EDPS

**EUROPEAN DATA PROTECTION SUPERVISOR**

The EU's independent data protection authority

10. Januar 2024

# Stellungnahme 2/2024

zu dem Vorschlag für eine Verordnung zur Änderung des Rechtsakts zur Cybersicherheit im Hinblick auf verwaltete Sicherheitsdienste

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", und 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 (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 zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste.[1] Die vorliegende Stellungnahme schließt künftige zusätzliche Bemerkungen 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. Die Stellungnahme beschränkt sich auf die Bestimmungen des Vorschlags, die unter dem Gesichtspunkt des Datenschutzes relevant sind.*

[1] COM(2023) 208 final.

**Zusammenfassung**

Am 18. April 2023 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste.

Ziel des Vorschlags ist es, europäische Systeme für die Cybersicherheitszertifizierung für „verwaltete Sicherheitsdienste" einzuführen, und zwar zusätzlich zu denen für IKT-Produkte, -Dienste und -Prozesse, die bereits unter die Verordnung (EU) 2019/881 fallen. Der EDSB wurde von der Europäischen Kommission am 14. November 2023 gemäß Artikel 42 Absatz 1 der EU-DSVO konsultiert.

In der vorliegenden Stellungnahme begrüßt der EDSB die Ziele des Vorschlags und ist der Ansicht, dass Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste in der Tat Anreize für Anbieter solcher Dienste schaffen und gleichzeitig kleinen und mittleren Unternehmen, die über keine internen Sicherheitsspezialisten verfügen und von externen Dienstleistern abhängig sind, die Auswahl eines qualifizierten Dienstleisters erleichtern könnten. Der EDSB schlägt eine Reihe von Änderungen an Elementen des neuen Artikels 51a vor und empfiehlt, im Vorschlag als Voraussetzung für die Zertifizierung festzulegen, dass die Anbieter einen Eigenerklärung abgeben, dass ihre Dienste und vorgeschlagenen Maßnahmen im Einklang mit dem geltenden Rechtsrahmen, einschließlich der Datenschutzvorschriften, stehen.

# 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, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[2], insbesondere Artikel 42 Absatz 1,

**HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:**

# 1. Einleitung

1. Am 18. April 2023 veröffentlichte die Europäische Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste[3] („der Vorschlag").

2. Ziel des Vorschlags ist es, europäische Systeme für die Cybersicherheitszertifizierung für „verwaltete Sicherheitsdienste" einzuführen, und zwar zusätzlich zu denen für IKT-Produkte, -Dienste und -Prozesse, die bereits unter den Rechtsakt zur Cybersicherheit fallen.[4] Der Begründung zufolge[5] spielen verwaltete Sicherheitsdienste eine immer größere Rolle bei der Verhütung und Eindämmung von Cybersicherheitsvorfällen. Die Zertifizierung verwalteter Sicherheitsdienste wird als wirksames Mittel erachtet, um Vertrauen in die Qualität solcher Dienste aufzubauen und dadurch das Entstehen einer europäischen Branche für vertrauenswürdige Cybersicherheitsdienste zu erleichtern. Einige Mitgliedstaaten haben bereits mit der Einführung von Zertifizierungssystemen für verwaltete Sicherheitsdienste begonnen. Daher besteht zunehmend die Gefahr einer Fragmentierung des Binnenmarkts für verwaltete Sicherheitsdienste, wenn in der Union uneinheitliche Systeme für die Cybersicherheitszertifizierung eingeführt werden. Der vorliegende Vorschlag ermöglicht die Schaffung europäischer Systeme für die Cybersicherheitszertifizierung solcher Dienste, womit eine solche Fragmentierung verhindert werden soll.[6]

3. Mit der vorliegenden Stellungnahme des EDSB wird gemäß Artikel 42 Absatz 1 der EU-DSVO das Konsultationsersuchen der Europäischen Kommission vom 14. November 2023

[2] ABl. L 295 vom 21.11.2018, S. 39.
[3] COM(2023) 208 final.
[4] 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.
[5] COM(2023) 208 final, S. 1.
[6] COM(2023) 208 final, S. 1.

beantwortet. Der EDSB begrüßt, dass im letzten (nicht nummerierten) Erwägungsgrund des Vorschlags auf diese Konsultation verwiesen wird.

## 2. Allgemeine Bemerkungen

4. Der EDSB begrüßt die Ziele des Vorschlags und ist der Ansicht, dass Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste in der Tat Anreize für Anbieter solcher Dienste schaffen und gleichzeitig kleinen und mittleren Unternehmen, die über keine internen Sicherheitsspezialisten verfügen und von externen Dienstleistern abhängig sind, die Auswahl eines qualifizierten Dienstleisters erleichtern könnten.

5. Der EDSB erinnert an die Empfehlungen in der Stellungnahme 7/2022[7] des EDSB zum Zusammenhang zwischen Cybersicherheit und Datenschutz, die auch im Kontext des vorliegenden Vorschlags gültig sind. Während die Cybersicherheit von Anfang an Teil der Datenschutzvorschriften ist und nun in Artikel 5 Absatz 1 Buchstabe f der DSGVO als einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten verankert ist, erinnerte der EDSB ferner daran, dass Maßnahmen zur Informationssicherheit nicht nur die Sicherheit personenbezogener Daten erhöhen und zum Schutz personenbezogener Daten beitragen, sondern auch in die Rechte und Freiheiten der betroffenen Personen eingreifen können, insbesondere in die Grundrechte auf Schutz personenbezogener Daten und auf Privatsphäre in der elektronischen Kommunikation. Einige der als verwaltete Sicherheitsdienste angebotenen Dienstleistungen, z. B. Penetrationstests, könnten schwerwiegend in die genannten Grundrechte eingreifen. Daher ist der EDSB der Auffassung, dass Anbieter verwalteter Sicherheitsdienste, auch wenn sie offiziell nicht als Verantwortliche für eine von ihnen vorgeschlagene oder eingeleitete Verarbeitung gelten, nach Möglichkeit nur Sicherheitsmaßnahmen einführen oder vorschlagen sollten, die im Einklang mit dem für ihre Dienste und den vorgeschlagenen Maßnahmen geltenden Rechtsrahmen, einschließlich der Datenschutzvorschriften, stehen, damit sie im Rahmen der europäischen Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste zertifiziert werden können. Dies würde es den Anbietern ermöglichen, rechtlich tragfähige Maßnahmen vorzuschlagen und die Compliance-Risiken für kleine und mittlere Unternehmen zu verringern.

6. Zwei Bestimmungen des Vorschlags befassen sich inhaltlich mit der Ausweitung der Systeme für die Cybersicherheitszertifizierung auf verwaltete Sicherheitsdienste. Daher hat der EDSB insbesondere die vorgeschlagenen Änderungen in Artikel 46 Absatz 2 und die Aufnahme eines Artikels 51a in die Verordnung (EU) 2019/881 geprüft. Der EDSB stellt fest, dass es sich bei den anderen Änderungen um sich daraus ergebende redaktionelle Änderungen handelt.

[7] Stellungnahme 7/2022 des EDSB zu dem Vorschlag für eine Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union, veröffentlicht am 17. Mai 2022, Absätze 9 und 10.

## 3. Angemessene Kenntnisse im Bereich des Datenschutzes

7. Der neue Artikel 51a würde die Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung von verwalteten Sicherheitsdiensten auflisten, d. h. im Wesentlichen die Ziele, die durch ein solches Zertifizierungssystem gewährleistet werden. Die Liste basiert auf dem früheren Artikel 51 über die Sicherheitsziele europäischer Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, ist jedoch an die Besonderheiten von verwalteten Sicherheitsdiensten angepasst. Ähnlich wie IKT-Produkte, -Dienste und -Prozesse müssen verwaltete Sicherheitsdienste, die gemäß den Zertifizierungssystemen bewertet wurden, bestimmte Sicherheitsanforderungen erfüllen, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu schützen, auf die im Zusammenhang mit der Erbringung dieser Dienste zugegriffen wird bzw. die in diesem Zusammenhang verarbeitet, gespeichert oder übermittelt werden.[8] Darüber hinaus trägt der Vorschlag nach Ansicht des EDSB der Tatsache Rechnung, dass die Sicherheit als Dienst von Anbietern verwaltet wird und sich die Ziele daher eher auf Faktoren konzentrieren müssen, die die Fähigkeit des potenziellen Anbieters zur Erbringung dieser Dienste gewährleisten. Der EDSB stellt fest, dass dies durch die Zielsetzung erreicht wird, dass die Dienste kontinuierlich mit der erforderlichen Kompetenz, Sachkenntnis und Erfahrung von Personal mit einem sehr hohen Maß an einschlägigen Fachkenntnissen und beruflicher Integrität erbracht werden.

8. Der EDSB begrüßt den in dem neuen Artikel 51a gewählten Ansatz. Wie bereits in den allgemeinen Bemerkungen angedeutet, hat der EDSB jedoch einige Bedenken, wenn Aspekte in Bezug auf die Einhaltung der Rechtsvorschriften, insbesondere Datenschutzaspekte, nicht zu den Zielen gehören, die mit den Zertifizierungssystemen gewährleistet werden sollten.

9. Der EDSB erinnert daran, dass eine Funktion der Zertifizierung darin bestehen würde, Vertrauen in die Dienste zu schaffen und den Einrichtungen, die nur über geringe Ressourcen verfügen, verwaltete Sicherheitsdienste von hoher Qualität zur Verfügung zu stellen. Dieser Funktion würde entgegengewirkt, wenn vorgeschlagene Maßnahmen vom Kunden rechtmäßig bewertet werden müssten. Vor allem wenn sich ein kleines oder mittleres Unternehmen auf die Zertifizierung seiner Anbieter stützt, könnte es trotz seiner potenziellen Rolle als Verantwortlicher durch die Aufgabe, die Rechtmäßigkeit der vorgeschlagenen Maßnahmen unabhängig und kritisch zu bewerten, überfordert sein. Um zu vermeiden, dass zertifizierte Anbieter Maßnahmen vorschlagen, die eine unverhältnismäßige oder anderweitig illegale Datenverarbeitung beinhalten, empfiehlt der EDSB, als Voraussetzung für die Zertifizierung eine Eigenerklärung zur Konformität ihrer Dienste und der von ihnen vorgeschlagenen Maßnahmen mit dem geltenden Rechtsrahmen, einschließlich der Datenschutzvorschriften, festzulegen.

[8] Vgl. die vorgeschlagene Änderung von Artikel 46 Absatz 2 des Rechtsakts zur Cybersicherheit.

# 4. Sonstige Bemerkungen zu den Sicherheitszielen (Artikel 51a)

10. Artikel 51a Buchstabe c enthält eine Anforderung an den Anbieter, die von ihm bei der Erbringung verwalteter Sicherheitsdienste verarbeiteten Daten zu schützen. Obwohl der Wortlaut „anderweitig verarbeitet“ als Auffangbestimmung dient, schlägt der EDSB vor, das Wort „generiert“ in die Liste aufzunehmen. Gemäß der neuen Nummer 14a von Artikel 2 der Rechtsakte zur Cybersicherheit bezeichnet ein „verwalteter Sicherheitsdienst“ einen Dienst, der in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement besteht und unter anderem die Reaktion auf Sicherheitsvorfälle sowie Penetrationstests, Sicherheitsaudits und Beratung umfasst. Einige dieser Risikomanagementinstrumente sind in der Lage, Informationen zu ermitteln und zu sammeln, die für Angriffe auf Einrichtungen genutzt werden könnten (z. B. Schwachstellen des Systems, öffentlich zugängliche Informationen, die für Social-Engineering-Angriffe verwendet werden können). Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM) aggregieren Protokolle und ordnen Ereignisse zu, um Bedrohungen zu identifizieren und Berichte über die Sicherheit der Systeme zu erstellen. Nach Ansicht des EDSB wäre es daher angebracht, die Kritikalität der von diesen Systemen generierten Informationen hervorzuheben, indem diese durch Hinzufügen des Begriffs „generiert“ und zusammen mit den bereits aufgeführten Begriffen „zugegriffen, gespeichert, übermittelt“ explizit erwähnt werden.

11. In Buchstabe d ist als Ziel der Zertifizierungssysteme festgelegt, dass bei einem physischen oder technischen Sicherheitsvorfall die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht werden und der Zugang zu ihnen zeitnah wieder hergestellt wird. Der EDSB ist der Ansicht, dass beide Aspekte – physisch oder technisch – zwar erschöpfend sind, wenn es um Sicherheitsmaßnahmen geht, aber nicht das gesamte Spektrum möglicher Sicherheitsvorfälle abdecken. Sicherheitsvorfälle, die auf menschliches Versagen oder böswillige Handlungen von Mitarbeitern zurückzuführen sind, sollten ebenfalls erfasst werden, auch wenn sie weder einen Verstoß gegen die technische noch gegen die physische Sicherheit darstellen. Um keine Sicherheitsvorfälle auszuschließen, schlägt der EDSB folgenden Wortlaut vor: „Bei einem Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt“, ohne den Vorfall weiter einzuschränken.

12. In Buchstabe e ist als Ziel festgelegt, dass befugte Personen, Programme oder Maschinen nur Zugriff auf die Daten, Dienste oder Funktionen haben, „zu denen sie zugangsberechtigt sind“. Der EDSB stellt fest, dass der Wortlaut „zu denen sie zugangsberechtigt sind“ auf dem entsprechenden Buchstaben c des bestehenden Artikels 51 basiert. Der EDSB schlägt jedoch vor, die Gelegenheit zu nutzen, beide Bestimmungen umfassender und auch datenschutzorientierter zu gestalten: Derzeit sehen sie vor, dass die Nutzer nur auf die Ressourcen zugreifen sollten, zu denen ihnen Zugang gewährt wurde. Würde der Wortlaut jedoch durch „wenn dies für die Erfüllung ihrer Pflichten angemessen ist“ ersetzt, würde die formalistische Auffassung durch eine inhaltliche Auffassung ersetzt werden, die sowohl Sicherheits- als auch Datenschutzerwägungen Rechnung trägt, wonach die Zugangsrechte dem Grundsatz „Kenntnis nur, wenn nötig“ oder „Zugang erforderlich“ entsprechen müssen.

# 5. Schlussfolgerungen

13. Vor diesem Hintergrund empfiehlt der EDSB,

– *im Rahmen des Vorschlags als Voraussetzung für die Zertifizierung festzulegen, dass die Anbieter eine Eigenerklärung abgeben, dass ihre Dienste und die von ihnen vorgeschlagenen Maßnahmen im Einklang mit dem geltenden Rechtsrahmen, einschließlich der Datenschutzvorschriften, stehen.*

Brüssel, 10. Januar 2024

*(elektronisch unterzeichnet)*
Wojciech Rafał WIEWIÓROWSKI