1] Siehe Ziffer 11 der NIS 2.0-Stellungnahme

Speicherbeschränkungen und Verpflichtungen für rechtmäßige Datenübermittlungen. Nach Auffassung des EDSB muss deutlich gemacht werden, dass **alle Informationssicherheitsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten mit dem geltenden Rechtsrahmen für Datenschutz und Privatsphäre im Einklang stehen sollten** und dass die Organe und Einrichtungen der Union einschlägige technische und organisatorische Maßnahmen ergreifen sollten, um diesen Einklang in verantwortlicher Weise sicherzustellen. Dies gilt umso mehr, wenn es keine geeignete Rechtsgrundlage für Organe und Einrichtungen der Union gibt, um personenbezogene Daten zur Umsetzung bestimmter Sicherheitsmaßnahmen zu verarbeiten; dann sollte die Schaffung und Begründung einer solchen Rechtsgrundlage geprüft werden.

19. 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 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).

20. Im Sinne von Rechtssicherheit und Vorhersehbarkeit und um die Einhaltung der EU-DSVO, insbesondere von deren Artikel 5 Absatz 1 Buchstabe a und Artikel 5 Absatz 2, zu gewährleisten, **empfiehlt der EDSB nachdrücklich, dass in dem Vorschlag die Verarbeitung personenbezogener Daten, die für die Zwecke dieser Verordnung zulässig ist (sofern in einem anderen sektorspezifischen/spezifischen Rechtstext nicht anders festgelegt) klar geregelt wird** und unter anderem festgelegt werden: der/die Zwecke(e) der Verarbeitung; Kategorien personenbezogener Daten; Kategorien betroffener Personen; gegebenenfalls die Rollen (Verantwortlicher, Auftragsverarbeiter, gemeinsam Verantwortliche), Aufbewahrungsfristen, Empfänger im Falle der Übermittlung an Stellen, die nicht der EU-DSVO unterliegen. Nach Auffassung des EDSB sollten diese Elemente ausdrücklich in dem Vorschlag oder zumindest in einem delegierten Rechtsakt enthalten sein, der anschließend von der Kommission erlassen wird. Der Vorschlag sollte einen solchen delegierten Rechtsakt vorsehen. Der EDSB weist ferner darauf hin, dass die Einhaltung der EU-DSVO-Vorschriften für die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen sichergestellt werden muss.

21. Der EDSB **begrüßt** Erwägungsgrund 6, wonach der Vorschlag die EU-DSVO unberührt lässt. Des Weiteren stellt der EDSB fest, dass Artikel 46 Absatz 9 einen Verweis auf die EU-DSVO enthält, insbesondere mit Blick auf die Übermittlung von EU-VS, die personenbezogene Daten enthalten, an Drittländer. Der EDSB erinnert daran, dass die EU-DSVO für jede kraft Gesetzes erfolgende Verarbeitung personenbezogener Daten gilt. Daher ist im verfügenden Teil des Vorschlags keine Bestimmung erforderlich, die die vollständige oder teilweise Anwendung der EU-DSVO vorsieht. Der EDSB räumt ein, dass internationale Übermittlungen personenbezogener Daten ein komplexes Thema sind, das eine zusätzliche Erinnerung an die Anwendbarkeit der EU-DSVO erfordert. In diesem Fall empfiehlt der EDSB, in einem Erwägungsgrund, möglicherweise in Erwägungsgrund 6, zu erläutern, dass **alle Bestimmungen der EU-DSVO, einschließlich** der Vorschriften über internationale Übermittlungen, Anwendung finden. Erwägungsgrund 6 kann auch

herangezogen werden, um weitere allgemeine Datenschutzempfehlungen aus dieser Stellungnahme aufzunehmen, die nicht auf eine Änderung der materiellrechtlichen Bestimmungen abzielen.

22. Der Vorschlag regelt den Umgang mit EU-Verschlusssachen sehr umfassend. EU-VS können wie alle anderen Informationen, die in den Anwendungsbereich des Vorschlags fallen, auch personenbezogene Daten enthalten. Folglich unterliegen sie den geltenden Datenschutzvorschriften, die auch in diesem Fall gelten und zusätzlich zu den EU-VS-Bestimmungen berücksichtigt werden müssen. Angesichts des Detailgrads der EU-VS-Vorschriften im Wortlaut empfehlen wir, dies in einem Erwägungsgrund ausdrücklich zu erwähnen.

3.2. Synergien mit dem Datenschutz und dem Schutz der Privatsphäre

23. In Artikel 33 EU-DSVO werden Personen und ihre Rechte und Freiheiten als Werte betrachtet, die im Rahmen des Sicherheitsrisikomanagements bei der Verarbeitung personenbezogener Daten zu schützen sind.

24. Der EDSB weist erneut darauf hin, dass **die Integration der Werte und der Perspektive „Schutz der Privatsphäre“ und „Datenschutz“ in den traditionellen Prozess des Informationssicherheitsmanagements einen ganzheitlichen Ansatz gewährleistet und Synergien zwischen den Organen und Einrichtungen der Union beim Management der Informationssicherheit und beim Schutz der von ihnen verarbeiteten Informationen ohne unnötige Vervielfachung der Anstrengungen ermöglichen wird**.

25. Der Einsatz von Technologien zur Verbesserung der Informationssicherheit sollte die Rechte und Freiheiten des Einzelnen nicht unangemessen beeinträchtigen. Der erste Schritt zur Vermeidung oder Eindämmung dieser Risiken besteht in der Umsetzung der Vorgaben des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 27 EU-DSVO, die dazu beitragen werden, geeignete Garantien wie **Pseudonymisierung**, **Verschlüsselung**, **Speicherbegrenzung und Datenminimierung** bei der Gestaltung und Nutzung dieser Technologien und Systeme zu integrieren.

26. Der EDSB erinnert daran, dass Verschlüsselung, einschließlich End-to-End-Verschlüsselung, kritische und unersetzliche Technologien für einen wirksamen Datenschutz und einen wirksamen Schutz der Privatsphäre sind.[2] Der EDSB begrüßt die Artikel 11 und 17 des Vorschlags, die die Verschlüsselung in die Liste der Mindestmaßnahmen zum Schutz von ruhenden Informationen und von Informationen während der Übertragung aufnehmen.

27. Da die Nutzung von Instrumenten und Diensten für die elektronische Zusammenarbeit und Kommunikation inzwischen in unserem normalen Arbeitsalltag üblich geworden ist, ist es sehr wichtig, auch die Sicherheit der elektronischen Kommunikation zu gewährleisten.

[2] *„Die Zukunft der Verschlüsselung in der EU“, Grundsatzrede des Datenschutzbeauftragten Wiewiórowski auf dem ISOC 2020 Webinar.*

Über ihre Vorteile für den Schutz der Privatsphäre in der elektronischen Kommunikation hinaus kann die **End-to-End-Verschlüsselung** auch Informationen schützen, die unter den Anwendungsbereich dieses Vorschlags fallen, wenn sie unter Einsatz elektronischer Kooperations- und Kommunikationsmittel ausgetauscht werden. Aus diesem Grund **empfiehlt der EDSB nachdrücklich, die End-to-End-Verschlüsselung gegebenenfalls in die Liste der Mindestsicherheitsmaßnahmen des Vorschlags aufzunehmen, insbesondere beim Austausch nicht als Verschlusssache eingestufter vertraulicher Informationen**.

28. Unter Berücksichtigung der immer häufigeren Nutzung und Einführung von Cloud-Diensten durch die Organe und Einrichtungen der Union **empfiehlt der EDSB, in Artikel 5 Absatz 3 hinzuzufügen**, dass **zu den Faktoren, die im Informationssicherheitsrisiko-Managementprozess berücksichtigt werden, auch die Bedrohungen gehören, die sich aus dem Zugang auf der Grundlage der Rechtsvorschriften von Drittländern (z. B. durch deren Behörden) ergeben**. Dies ist ein weiteres Beispiel für mögliche Synergien zwischen Informationssicherheit und Datenschutz. Wird gegen diese Risiken in einem Bereich vorgegangen, wird auch gegen die Risiken in dem anderen Bereich für dieselben Informationssysteme vorgegangen, in denen in den Anwendungsbereich des Vorschlags fallende personenbezogene Daten und Informationen verarbeitet werden.

29. Schließlich ist es bezüglich des Umgangs mit Informationssicherheitsvorfällen, die eine Verletzung des Schutzes personenbezogener Daten nach sich ziehen können, oder des Umgangs mit einer Verletzung des Schutzes personenbezogener Daten, die nützliche Elemente zur Bewältigung eines Informationssicherheitsvorfalls aufzeigt, **dringend ratsam, in einem entsprechenden Erwägungsgrund** die Vorteile eines **integrierten Verfahrens zur Bewältigung von Vorfällen[3] zu erläutern, das sowohl der Informationssicherheit als auch den Datenschutzpflichten bei Meldungen von Datenschutzverletzungen dient**. Auf diese Weise kann der Verantwortliche Zeit und Ressourcen sparen und in beiden Bereichen viel effizienter auf Vorfälle reagieren.

30. Um solche Synergien zwischen Informationssicherheit und Datenschutz zu gewährleisten, **empfiehlt der EDSB nachdrücklich, dass der Vorschlag eine spezifische Verpflichtung für die für Informationssicherheit zuständigen EU-Beamten vorsieht, eng mit dem gemäß Artikel 43 EU-DSVO benannten Datenschutzbeauftragten zusammenzuarbeiten**, wenn es um Tätigkeiten wie die Anwendung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf Informationssicherheitsmaßnahmen, die Auswahl von Sicherheitsmaßnahmen, die personenbezogene Daten umfassen, das integrierte Risikomanagement und die integrierte Behandlung von Sicherheitsvorfällen geht.

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

4. Schlussfolgerungen

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

- Der EDSB empfiehlt nachdrücklich, dass in dem Vorschlag die Verarbeitung personenbezogener Daten, die für die Zwecke dieser Verordnung zulässig ist, klar geregelt wird und unter anderem festgelegt werden: der/die Zwecke(e) der Verarbeitung; Kategorien personenbezogener Daten; Kategorien betroffener Personen, gegebenenfalls die Rollen (Verantwortlicher, Auftragsverarbeiter, gemeinsam Verantwortliche), Aufbewahrungsfristen, Empfänger im Falle der Übermittlung an Stellen, die nicht der EU-DSVO unterliegen. Nach Auffassung des EDSB sollten diese Elemente ausdrücklich in dem Vorschlag oder zumindest in einem delegierten Rechtsakt enthalten sein, der anschließend von der Kommission erlassen wird. Der Vorschlag sollte einen solchen delegierten Rechtsakt vorsehen.

- Der EDSB empfiehlt, in einem Erwägungsgrund zu erläutern, dass alle Bestimmungen der EU-DSVO gelten, einschließlich der Vorschriften über internationale Übermittlungen. Erwägungsgrund 6 kann auch herangezogen werden, um weitere allgemeine Datenschutzempfehlungen aus dieser Stellungnahme aufzunehmen, die nicht auf eine Änderung der materiellrechtlichen Bestimmungen abzielen.

- Der EDSB empfiehlt nachdrücklich, die End-to-End-Verschlüsselung gegebenenfalls in die Liste der Mindestsicherheitsmaßnahmen des Vorschlags aufzunehmen, insbesondere beim Austausch nicht als Verschlusssache eingestufter vertraulicher Informationen.

- Der EDSB empfiehlt, in Artikel 5 Absatz 3 hinzuzufügen, dass zu den Faktoren, die im Informationssicherheitsrisiko-Managementprozess berücksichtigt werden, auch die Bedrohungen gehören, die sich aus dem Zugang auf der Grundlage der Rechtsvorschriften von Drittländern (z. B. durch deren Behörden) ergeben.

- Der EDSB empfiehlt nachdrücklich, in einem entsprechenden Erwägungsgrund die Vorteile eines integrierten Informationssicherheitsrisiko-Managementprozesses und eines integrierten Verfahrens für den Umgang mit Vorfällen zu erläutern, das sowohl der Informationssicherheit als auch den Datenschutzpflichten bei Meldungen von Datenschutzverletzungen dient.

- Der EDSB empfiehlt nachdrücklich, dass der Vorschlag eine spezifische Verpflichtung für die für Informationssicherheit zuständigen EU-Beamten vorsieht, bei Tätigkeiten wie der Anwendung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf Informationssicherheitsmaßnahmen, der Auswahl von Sicherheitsmaßnahmen, die personenbezogene Daten umfassen, dem integrierten Risikomanagement und dem integrierten Umgang mit Sicherheitsvorfällen eng mit dem gemäß Artikel 43 EU-DSVO benannten Datenschutzbeauftragten zusammenzuarbeiten.

Brüssel, den 17. Mai 2022

Wojciech Rafał WIEWIÓROWSKI

[elektronisch unterzeichnet]

Endnoten

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] COM(2022) 119 final.
[3] COM(2022) 122 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, S. 5 der Strategie.
[6] Gemeinsame Mitteilung der Europäischen 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 2.0-Richtlinie.
[8] 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).