EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

9. November 2022

Stellungnahme 23/2022

zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

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

*Gemäß **Artikel 42 Absatz 1** der Verordnung 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".*

Die vorliegende Stellungnahme bezieht sich auf den Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020. 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 15. September 2022 legte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (im Folgenden „Vorschlag“) vor.

Der EDSB begrüßt den Vorschlag und unterstützt uneingeschränkt dessen allgemeines Ziel, das Funktionieren des Binnenmarkts zu verbessern und dazu einen einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festzulegen.

Der EDSB weist erneut darauf hin, dass in Artikel 5 Absatz 1 Buchstabe f der DSGVO die Sicherheit als einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten verankert ist. In Artikel 32 der DSGVO wird diese Verpflichtung, die sowohl für Verantwortliche als auch für Auftragsverarbeiter gilt, weiter ausgeführt, um ein angemessenes Maß an Sicherheit zu gewährleisten. Daher begrüßt der EDSB, dass die Grundsätze der Sicherheit und Datenminimierung bereits in den in Anhang I des Vorschlags aufgeführten grundlegenden Cybersicherheitsanforderungen enthalten sind. Darüber hinaus empfiehlt der EDSB nachdrücklich, den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in die grundlegenden Cybersicherheitsanforderungen für Produkte mit digitalen Elementen aufzunehmen.

Erwägungsgrund 17 enthält sehr wichtige Governance-Bestimmungen, die im operativen Teil des Vorschlags nicht berücksichtigt werden. Daher empfiehlt der EDSB, im operativen Teil des Vorschlags alle Aspekte im Zusammenhang mit der Schaffung von Synergien sowohl bei der Normung als auch bei der Zertifizierung im Bereich der Cybersicherheit sowie Synergien zwischen diesem Vorschlag und dem Datenschutzrecht der Union im Bereich der Marktüberwachung und der Rechtsdurchsetzung zu spezifizieren. Ferner erachtet es der EDSB für erforderlich, klarzustellen, dass mit dem Vorschlag nicht versucht wird, die Anwendung der bestehenden EU-Rechtsvorschriften für die Verarbeitung personenbezogener Daten zu beeinträchtigen, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, denen die Überwachung der Einhaltung dieser Instrumente obliegt.

Der EDSB begrüßt, dass in dieser Bestimmung anerkannt wird, dass die Verarbeitung personenbezogener Daten eine kritische und sensible Funktion ist und als solche für entsprechende kritische Produkte mit digitalen Elementen ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung notwendig machen könnte. Gleichzeitig empfiehlt der EDSB, in einem Erwägungsgrund des Vorschlags klarzustellen, dass die Erlangung einer europäischen Cybersicherheitszertifizierung im Rahmen des Vorschlags keine Garantie für die Einhaltung der DSGVO darstellt.

Schließlich begrüßt der EDSB die vorgeschlagenen Sanktionen, die denen der DSGVO für einen Verstoß gegen Artikel 32 der DSGVO über die Sicherheit der Verarbeitung ähneln und in Form einer Geldbuße von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes verhängt werden sollen.

Somit könnte der Vorschlag in Verbindung mit den Bestimmungen der DSGVO eine weitere Form des Schutzes für natürliche Personen bieten, die ihren Wohnsitz in EU-Mitgliedstaaten haben.

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, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr[1] (EU-DSVO), insbesondere auf Artikel 42 Absatz 1, –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1. Am 15. September 2022 legte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (im Folgenden „Vorschlag“) vor.

2. Das Ziel des Vorschlags besteht darin, das Funktionieren des Binnenmarkts zu verbessern und dazu einen einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festzulegen.[2] Der Vorschlag soll insbesondere die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen schaffen, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des gesamten Lebenszyklus eines Produkts ernsthaft um die Sicherheit kümmern. Außerdem sollen Bedingungen geschaffen werden, die es den Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen.[3]

3. Zu diesem Zweck wird mit dem Vorschlag Folgendes festgelegt[4]:

   - Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;

   - grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;

   - grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit

[1] ABl. L 295 vom 21.11.2018, S. 39.
[2] Erwägungsgrund 1 des Vorschlags.
[3] Erwägungsgrund 2 des Vorschlags.
[4] Artikel 1 des Vorschlags.

digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;

- Vorschriften für die Marktüberwachung und die Durchsetzung der oben genannten Vorschriften und Anforderungen.

4. Der Rechtsrahmen der EU umfasst mehrere horizontale Rechtsvorschriften, die bestimmte Aspekte im Zusammenhang mit der Cybersicherheit aus unterschiedlichen Blickwinkeln (Produkte, Dienste, Krisenmanagement und Straftaten) abdecken. Im Jahr 2013 trat die Richtlinie über Angriffe auf Informationssysteme[5] in Kraft, mit der die Strafbarkeit und die Strafen für eine Reihe von Straftaten gegen Informationssysteme harmonisiert wurden. Im August 2016 trat die Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[6] als erster EU-weiter Rechtsakt zur Cybersicherheit in Kraft. Durch ihre Überarbeitung, die zur NIS-2-Richtlinie führte, wurde die gemeinsame Zielvorgabe der EU in Bezug auf die Cybersicherheit von IKT-Diensten heraufgesetzt. 2019 trat der EU-Rechtsakt zur Cybersicherheit[7] in Kraft, mit dem die Sicherheit von IKT-Produkten, -Diensten und -Prozessen durch die Einführung eines freiwilligen europäischen Rahmens für die Cybersicherheitszertifizierung erhöht werden sollte.

5. Mit der vorliegenden Stellungnahme des EDSB wird das Konsultationsersuchen der Europäischen Kommission vom 15. September 2022 gemäß Artikel 42 Absatz 1 der EU-DSVO beantwortet. Der EDSB begrüßt, dass in Erwägungsgrund 71 des Vorschlags auf diese Konsultation verwiesen wird. In diesem Zusammenhang stellt der EDSB auch erfreut fest, dass er bereits vorab informell gemäß Erwägungsgrund 60 EU-DSVO konsultiert wurde.

2. Allgemeine Bemerkungen

6. Der EDSB begrüßt den Vorschlag und unterstützt uneingeschränkt dessen allgemeines Ziel, das Funktionieren des Binnenmarkts zu verbessern und dazu einen einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festzulegen.

7. Der Vorschlag sieht vor, dass Produkte mit digitalen Elementen nur dann auf dem Markt bereitgestellt werden dürfen, wenn sie bestimmte grundlegende Cybersicherheitsanforderungen an die Konzeption, Entwicklung und Herstellung dieser Produkte erfüllen. Darüber hinaus enthält der Vorschlag Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit. So müssen Hersteller beispielsweise bei der Konzeption und Entwicklung von Produkten mit digitalen Elementen die Cybersicherheit berücksichtigen.

---

[5] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218 vom 14.8.2013, S. 8.

[6] 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.

[7] 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.

8. Analog zur Einbeziehung der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in den Anwendungsbereich der NIS-2-Richtlinie, um ein hohes gemeinsames Cybersicherheitsniveau ihrer IKT-Systeme zu erreichen, würden mit dem vorliegenden Vorschlag gemeinsame Cybersicherheitsvorschriften für Hersteller und Entwickler von Produkten mit digitalen Elementen eingeführt, die sowohl Hardware als auch Software abdecken. Der EDSB stellt fest, dass solche Produkte in die IKT-Systeme von Anbietern digitaler Dienste eingebettet werden können, die als Einrichtungen im Sinne der NIS-2-Richtlinie fungieren, und von natürlichen Personen genutzt werden können, die digitale Dienste wie Mobiltelefone, Personalcomputer, Betriebssysteme und Softwareanwendungen nutzen. In diesem Zusammenhang erinnert der EDSB an seine Stellungnahme zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie[8].

9. In der Begründung[9] heißt es, dass die horizontalen Cybersicherheitsanforderungen:

   - zur Sicherheit personenbezogener Daten beitragen würden, indem sie die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Produkten mit digitalen Elementen schützen.

   - die Einhaltung der Sicherheitsanforderungen der DSGVO an die Verarbeitung personenbezogener Daten erleichtern.

   - die Transparenz und die Informationen für die Nutzer verbessern, auch für jene Nutzer, die geringere Cybersicherheitskompetenzen haben mögen. Die Nutzer würden auch besser über die Risiken, Fähigkeiten und Beschränkungen von Produkten mit digitalen Elementen informiert, wodurch sie besser in die Lage versetzt würden, die nötigen Präventions- und Minderungsmaßnahmen zu ergreifen, um die Restrisiken zu verringern.

10. Der EDSB weist darauf hin, dass nach Artikel 5 Absatz 1 Buchstabe f DSGVO die Sicherheit einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten ist. 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. Daher begrüßt der EDSB, dass die Grundsätze der Sicherheit und Datenminimierung bereits in den in Anhang I des Vorschlags aufgeführten grundlegenden Cybersicherheitsanforderungen enthalten sind.

11. Die Cybersicherheit von Produkten mit digitalen Elementen, die von natürlichen Personen genutzt werden, ist von größter Bedeutung, um ihre Rechte und Freiheiten, insbesondere das Recht auf Privatsphäre, zu schützen und ihr Vertrauen in digitale Dienste zu stärken. Ohne entsprechende Anforderungen können natürliche Personen Opfer von Cyberangriffen werden, die darauf abzielen, Zugang zu ihren personenbezogenen Daten und ihrer vertraulichen Kommunikation zu erhalten.

12. Aus diesem Grund ist der EDSB der Auffassung, dass die Festlegung eines einheitlichen Rechtsrahmens für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen für die Wahrung der Grundrechte und Grundfreiheiten, einschließlich des Rechts auf Privatsphäre und des Schutzes personenbezogener Daten, von wesentlicher Bedeutung ist, und unterstützt nachdrücklich

[8] Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie vom 11. März 2021.
[9] COM(2022) 454 final, S. 10.

den Vorschlag für ein umfassendes Paket einschlägiger wirksamer technischer und organisatorischer Maßnahmen.

13. Darüber hinaus erinnert der EDSB daran, dass in Artikel 25 DSGVO der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen festgelegt ist, der darauf abzielt, den Datenschutz und den Schutz der Privatsphäre in die Gestaltung von Verarbeitungsvorgängen und Informationssystemen vor der eigentlichen Verarbeitung zu integrieren und sicherzustellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich ist, verarbeitet werden. In der Praxis erfordert dieser Grundsatz u. a. den Einsatz von Technologien zum Schutz der Privatsphäre wie Verschlüsselung und Pseudonymisierung. In den Bestimmungen der DSGVO wird klargestellt, dass Sicherheit und Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen für die Einhaltung des EU-Datenschutzrechts von wesentlicher Bedeutung sind.

14. Bei Produkten mit digitalen Elementen beschränkt sich die Rolle der Hersteller in der Regel auf die Abgabe des Produkts an natürliche Personen. In der DSGVO werden den Herstellern keine direkten Anforderungen auferlegt, sondern die Hersteller sollten laut Erwägungsgrund 78 DSGVO lediglich „ermutigt werden", „*das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen*". Es liegt jedoch auf der Hand, dass sich die Nutzer letztlich gegen ein Produkt entscheiden werden, wenn sie bei seiner Nutzung in ihrer Rolle als Verantwortliche nicht in der Lage wären, die Datenschutzanforderungen einzuhalten. Daraus ergibt sich die indirekte „Anforderung" für die Hersteller, ihre Produkte so zu gestalten, dass die Nutzer die Anforderungen der DSGVO bei der künftigen Verarbeitung von Daten einhalten können.

15. Daher ist es trotz der Tatsache, dass die DSGVO nicht direkt an die Hersteller von Produkten mit digitalen Elementen gerichtet ist, sondern nur an Verantwortliche, deren IKT-Systeme solche Produkte enthalten, von wesentlicher Bedeutung, dass der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auch auf Produkte angewandt wird. Dies würde zum einen den Verantwortlichen die Einhaltung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erleichtern und zum anderen sicherstellen, dass personenbezogene Daten von natürlichen Personen, die mithilfe solcher Produkte auf digitale Dienste zugreifen, angemessen geschützt werden. Daher empfiehlt der EDSB nachdrücklich, den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in die grundlegenden Cybersicherheitsanforderungen für Produkte mit digitalen Elementen aufzunehmen.

3. Anwendungsbereich des Vorschlags

16. Der weit gefasste Anwendungsbereich des Vorschlags erstreckt sich auf jegliches Produkt mit digitalen Elementen, insbesondere „*ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- und Hardwarekomponenten, die*

getrennt in Verkehr gebracht werden sollen“[10] und dessen „*bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt*“[11]. Ein solches Produkt kann entweder physisch über Hardware-Schnittstellen oder logisch verbunden werden, z. B. über Netzwerksteckdosen, Leitungen, Dateien, APIs und sonstige Softwareschnittstellen.

17. Der EDSB geht davon aus, dass Produkte mit digitalen Elementen, die in den Anwendungsbereich des Vorschlags fallen, in die IKT-Systeme[12] der Verantwortlichen integriert und von natürlichen Personen verwendet werden können[13], um Zugang zu den von den Verantwortlichen erbrachten Diensten zur Verarbeitung personenbezogener Daten zu erhalten.

18. In diesem Zusammenhang empfiehlt der EDSB, in der Präambel des Vorschlags die Bedeutung von Produkten mit digitalen Elementen zu erläutern, die kryptografische Operationen[14] durchführen. Dazu gehören die Verschlüsselung gespeicherter oder gerade verwendeter oder übermittelter Daten sowie die Pseudonymisierung, wie es im Interesse einer wirksamen Informationssicherheit und Cybersicherheit sowie eines wirksamen Datenschutzes und Schutzes der Privatsphäre erforderlich ist. Darüber hinaus empfiehlt der EDSB im Einklang mit Erwägungsgrund 26 des Vorschlags, in Anhang II materielle und immaterielle Produkte mit digitalen Elementen, die kryptografische Operationen durchführen, aufzunehmen.

19. Der EDSB stellt fest, dass bestimmte digitale Produkte und Dienstleistungen, die sektorspezifischen Rechtsvorschriften unterliegen, nicht in den Anwendungsbereich des Vorschlags fallen. Hierzu gehören Software-as-a-Service, Medizinprodukte, In-vitro-Diagnostika, Kraftfahrzeuge sowie Produkte, die ausschließlich für die nationale Sicherheit oder militärische Zwecke verwendet werden oder speziell für die Verarbeitung von Verschlusssachen bestimmt sind.

20. Allerdings sind die sicherheitsrelevanten Bestimmungen einiger sektorspezifischer Rechtsvorschriften, die vom Anwendungsbereich des Vorschlags ausgenommen sind, nicht immer so detailliert und konkret wie die Bestimmungen des Vorschlags selbst. Dies gilt für die Verordnung (EU) 2017/745[15], in der allgemeine Sicherheitsmaßnahmen für Medizinprodukte festgelegt sind, jedoch nicht vorgeschrieben ist, dass die Produkte ohne bekannte Schwachstellen geliefert werden müssen oder dass relevante Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, nach dem neuesten Stand der Technik verschlüsselt werden müssen. Darüber hinaus sieht diese Verordnung vor: *„Die Hersteller führen ein Risikomanagementsystem ein, setzen dieses um, dokumentieren es und schreiben es fort.“* Es ist jedoch unklar, ob ein solches System auch Aspekte im

[10] Laut Artikel 3 Absatz 1 des Vorschlags bezeichnet der Ausdruck „Produkt mit digitalen Elementen“ ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen.

[11] In Artikel 3 Absatz 2 des Vorschlags heißt es: „Diese Verordnung gilt für Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.“

[12] Hardware und Betriebssystem von Servern, Software von Anwendungsservern, Software für Webanwendungen usw.

[13] Mobiltelefone, Personalcomputer, Betriebssysteme, Softwareanwendungen usw.

[14] Der EDSB erinnert an die Auswirkungen von Fehlern in von Diensteanbietern und Nutzern verwendeten Verschlüsselungsprodukten, wie die Sicherheitslücken „Heartbleed“ und „POODLE“, und an den Fall „VeraCrypt“.

[15] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. L 117 vom 5.5.2017, S. 1.

Zusammenhang mit der Cybersicherheit und dem Datenschutz abdecken muss. Daher empfiehlt der EDSB, die Verordnung (EU) 2017/745 aus der Liste der Rechtsvorschriften zu streichen, die von der Anwendung des Vorschlags ausgenommen sind.

21. Der EDSB stellt ferner fest, dass in Erwägungsgrund 15 auf Folgendes hingewiesen wird: „Die in dieser Verordnung festgelegten grundlegenden Anforderungen umfassen alle Elemente der grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU“ über die Bereitstellung von Funkanlagen[16]. Da sich Buchstabe e auf personenbezogene Daten und die Privatsphäre bezieht, empfiehlt der EDSB, in dem Vorschlag ausdrücklich klarzustellen, auf welche Elemente der grundlegenden Anforderungen zu personenbezogenen Daten und zum Schutz der Privatsphäre sich Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU erstreckt.

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

22. Der EDSB stellt fest, dass in Erwägungsgrund 17 des Vorschlags klargestellt wird, dass die Verordnung „unbeschadet“ der DSGVO gilt und dass Folgendes festgestellt wird:

    - Sowohl bei der Normung als auch bei der Zertifizierung von Cybersicherheitsaspekten sollten Synergien im Rahmen der Zusammenarbeit zwischen der Kommission, den europäischen Normungsorganisationen, der Agentur der Europäischen Union für Cybersicherheit (ENISA), dem durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss (EDSA) und den nationalen Datenschutzaufsichtsbehörden berücksichtigt werden.
    - Synergien zwischen dieser Verordnung und dem Datenschutzrecht der Union sollten auch im Bereich der Marktüberwachung und Rechtsdurchsetzung angestrebt werden. Dazu sollten die nach dieser Verordnung benannten nationalen Marktüberwachungsbehörden mit den Behörden zusammenarbeiten, die die Anwendung des Datenschutzrechtes der Union beaufsichtigen. Letztere Behörden sollten auch Zugang zu Informationen haben, die für die Erfüllung ihrer Aufgaben von Bedeutung sind.

23. Der EDSB stellt fest, dass Erwägungsgrund 17 sehr wichtige Governance-Bestimmungen enthält, die im operativen Teil des Vorschlags nicht berücksichtigt werden. Darüber hinaus wird nicht im Einzelnen ausgeführt, auf welche Weise diese „Synergien“ geschaffen werden könnten. Der EDSB befürchtet, dass solche Synergien in der Praxis mangels klarer entsprechender Bestimmungen unwahrscheinlich sind. Daher empfiehlt der EDSB, im operativen Teil des Vorschlags alle Aspekte im Einzelnen aufzuführen, die mit Synergien bei der Normung und Zertifizierung im Bereich Cybersicherheit sowie mit Synergien zwischen diesem Vorschlag und dem Datenschutzrecht der Union im Bereich der Marktüberwachung und Rechtsdurchsetzung (z. B. strukturierte Zusammenarbeit zwischen den einschlägigen Stellen, Bestimmungen über den Informationsaustausch,

[16] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. L 153 vom 22.5.2014, S. 62.

einschließlich personenbezogener Daten, in bestimmten Fällen usw.) in Zusammenhang stehen.

24. Ferner erachtet es der EDSB für erforderlich, ausdrücklich klarzustellen, dass mit dem Vorschlag nicht versucht wird, die Anwendung der bestehenden EU-Rechtsvorschriften für die Verarbeitung personenbezogener Daten zu beeinträchtigen, einschließlich der Aufgaben und Befugnisse der Aufsichtsbehörden, denen die Überwachung der Einhaltung dieser Instrumente obliegt.

5. Kritische digitale Produkte für die Verarbeitung personenbezogener Daten und europäisches Cybersicherheitssystem

25. In Erwägungsgrund 39 heißt es, dass mit dem Vorschlag Synergien mit der Verordnung (EU) 2019/881, dem EU-Rechtsakt zur Cybersicherheit[17], geschaffen werden sollen, mit der ein freiwilliger europäischer Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Prozessen und -Diensten hergestellt wird.

26. Darüber hinaus wird der Kommission gemäß Artikel 6 Absatz 5 Buchstabe b des Vorschlags die Befugnis übertragen, delegierte Rechtsakte zu erlassen, um Kategorien hochkritischer Produkte mit digitalen Elementen festzulegen, für die die Hersteller ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung erlangen müssen. Bei der Festlegung solcher Kategorien hochkritischer Produkte mit digitalen Elementen berücksichtigt die Kommission u. a. die bestimmungsgemäße Verwendung kritischer oder sensibler Funktionen, wie der Verarbeitung personenbezogener Daten[18].

27. In diesem Zusammenhang begrüßt der EDSB, dass im Vorschlag anerkannt wird, dass die Verarbeitung personenbezogener Daten eine kritische und sensible Funktion ist und als solche für entsprechende kritische Produkte mit digitalen Elementen ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung notwendig machen könnte. Gleichzeitig empfiehlt der EDSB, in der Präambel klarzustellen, dass die Erlangung einer europäischen Cybersicherheitszertifizierung im Rahmen des Vorschlags keine Garantie für die Einhaltung der DSGVO darstellt.

[17] 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.

[18] Artikel 6 Absatz 2 Buchstabe c des Vorschlags.

6. Sanktionen bei Verstößen der Wirtschaftsakteure

28. Im Einklang mit dem Vorschlag legen die Mitgliedstaaten bei Verstößen der Wirtschaftsakteure Sanktionen mit folgenden Obergrenzen fest:

   - Bei Nichteinhaltung der grundlegenden Anforderungen in Anhang I und der Herstellerpflichten werden Geldbußen von bis zu 15 Mio. EUR oder bis zu 2,5 % des gesamten weltweiten Jahresumsatzes verhängt, je nachdem, welcher Betrag höher ist.
   - Bei Verstößen gegen andere Pflichten aus der Verordnung über horizontale Cybersicherheitsanforderungen werden Geldbußen von bis zu 10 Mio. EUR oder bis zu 2 % des gesamten weltweiten Jahresumsatzes verhängt, je nachdem, welcher Betrag höher ist.

29. Werden gegenüber notifizierten Stellen und Marktüberwachungsbehörden auf deren Auskunftsverlangen hin falsche, unvollständige oder irreführende Angaben gemacht, so werden gegen den Rechtsverletzer Geldbußen von bis zu 5 Mio. EUR oder von bis zu 1 % des gesamten weltweiten Jahresumsatzes verhängt, je nachdem, welcher Betrag höher ist.

30. Der EDSB begrüßt die vorgeschlagenen Sanktionen, die denen der DSGVO für einen Verstoß gegen Artikel 32 DSGVO über die Sicherheit der Verarbeitung ähneln und in Form einer Geldbuße von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes verhängt werden sollen. Somit könnte der Vorschlag in Verbindung mit den Bestimmungen der DSGVO eine weitere Form des Schutzes für natürliche Personen bieten, die ihren Wohnsitz in EU-Mitgliedstaaten haben.

7. Schlussfolgerungen

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

(1) den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in die grundlegenden Cybersicherheitsanforderungen für Produkte mit digitalen Elementen aufzunehmen;

(2) in der Präambel die Bedeutung von Produkten mit digitalen Elementen zu erläutern, die kryptografische Operationen durchführen. Dazu gehören die Verschlüsselung gespeicherter oder gerade verwendeter oder übermittelter Daten sowie die Pseudonymisierung, wie es im Interesse einer wirksamen Informationssicherheit und Cybersicherheit sowie eines wirksamen Datenschutzes und Schutzes der Privatsphäre erforderlich ist;

(3) in Anhang II materielle und immaterielle Produkte mit digitalen Elementen, die kryptografische Operationen ausführen, aufzunehmen;

(4) die Verordnung (EU) 2017/745 aus der Liste der Rechtsvorschriften zu streichen, die von der Anwendung des Vorschlags ausgenommen sind;

(5) in dem Vorschlag ausdrücklich klarzustellen, auf welche Elemente der grundlegenden Anforderungen zu personenbezogenen Daten und zum Schutz sich Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU erstreckt;

(6) im operativen Teil des Vorschlags die praktischen Aspekte im Zusammenhang mit der Schaffung von Synergien sowohl bei der Normung als auch bei der Zertifizierung im Bereich der Cybersicherheit sowie Synergien zwischen diesem Vorschlag und dem Datenschutzrecht der Union im Bereich der Marktüberwachung und der Rechtsdurchsetzung zu spezifizieren;

(7) klarzustellen, dass mit dem Vorschlag nicht versucht wird, die Anwendung der bestehenden EU-Rechtsvorschriften für die Verarbeitung personenbezogener Daten zu beeinträchtigen, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, denen die Überwachung der Einhaltung dieser Instrumente obliegt;

(8) einschlägige Begriffsbestimmungen für „freie Software“, „Open-Source-Software“ und „freie und quelloffene Software“ zu ergänzen;

(9) in einem Erwägungsgrund des Vorschlags klarzustellen, dass die Erlangung einer europäischen Cybersicherheitszertifizierung im Rahmen des Vorschlags keine Garantie für die Einhaltung der DSGVO darstellt.

Brüssel, den 9. November 2022

(elektronisch unterzeichnet)
Wojciech Rafał WIEWIÓROWSKI