# Amtsblatt der Europäischen Union

C 258

Ausgabe in deutscher Sprache

## Mitteilungen und Bekanntmachungen

65. Jahrgang

5. Juli 2022


Inhalt



DE

([1]) Text von Bedeutung für den EWR.

II

*(Mitteilungen)*

# MITTEILUNGEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

# EUROPÄISCHE KOMMISSION

## Keine Einwände gegen einen angemeldeten Zusammenschluss

## (Sache M.10708 — CURA / OCG / DEUTSCHE EUROSHOP JV)

**(Text von Bedeutung für den EWR)**

(2022/C 258/01)

Am 23. Juni 2022 hat die Kommission nach Artikel 6 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 139/2004 des Rates ([1]) entschieden, keine Einwände gegen den oben genannten angemeldeten Zusammenschluss zu erheben und ihn für mit dem Binnenmarkt vereinbar zu erklären. Der vollständige Wortlaut der Entscheidung ist nur auf Englisch verfügbar und wird in einer um etwaige Geschäftsgeheimnisse bereinigten Fassung auf den folgenden EU-Websites veröffentlicht:

— der Website der GD Wettbewerb zur Fusionskontrolle (http://ec.europa.eu/competition/mergers/cases/). Auf dieser Website können Fusionsentscheidungen anhand verschiedener Angaben wie Unternehmensname, Nummer der Sache, Datum der Entscheidung oder Wirtschaftszweig abgerufen werden,

— der Website EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=de). Hier kann diese Entscheidung anhand der Celex-Nummer 32022M10708 abgerufen werden. EUR-Lex ist das Internetportal zum Gemeinschaftsrecht.

([1]) ABl. L 24 vom 29.1.2004, S. 1.

**Keine Einwände gegen einen angemeldeten Zusammenschluss**

**(Sache M.10529 — HEIDELBERGCEMENT / THOMA BRAVO / COMMAND ALKON)**

**(Text von Bedeutung für den EWR)**

(2022/C 258/02)

Am 11. April 2022 hat die Kommission nach Artikel 6 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 139/2004 des Rates ([1]) entschieden, keine Einwände gegen den oben genannten angemeldeten Zusammenschluss zu erheben und ihn für mit dem Binnenmarkt vereinbar zu erklären. Der vollständige Wortlaut der Entscheidung ist nur auf Englisch verfügbar und wird in einer um etwaige Geschäftsgeheimnisse bereinigten Fassung auf den folgenden EU-Websites veröffentlicht:

— der Website der GD Wettbewerb zur Fusionskontrolle (http://ec.europa.eu/competition/mergers/cases/). Auf dieser Website können Fusionsentscheidungen anhand verschiedener Angaben wie Unternehmensname, Nummer der Sache, Datum der Entscheidung oder Wirtschaftszweig abgerufen werden,

— der Website EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=de). Hier kann diese Entscheidung anhand der Celex-Nummer 32022M10529 abgerufen werden. EUR-Lex ist das Internetportal zum Gemeinschaftsrecht.

([1]) ABl. L 24 vom 29.1.2004, S. 1.

IV

*(Informationen)*

# INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

# EUROPÄISCHE KOMMISSION

## Euro-Wechselkurs [1]

**4. Juli 2022**

(2022/C 258/03)

**1 Euro =**

| | Währung | Kurs | | Währung | Kurs |
|---|---|---|---|---|---|
| USD | US-Dollar | 1,0455 | CAD | Kanadischer Dollar | 1,3435 |
| JPY | Japanischer Yen | 141,51 | HKD | Hongkong-Dollar | 8,2033 |
| DKK | Dänische Krone | 7,4391 | NZD | Neuseeländischer Dollar | 1,6748 |
| GBP | Pfund Sterling | 0,85960 | SGD | Singapur-Dollar | 1,4587 |
| SEK | Schwedische Krone | 10,7658 | KRW | Südkoreanischer Won | 1 353,40 |
| CHF | Schweizer Franken | 1,0037 | ZAR | Südafrikanischer Rand | 17,0275 |
| ISK | Isländische Krone | 139,30 | CNY | Chinesischer Renminbi Yuan | 6,9977 |
| NOK | Norwegische Krone | 10,2958 | HRK | Kroatische Kuna | 7,5301 |
| BGN | Bulgarischer Lew | 1,9558 | IDR | Indonesische Rupiah | 15 684,13 |
| CZK | Tschechische Krone | 24,745 | MYR | Malaysischer Ringgit | 4,6138 |
| HUF | Ungarischer Forint | 401,52 | PHP | Philippinischer Peso | 57,487 |
| PLN | Polnischer Zloty | 4,7100 | RUB | Russischer Rubel | |
| RON | Rumänischer Leu | 4,9440 | THB | Thailändischer Baht | 37,298 |
| TRY | Türkische Lira | 17,5994 | BRL | Brasilianischer Real | 5,5663 |
| AUD | Australischer Dollar | 1,5205 | MXN | Mexikanischer Peso | 21,1972 |
| | | | INR | Indische Rupie | 82,5067 |

[1] *Quelle*: Von der Europäischen Zentralbank veröffentlichter Referenz-Wechselkurs.

# RECHNUNGSHOF

## Sonderbericht 14/2022

## "Reaktion der Kommission auf Betrug im Bereich der Gemeinsamen Agrarpolitik: Es ist an der Zeit, das Problem an der Wurzel anzugehen"

(2022/C 258/04)

Der Europäische Rechnungshof teilt mit, dass der Sonderbericht 14/2022 "Reaktion der Kommission auf Betrug im Bereich der Gemeinsamen Agrarpolitik: Es ist an der Zeit, das Problem an der Wurzel anzugehen" soeben veröffentlicht wurde.

Der Bericht kann auf der Website des Europäischen Rechnungshofs direkt aufgerufen oder von dort heruntergeladen werden: https://www.eca.europa.eu/de/Pages/DocItem.aspx?did=61337

# EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

## Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung über den Schutz geografischer Angaben für handwerkliche und gewerbliche Erzeugnisse

*(Der vollständige Text dieser Stellungnahme ist in englischer, französischer und deutscher Sprache auf der Internetpräsenz des EDSB unter www.edps.europa.eu erhältlich)*

(2022/C 258/05)

Am 13. April 2022 nahm die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Schutz geografischer Angaben für handwerkliche und gewerbliche Erzeugnisse und zur Änderung der Verordnungen (EU) 2017/1001 und (EU) 2019/1753 des Europäischen Parlaments und des Rates und des Beschlusses (EU) 2019/1754 des Rates (im Folgenden „Vorschlag“) an.

Mit dem Vorschlag soll das System der EU für den Schutz geografischer Angaben ergänzt werden, das es bereits für landwirtschaftliche Erzeugnisse und Lebensmittel, Weine und Spirituosen gibt, und soll die wirksame Erfüllung der Verpflichtungen ermöglicht werden, die sich aus dem Beitritt der EU zur Genfer Akte des Lissabonner Abkommens ergeben.

Der EDSB begrüßt, dass in dem Vorschlag die Rollen der Kommission, des EUIPO und der zuständigen Behörden der Mitgliedstaaten bei der Verarbeitung personenbezogener Daten in den Verfahren nach diesem Vorschlag festgelegt werden.

Der EDSB empfiehlt, klarzustellen, ob die verschiedenen Verantwortlichen, die an der Verarbeitung personenbezogener Daten beteiligt sind, als gemeinsam Verantwortliche fungieren oder nicht. Sollte dies der Fall sein, empfiehlt der EDSB, eine Regelung gemäß Artikel 28 EU-DSVO und/oder Artikel 26 DSGVO vorzusehen. In diesem Zusammenhang erinnert der EDSB daran, dass detaillierte Regelungen zur Gewährleistung der Einhaltung der Datenschutzanforderungen erforderlichenfalls auch im Wege eines Durchführungsrechtsakts festgelegt werden können.

Der EDSB stellt fest, dass der Vorschlag die Einrichtung eines öffentlich zugänglichen elektronischen Registers geografischer Angaben für handwerkliche und gewerbliche Erzeugnisse vorsieht. In diesem Zusammenhang empfiehlt der EDSB eine klare Abgrenzung der Kategorien von Daten, die verarbeitet werden sollen. Der EDSB empfiehlt, in dem Vorschlag selbst alle Kategorien betroffener personenbezogener Daten zu spezifizieren. Schließlich ist der EDSB der Auffassung, dass die gewählte Datenspeicherfrist für die Unterlagen im Zusammenhang mit der Löschung geografischer Angaben weiter begründet werden sollte.

## 1. EINLEITUNG

1. Am 13. April 2022 nahm die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Schutz geografischer Angaben für handwerkliche und gewerbliche Erzeugnisse und zur Änderung der Verordnungen (EU) 2017/1001 und (EU) 2019/1753 des Europäischen Parlaments und des Rates sowie des Beschlusses (EU) 2019/1754 des Rates (im Folgenden „der Vorschlag“) an.

2. Ziel des Vorschlags ist es, einen unmittelbar anwendbaren Schutz geografischer Angaben (g.A.) für handwerkliche und gewerbliche Erzeugnisse auf EU-Ebene einzuführen. Außerdem soll sichergestellt werden, dass die Erzeuger in den Genuss des internationalen Rahmens für die Eintragung und den Schutz geografischer Angaben (im Folgenden „Lissabon-System“) kommen ([1]).

3. Der Vorschlag ergänzt den bestehenden EU-Schutz für geografische Angaben im Agrarbereich. In Bezug auf die Voraussetzungen für die Eintragung und den Schutz geografischer Angaben folgt er ähnlichen Ansätzen, wie sie für landwirtschaftliche Erzeugnisse und Lebensmittel, Weine und Spirituosen gelten, z. B. in

   — der Verordnung (EU) Nr. 1151/2012 des Europäischen Parlaments und des Rates ([2]) über Qualitätsregelungen für Agrarerzeugnisse und Lebensmittel,

([1]) COM(2022) 174 final, S. 1.
([2]) ABl. L 343 vom 14.12.2012, S. 1.

— der Verordnung (EU) 2019/787 des Europäischen Parlaments und des Rates ([3]) über die Begriffsbestimmung, Bezeichnung, Aufmachung und Kennzeichnung von Spirituosen und

— der Verordnung (EU) Nr. 1308/2013 des Europäischen Parlaments und des Rates ([4]) über eine gemeinsame Marktorganisation für landwirtschaftliche Erzeugnisse ([5]).

4. Mit dem Vorschlag würde die Verordnung (EU) 2017/1001 des Europäischen Parlaments und des Rates über die Unionsmarke im Hinblick auf mögliche Konflikte zwischen geografischen Angaben und Marken geändert und würden zusätzliche Aufgaben für das Amt der Europäischen Union für geistiges Eigentum („EUIPO") festgelegt. Er schlägt ferner eine Änderung des Beschlusses (EU) 2019/1754 des Rates über den Beitritt der Europäischen Union zur Genfer Akte des Lissabonner Abkommens über Ursprungsbezeichnungen und geografische Angaben vor, um eine Verbindung zwischen dem EU-System zum Schutz geografischer Angaben für handwerkliche und gewerbliche Erzeugnisse und dem Lissabonner System herzustellen ([6]).

5. Mit der vorliegenden Stellungnahme des EDSB wird das Konsultationsersuchen der Europäischen Kommission vom 13. April 2022 gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 beantwortet. Der EDSB begrüßt, dass in Erwägungsgrund 63 des Vorschlags auf diese Konsultation verwiesen wird. Die Anmerkungen und Empfehlungen in dieser Stellungnahme beschränken sich auf diejenigen Bestimmungen des Vorschlags, die aus datenschutzrechtlicher Sicht am relevantesten sind.

## 4. **SCHLUSSFOLGERUNG**

16. Vor diesem Hintergrund

— begrüßt der EDSB die ausdrückliche Benennung der für die Verarbeitung personenbezogener Daten in den im Vorschlag festgelegten Verfahren Verantwortlichen;

— empfiehlt er, klarzustellen, ob die Verantwortlichen als „gemeinsam Verantwortliche" im Sinne von Artikel 28 EU-DSVO und Artikel 26 DSGVO betrachtet werden sollten;

— empfiehlt er, in dem Vorschlag alle Kategorien von Daten zu spezifizieren, die in das Register der geografischen Angaben der Union für handwerkliche und gewerbliche Erzeugnisse aufzunehmen sind;

— ist er der Auffassung, dass die vorgeschlagene Aufbewahrungsfrist für Unterlagen im Zusammenhang mit der Löschung der Eintragung von geografischen Angaben in Bezug auf personenbezogene Daten entweder näher begründet oder verkürzt werden sollte.

Brüssel, den 2. Juni 2022.

*Wojciech* Rafał WIEWIÓROWSKI

([3]) ABl. L 130 vom 17.5.2019, S. 1.
([4]) ABl. L 347 vom 20.12.2013, S. 671.
([5]) 1. Der EDSB wurde zu der Verordnung (EU) Nr. 1308/2013 konsultiert und nahm seine Stellungnahme am 14. Dezember 2011 an.
([6]) COM(2022) 174 final, S. 2.

# Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union

*(Der vollständige Text dieser Stellungnahme ist in englischer, französischer und deutscher Sprache auf der Internetpräsenz des EDSB unter www.edps.europa.eu erhältlich)*

(2022/C 258/06)

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.

## 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 ([1]) (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 ([2]) (im Folgenden „Cybersicherheitsvorschlag“) an.

([1]) COM(2022) 119 final.
([2]) COM(2022) 122 final.

3. Beide Vorschläge waren in der am 16. Dezember 2020 vorgelegten Cybersicherheitsstrategie der EU für die digitale Dekade ([3]) (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 ([4]).

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 ([5]) und zur NIS 2.0-Richtlinie („NIS 2.0-Stellungnahme") ([6]). 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 des Europäischen Parlaments und des Rates („EU-DSVO") ([7]). Die Anmerkungen und Empfehlungen in dieser Stellungnahme beschränken sich auf diejenigen Bestimmungen des Vorschlags, die für den Datenschutz am relevantesten sind.

([3]) 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).

([4]) Siehe Kapitel I EINLEITUNG, S. 5 der Strategie.

([5]) 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".

([6]) Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS 2.0-Richtlinie.

([7]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

## 4. **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

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

*[Der vollständige Text dieser Stellungnahme ist in englischer, französischer und deutscher Sprache auf der Internetpräsenz des EDSB unter www.edps.europa.eu erhältlich.]*

(2022/C 258/07)

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

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

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

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

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

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

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

## 1. EINLEITUNG

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

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

([1]) COM(2022) 122 final.
([2]) COM(2022) 119 final.

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

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

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

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

5. Der EDSB hält fest, dass der Gegenstand des vorliegenden Vorschlags mit dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 („NIS-2-Vorschlag“) eng verknüpft ist. Der EDSB erinnert an seine Stellungnahme 5/2021 zur Cybersicherheitsstrategie ([5]) und zur NIS-2-Richtlinie („NIS-2-Stellungnahme“) ([6]). Daher wird in der vorliegenden Stellungnahme auf die NIS-2-Stellungnahme verwiesen.

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

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

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

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

— für das Reaktionsteam für IT-Sicherheitsvorfälle für die Organe, Einrichtungen und sonstigen Stellen der Union („CERT-EU“) ([7]) als „Cybersicherheitszentrum“ für die Organe, Einrichtungen und sonstigen Stellen der Union im Einklang mit den Entwicklungen in den Mitgliedstaaten und weltweit eine neue Rolle definiert wird.

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

---

([3]) 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).

([4]) Siehe Kapitel I. EINLEITUNG der Strategie, S. 5.

([5]) Gemeinsame Mitteilung der Europäische Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade“.

([6]) Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie.

([7]) Die derzeitige Rolle des CERT-EU ergibt sich aus der Interinstitutionellen Vereinbarung 2018/C 12/01.

([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 vom 21.11.2018, S. 39).

## 4. **SCHLUSSFOLGERUNGEN**

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

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

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

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

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

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

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

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

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

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

Brüssel, den 17. Mai 2022

*Wojciech* Rafał WIEWIÓROWSKI

# INFORMATIONEN DER MITGLIEDSTAATEN

## Aktualisierung der Richtbeträge für das Überschreiten der Außengrenzen gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) [1] ausstellen

(2022/C 258/08)

Die Veröffentlichung der Richtbeträge für das Überschreiten der Außengrenzen gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) [2] ausstellen, erfolgt auf der Grundlage der Angaben, die die Mitgliedstaaten der Kommission gemäß Artikel 39 des Schengener Grenzkodexes (Kodifizierter Text) mitteilen.

Neben der Veröffentlichung im Amtsblatt wird eine monatlich aktualisierte Fassung auf die Webseite der Generaldirektion „Inneres" gestellt.

### VON DEN NATIONALEN BEHÖRDEN FÜR DAS ÜBERSCHREITEN DER AUSSENGRENZEN FESTGELEGTE RICHTBETRÄGE

ISLAND

*Änderung der in ABl. C 247 vom 13.10.2006, S. 19 veröffentlichten Angaben*

Nach isländischem Recht müssen Ausländer nachweisen, dass sie über ausreichende Mittel für ihren Aufenthalt in Island und für ihre Rückreise verfügen. Der Richtbetrag wurde auf 8 000 ISK pro Person und Tag festgesetzt. Für Ausländer, deren Aufenthaltskosten von einem Dritten getragen werden, wird dieser Richtbetrag halbiert. Bei jeder Einreise ist ein Gesamtbetrag von mindestens 40 000 ISK nachzuweisen.

### Liste der früheren Veröffentlichungen

ABl. C 247 vom 13.10.2006, S. 19.
ABl. C 77 vom 5.4.2007, S. 11.
ABl. C 153 vom 6.7.2007, S. 22.
ABl. C 164 vom 18.7.2007, S. 45.
ABl. C 182 vom 4.8.2007, S. 18
ABl. C 57 vom 1.3.2008, S. 38.
ABl. C 134 vom 31.5.2008, S. 19.
ABl. C 331 vom 31.12.2008, S. 13.
ABl. C 33 vom 10.2.2009, S. 1.
ABl. C 36 vom 13.2.2009, S. 100.
ABl. C 37 vom 14.2.2009, S. 8.
ABl. C 98 vom 29.4.2009, S. 11.
ABl. C 35 vom 12.2.2010, S. 7.
ABl. C 304 vom 10.11.2010, S. 5.
ABl. C 24 vom 26.1.2011, S. 6.
ABl. C 157 vom 27.5.2011, S. 8.
ABl. C 203 vom 9.7.2011, S. 16.
ABl. C 11 vom 13.1.2012, S. 13.
ABl. C 72 vom 10.3.2012, S. 44.
ABl. C 199 vom 7.7.2012, S. 8.
ABl. C 298 vom 4.10.2012, S. 3.
ABl. C 56 vom 26.2.2013, S. 13.
ABl. C 98 vom 5.4.2013, S. 3.
ABl. C 269 vom 18.9.2013, S. 2.
ABl. C 57 vom 28.2.2014, S. 2.
ABl. C 152 vom 20.5.2014, S. 25.
ABl. C 224 vom 15.7.2014, S. 31.
ABl. C 434 vom 4.12.2014, S. 3.
ABl. C 447 vom 13.12.2014, S. 32.
ABl. C 38 vom 4.2.2015, S. 20
ABl. C 96 vom 11.3.2016, S. 7.
ABl. C 146 vom 26.4.2016, S. 12.
ABl. C 248 vom 8.7.2016, S. 12.
ABl. C 111 vom 8.4.2017, S. 11.
ABl. C 21 vom 20.1.2018, S. 3.
ABl. C 93 vom 12.3.2018, S. 4.
ABl. C 153 vom 2.5.2018, S. 8
ABl. C 186 vom 31.5.2018, S. 10.

[1] Siehe die Liste früherer Veröffentlichungen am Ende dieser Aktualisierung.
[2] ABl. L 77 vom 23.3.2016, S. 1.

ABl. C 264 vom 26.7.2018, S. 6.

ABl. C 366 vom 10.10.2018, S. 12.

ABl. C 459 vom 20.12.2018, S. 38.

ABl. C 140 vom 16.4.2019, S. 7.

ABl. C 178 vom 28.5.2020, S. 3.

ABl. C 102 vom 24.3.2021, S. 8.

ABl. C 486 vom 3.12.2021, S. 26.

ABl. C 139 vom 29.3.2022, S. 3.

ABl. C 143 vom 31.3.2022, S. 6.

ISSN 1977-088X (elektronische Ausgabe)
ISSN 1725-2407 (Papierausgabe)

Amt für Veröffentlichungen
der Europäischen Union
L-2985 Luxemburg
LUXEMBURG

DE