EUROPÄISCHE
KOMMISSION

Brüssel, den 19.11.2025
COM(2025) 837 final

2025/0360 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung)

{SWD(2025) 836 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

In ihrer Mitteilung über die Umsetzung und Vereinfachung („Ein einfacheres und schnelleres Europa“)[1] stellte die Kommission ihr Konzept für die Anpassung ihres Rechtsrahmens an eine zunehmend unsichere Welt vor: eine neue Initiative zur Vereinfachung, Klarstellung und Verbesserung des Besitzstands der EU als wichtige Maßnahme zur Förderung ihrer Wettbewerbsfähigkeit.

Diese Vision spiegelt den umfassenderen Plan wider, den Kommissionspräsidentin von der Leyen in ihren politischen Leitlinien für die Amtszeit 2024-2029 dargelegt hat[2]. Wie außerdem in den Berichten von Mario Draghi[3] und Enrico Letta[4] hervorgehoben wurde, hat sich die Anhäufung von Vorschriften bisweilen ungünstig auf die Wettbewerbsfähigkeit ausgewirkt. Menschen und Unternehmen brauchen rasche und sichtbare Verbesserungen, und zwar durch eine kosteneffizientere und innovationsfreundlichere Umsetzung unserer Vorschriften – unter Beibehaltung hoher Standards und der vereinbarten Ziele.

In seinen Schlussfolgerungen vom 20. März 2025 forderte der Europäische Rat die Kommission ferner auf, „weiter den EU-Besitzstand zu überprüfen und ihn Stresstests zu unterziehen, um Möglichkeiten zur weiteren Vereinfachung und Konsolidierung der bestehenden Rechtsvorschriften zu ermitteln“[5]. Ferner betonte der Rat, dass neue Vereinfachungsinitiativen folgen müssen. In seinen Schlussfolgerungen vom 26. Juni betonte der Europäische Rat, wie wichtig Rechtsvorschriften zur „einfachen Gestaltung“ sind, „ohne die Vorhersehbarkeit, die politischen Ziele und die hohen Standards zu untergraben“[6]. In seinen Schlussfolgerungen vom 23. Oktober 2025 bekräftigte der Europäische Rat, „dass dringend eine ehrgeizige und horizontal ausgerichtete Agenda für Vereinfachung und bessere Rechtsetzung auf allen Ebenen, d. h. auf EU-Ebene, auf nationaler und auf regionaler Ebene, sowie in allen Bereich vorangebracht werden muss, um die Wettbewerbsfähigkeit Europas sicherzustellen“. Ferner forderte der Rat die Kommission darin auf, „rasch weitere ehrgeizige Vereinfachungspakete, unter anderem [...] für den digitalen Bereich, [...] vorzulegen“.[7]

---

1 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Ein einfacheres und schnelleres Europa: Mitteilung über die Umsetzung und Vereinfachung, COM(2025) 47 final, 11. Februar 2025.

2 Von der Leyen, U., (2024) Europa hat die Wahl: Politische Leitlinien für die nächste Europäische Kommission 2024–2029. Abrufbar unter: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_de?filename=Political%20Guidelines%202024-2029_DE.pdf.

3 Draghi, M. (2024) The future of European competitiveness. Abrufbar unter: Draghi-Bericht über die Wettbewerbsfähigkeit der EU.

4 Letta, E. (2024) Much more than a market. Abrufbar unter: Enrico Letta - Much more than a market (April 2024).

5 Schlussfolgerungen des Europäischen Rates, EUCO 1/25, Brüssel, 20. März 2025, Absatz 13.

6 Schlussfolgerungen des Europäischen Rates, EUCO 12/25, Brüssel, 26. Juni 2025, Absatz 30.

7 Schlussfolgerungen des Europäischen Rates, EUCO 18/25, Brüssel, 23. Oktober 2025, Absätze 33 und 35.

In seiner Entschließung zur „Umsetzung und Straffung der EU-Binnenmarktvorschriften zur Stärkung des Binnenmarkts“, über die das Plenum am 11. September abstimmte[8], betonte das Europäische Parlament die Notwendigkeit von Vereinfachungen, um die Einhaltung der Vorschriften durch die Unternehmen zu erleichtern, ohne die zentralen politischen Ziele der EU zu gefährden.

Im Rahmen der Tätigkeiten der Konsultation und der Einbeziehung der Kommission hinsichtlich der Vereinfachungsagenda haben Interessenträger, die verschiedene Interessen vertreten, gezielte Änderungen bestimmter Vorschriften im digitalen Bereich gefordert, um die Befolgungskosten zu straffen und die Wechselwirkungen zwischen den Vorschriften in ihrem Sektor zu klären.

Mit einem Mehrwert von 791 Mrd. EUR in der gesamten Europäischen Union im Jahr 2022[9] spielt der Sektor der Informations- und Kommunikationstechnologien (IKT) eine entscheidende Rolle bei der Förderung der Wettbewerbsfähigkeit der EU in allen Wirtschaftszweigen, sowohl durch das Wachstum digitaler Unternehmen als auch aufgrund des Angebots wichtiger digitaler Lösungen in allen Bereichen. Die Digitalvorschriften haben entscheidend dazu beigetragen, ein faires Unternehmensumfeld in der EU zu schaffen. Sie haben einen echten Binnenmarkt für digitale Dienste geschaffen. Die EU hat eine Vorreiterrolle bei der digitalen Regulierung gespielt und den „Goldstandard“ für den besten Schutz der Grundrechte, der Verbrauchersicherheit und der europäischen Werte gesetzt.

Die Kommission setzt sich für einen umfassenden „Stresstest“ des digitalen Regelwerks während der gesamten Legislaturperiode ein. Das Ziel ist sehr klar: Es ist zu gewährleisten, dass die Vorschriften weiterhin geeignet sind, Innovation und Wachstum zu fördern, dass sie ihre Ziele erfüllen und ein Motor für die Wettbewerbsfähigkeit sind. In diesem gesamten Prozess wird sich die Kommission um überzeugende Lösungen bemühen, um die Wirksamkeit der Vorschriften zu verbessern und ihre Durchsetzung mit allen verfügbaren Instrumenten zu vereinfachen, zu klären und zu festigen, sei es durch regulatorische Anpassungen, verstärkte Zusammenarbeit von Behörden, Förderung digitaler Lösungen, die durch ihre konzeptuelle Gestaltung die Einhaltung der Vorschriften vereinfachen, oder durch andere begleitende Maßnahmen.

Der **Digital-Omnibus-Vorschlag ist ein erster Schritt** hin zu einer optimierten Anwendung des digitalen Regelwerks. Er enthält eine ganze Reihe technischer Änderungen an einem großen Bestand von Rechtsvorschriften für den digitalen Bereich, die ausgewählt wurden, um Unternehmen, öffentliche Verwaltungen sowie Bürgerinnen und Bürger sofort zu entlasten und so die Wettbewerbsfähigkeit zu fördern. Als unmittelbares Ziel soll die Einhaltung der Vorschriften zu geringeren Kosten und mit Erfüllung derselben Ziele erreicht werden, was den verantwortlichen Unternehmen einen Wettbewerbsvorteil bietet. Anhand der Konsultationen mit Interessenträgern und im ersten, von der Exekutiv-Vizepräsidentin Henna

---

8 Europäisches Parlament, Entschließung zur Umsetzung und Straffung der EU-Binnenmarktvorschriften zur Stärkung des Binnenmarkts, 11. September 2025 (2025/2009/INI).

9 Eurostat (2025) Statistics explained: ICT sector – value added, employment and R&D. Abrufbar unter: ICT sector - value added, employment and R&D - Statistics Explained - Eurostat.

Virkkunen und dem Kommissionsmitglied Michael McGrath geleiteten Umsetzungsdialog wurden vorrangige Änderungsanliegen ermittelt.

Somit liegt der Schwerpunkt der angestrebten Änderungen auf dem Erschließen von Chancen der Datennutzung als grundlegende Ressource der EU-Wirtschaft; das gilt nicht zuletzt hinsichtlich der Unterstützung von Entwicklung und Nutzung vertrauenswürdiger KI-Lösungen auf dem EU-Markt. Gezielte Änderungen der Vorschriften über den Datenschutz und den Schutz der Privatsphäre unterstützen dieses Ziel und bieten sofortige Vereinfachungsmaßnahmen für Unternehmen und Einzelpersonen, die ihre Fähigkeit zur Ausübung ihrer Rechte stärken.

Darüber hinaus liegen die Änderungen der Verordnung (EU) 2024/1689 (über künstliche Intelligenz[10]) als gesonderter Legislativvorschlag und Teil des Digital-Omnibus-Vorschlags vor; sie zielen darauf ab, die reibungslose und wirksame Anwendung der Vorschriften für die sichere und vertrauenswürdige Entwicklung und Nutzung von KI zu erleichtern.

Außerdem enthält der Digital-Omnibus-Vorschlag einen sehr klaren Lösungsvorschlag für die Straffung der Meldung von Cybersicherheitsvorfällen, der alle diesbezüglichen Meldepflichten in einem einheitlichen Meldemechanismus zusammenfasst.

Abschließend werden mit dem Vorschlag veraltete Vorschriften im Bereich der Regulierung von Plattformen aufgehoben und durch neuere Vorschriften ersetzt.

Diese Änderungen sollen die Vorschriften straffen, die Zahl der Rechtsvorschriften verringern und die Bestimmungen harmonisieren. Durch die Vereinfachung von Bestimmungen und Verfahren senken sie die Verwaltungskosten. Außerdem befreien die Änderungen kleine Midcap-Unternehmen von bestimmten Verpflichtungen gemäß den Datenrechtsvorschriften und der Verordnung (EU) 2024/1689 (über künstliche Intelligenz[11]) – neben den Klein- und Kleinstunternehmen, für die bereits eine Sonderregelung gilt. Sie fördern auch die Möglichkeiten für ein dynamisches Unternehmensumfeld und schaffen mehr Rechtssicherheit und Chancen, insbesondere beim Austausch und der Weiterverwendung von Daten, bei der Verarbeitung personenbezogener Daten oder beim Training von Systemen und Modellen der künstlichen Intelligenz.

Die vorgeschlagenen Änderungen sind weiterhin technischer Natur und zielen darauf ab, den Rechtsrahmen anzupassen, ohne seine zugrunde liegenden Ziele zu ändern. Die Maßnahmen sind so abgestimmt, dass dieselben Standards des Schutzes der Grundrechte gewahrt bleiben.

Zusammen mit dem Digital-Omnibus-Vorschlag bringt die Kommission auch ihren Verordnungsvorschlag für die **europäischen Unternehmensbrieftaschen** ein – eine zentrale Initiative zur vereinfachten Einhaltung der Rechtsvorschriften und für geringeren Verwaltungsaufwand für Unternehmen. Die Unternehmensbrieftaschen werden als sichere digitale Instrumente für Unternehmen entworfen und dienen als einheitliche Plattform für deren vereinfachte Interaktionen in der EU. Eine eindeutige und dauerhafte Kennung soll die

---

[10] Als separater Legislativvorschlag.

[11] Als separater Vorschlag.

Unternehmen in die Lage versetzen, Identitäten digital zu überprüfen, Dokumente zu unterzeichnen, Zeitstempel anzubringen und verifizierte digitale Informationen mithilfe einer einzigen Lösung nahtlos über Grenzen hinweg auszutauschen. Mit den europäischen Unternehmensbrieftaschen können Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), einfach die Einhaltung der Vorschriften sicherstellen. Das setzt wichtige Ressourcen frei, die sich auf Wachstum und Innovation lenken lassen.

Als zweiten Schritt gemäß der Verpflichtung zum „Stresstest" des digitalen Regelwerks führt **die Kommission auch eine digitale Eignungsprüfung durch**. Während die Digital-Omnibus-Vorschläge unmittelbar und zielgerichtet wirken, konzentriert sich die Analyse der digitalen Eignungsprüfung der Kommission auf die kumulativen Auswirkungen der Digitalvorschriften und soll prüfen, wie diese Vorschriften die Wettbewerbsfähigkeit der EU unterstützen können und wo in der zweiten Hälfte der Legislaturperiode weitere Anpassungen erforderlich sein werden.

Die digitale Eignungsprüfung wird mit einer breit angelegten öffentlichen Konsultation zeitgleich mit dem Omnibus-Vorschlag eingeleitet. Dabei ist die Kommission bestrebt, auf alle Interessenträger zuzugehen und breit angelegte Konsultationen durchzuführen. Das Ziel besteht darin, einen Überblick und eine umfassende Bestandsaufnahme darüber zu erstellen, wie das digitale Regelwerk strategische Sektoren der EU-Industrie abdeckt; auch geht es darum, wie sich die kumulative Wirkung der Vorschriften auf die Wettbewerbsfähigkeit auswirkt. Auf dieser Grundlage soll ein zweiter Analyseschritt tiefer in die Synergien und Bereiche eindringen, die weiter aufeinander abgestimmt werden könnten, von Definitionen und Rechtsbegriffen bis hin zur Wirksamkeit und dem Zusammenspiel der Verwaltungssysteme und anderer unterstützender Maßnahmen.

Auch in Umsetzungsdialogen und **Evaluierungen aller wichtigen Rechtsinstrumente** wird sich der „Stresstest" des digitalen Besitzstands fortsetzen. In der derzeitigen Planung geht die Kommission davon aus, neben anderen Initiativen im Jahr 2026 Folgendes zu veröffentlichen: Überprüfungen des Gesetzes über digitale Märkte, des Politikprogramms für die digitale Dekade, des Chip-Gesetzes und der Richtlinie über audiovisuelle Mediendienste sowie eine Bewertung der Urheberrechtsrichtlinie. Im Jahr 2027 werden voraussichtlich unter anderem die Cybersolidaritätsverordnung, die Verordnung über ein offenes Internet, die NIS-2-Richtlinie und das Gesetz über digitale Dienste bewertet werden. Im Jahr 2028 sollte die Kommission beispielsweise das Europäische Medienfreiheitsgesetz und die Datenverordnung bewerten; gleiches gilt anschließend im Jahr 2029 für die KI-Verordnung und die Verfallsklausel der Verordnung über die Einrichtung des Europäischen Kompetenzzentrums und Netzes für Cybersicherheit.

Interessenträger betonten wiederholt, bei den Vereinfachungsbemühungen gehe es in vielen Fällen weniger um die Änderung von Vorschriften als vielmehr um die Klärung ihrer Anwendung. Unbeschadet der Auslegungen des Gerichtshofs **betrachtet die Kommission eine Reihe von Leitlinien**, die eine einheitliche Anwendung der Vorschriften unterstützen sollen, als **vorrangig**.

Bezüglich des Regelungsrahmens für Daten kündigte die Kommission ihre Prioritäten in der Strategie für die Datenunion an: Sie konzentriert sich insbesondere auf Leitlinien für angemessene Gegenleistungen, um zu klären, was für die gemeinsame Datennutzung in Rechnung gestellt werden darf, was sowohl den Dateninhabern als auch den

Datenempfängern Rechtssicherheit bieten soll, sowie auf Leitlinien zur Klärung von Begriffsbestimmungen.

Um die Anwendung der Verordnung über künstliche Intelligenz zu unterstützen, räumt die Kommission der Herausgabe von Leitlinien zu mehreren Aspekten weiterhin Vorrang ein, wie in der Begründung des Digital-Omnibus-Vorschlags zur Änderung der Verordnung über künstliche Intelligenz näher ausgeführt ist.

Vorschläge des Digital-Omnibus-Pakets

In den letzten Jahren wurde der „**legislative Besitzstand im Datenbereich**“ ausgeweitet, sodass er nun aus einer ganzen Reihe von Rechtsvorschriften besteht, was nicht nur zu rechtlicher Komplexität geführt hat, sondern auch zu Überschneidungen, nicht vollständig angeglichenen Begriffsbestimmungen und Fragen zum Zusammenspiel der Rechtsinstrumente. Insbesondere sollte mit dem Erlass der Verordnung (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten) ein Binnenmarkt für Cloud-Dienste geschaffen werden. Diese Verordnung wurde teilweise durch Kapitel VI der Verordnung (EU) 2023/2854 (Datenverordnung) ersetzt, in der Verpflichtungen zum Wechsel zwischen Datenverarbeitungsdiensten festgelegt wurden.

Ein anderer solcher Fall ist Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt), das die Vorschriften über die Weiterverwendung von Informationen des öffentlichen Sektors der Richtlinie (EU) 2019/1024 (über offene Daten) in Bezug auf Daten, die sich nicht ohne Einschränkungen weiterverwendet lassen, ergänzt. Darüber hinaus wurden in anderen Kapiteln der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) Vorschriften über Datenvermittlungsdienste, Datenaltruismus und Anforderungen für Anträge ausländischer Regierungen auf Zugang zu nicht-personenbezogenen Daten eingeführt, und es wurde der Europäische Dateninnovationsrat eingerichtet. Andererseits wurde mit der Verordnung (EU) 2023/2854 (Datenverordnung) eine wesentliche Verpflichtung für Hersteller vernetzter Geräte und Anbieter diesbezüglicher Dienste bezüglich der Datenweitergabe an ihre Nutzer und für Unternehmen bezüglich der Datenweitergabe an Regierungsstellen eingeführt, ebenso wie Vorschriften über faire Datenweitergabevereinbarungen.

Diesbezüglich enthält der Digital-Omnibus-Vorschlag einen Vorschlag zur Aufhebung veralteter Vorschriften, insbesondere der Vorgaben der Verordnung (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten); als Ausnahme hiervon besteht weiterhin das Verbot von Datenlokalisierungsauflagen in der Union, außerdem sind die Vorschriften der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) zu konsolidieren und zu straffen, etwa die Vorschriften über Datenaltruismus und Datenvermittlungsdienste, um diese Datenweitergabemechanismen attraktiver zu machen. Gleichzeitig schaffen die Vorschriften des Daten-Governance-Rechtsaktes über die Weiterverwendung geschützter Daten zusammen mit den Vorschriften der Richtlinie (EU) 2019/1024 (über offene Daten) einen einheitlichen Rahmen für die Weiterverwendung von Daten, die im Besitz öffentlicher Stellen sind; dies fließt in die Verordnung (EU) 2023/2854 (Datenverordnung) mit ein. Diese Lösung bietet zahlreiche Vorteile für öffentliche Verwaltungen mit Daten des öffentlichen Sektors, sowie für Weiterverwender, denn sie strafft Verfahren und verringert den Verwaltungsaufwand der Auslegung und Umsetzung diverser nationaler Rechtsvorschriften.

Ferner eröffnet der Vorschlag öffentlichen Stellen die Möglichkeit, unterschiedliche Bedingungen festzulegen und für die Weiterverwendung durch sehr große Unternehmen höhere Gebühren zu erheben; das gilt insbesondere für als Torwächter benannte Unternehmen

im Sinne des Artikels 3 der Verordnung (EU) 2022/1925 (Gesetz über digitale Märkte), die über eine beträchtliche Marktmacht und erheblichen Einfluss auf den Binnenmarkt verfügen. Um zu verhindern, dass solche Einrichtungen ihre erhebliche Marktmacht zum Nachteil des fairen Wettbewerbs und der Innovation ausnutzen, können öffentliche Stellen besondere Bedingungen für die Weiterverwendung von Daten und Dokumenten seitens dieser Stellen festlegen.

Der Vorschlag umfasst die konsolidierten und gestrafften Vorschriften der Verordnungen (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten) und (EU) 2022/868 (Daten-Governance-Rechtsakt) sowie der Richtlinie (EU) 2019/1024 (über offene Daten) in der Verordnung (EU) 2023/2854 (Datenverordnung), was gemeinsam ein einziges konsolidiertes Instrument für die europäische Datenwirtschaft schafft. Die Verordnung (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten), die Richtlinie (EU) 2019/1024 (über offene Daten) und die Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) werden aufgehoben. Die Vorschriften aller vier Instrumente werden gestrafft und besser aufeinander abgestimmt; so sorgen sie für mehr Klarheit und Kohärenz, sind wirksamer und unterstützen die Unternehmen bei der Innovationsförderung. Diese Initiative steht im Einklang mit der Strategie der Datenunion, die im Wesentlichen den Rechtsrahmen vereinfachen soll.

Um kleinere Unternehmen weiter zu unterstützen, werden die Vorschriften, die kleinen und mittleren Unternehmen (KMU) die Einhaltung der EU-Datenrechtsvorschriften erleichtern, auf kleine Unternehmen mit mittlerer Kapitalisierung (Midcap-Unternehmen) ausgeweitet. Die Verordnung (EU) 2023/2854 (Datenverordnung), die am 12. September 2025 in Kraft trat, ist ein wichtiger Schritt hin zu einer fairen und wettbewerbsfähigen Datenwirtschaft in der EU. Die darin vorgeschlagenen Änderungen sollen die Errungenschaften der Verordnung (EU) 2023/2854 (Datenverordnung) nicht ändern.

Jedoch sind vier wichtige Elemente abzustimmen, um das Ziel des Gleichgewichts von Innovation und Datenverfügbarkeit einerseits und Schutz der Rechte und Interessen der Dateninhaber andererseits in vollem Umfang zu erreichen. Insbesondere ist es wichtig, zu gewährleisten, dass die Verordnung (EU) 2023/2854 (Datenverordnung) nicht nur den Aufwand verringert, sondern auch die Rechtsklarheit erhöht und die Wettbewerbsfähigkeit fördert. Erstens ist es dringend erforderlich, die Schutzvorkehrungen gegen das Durchsickern von Geschäftsgeheimnissen in Drittländer zu stärken; das gilt im Kontext der verbindlichen Bestimmungen über den Datenaustausch im Internet der Dinge (*Internet of Things*, IoT). Zweitens könnte der weit angewendete Rahmen der Beziehungen von Unternehmen mit Behörden möglicherweise zu rechtlichen Unklarheiten führen. Drittens könnten die wesentlichen Anforderungen an intelligente Verträge für die Ausführung von Datenweitergabevereinbarungen zu Rechtsunsicherheit führen. Abschließend behalten die Bestimmungen der Verordnung (EU) 2023/2854 (Datenverordnung) über den Wechsel zwischen Datenverarbeitungsdiensten ihre Bedeutung als zentraler Beitrag zu einem offeneren und wettbewerbsfähigeren Cloud-Markt. Jedoch berücksichtigten diese Bestimmungen nicht hinreichend die besondere Situation von Dienstleistungen, die wesentlich auf die Bedürfnisse des Kunden zugeschnitten sind, noch die von KMU und kleinen Midcap-Unternehmen erbrachten Leistungen. Mit den Änderungen dieses Vorschlags bleibt das Ziel erhalten, Abhängigkeiten von bestimmten Anbietern zu beseitigen, insbesondere im Hinblick auf Wechsel- und Datenextraktions-Entgelte, und den Verwaltungsaufwand für die Anbieter der oben genannten Dienste zu verringern. Somit erhöhen die Änderungen dieses Vorschlags die Rechtsklarheit und sind stark auf die allgemeinen Ziele der Verordnung (EU) 2023/2854 (Datenverordnung) abgestimmt.

Darüber hinaus sind darin die Vorschriften, welche die Konformität mit dem EU-Besitzstand im Bereich des Datenschutzes für kleine und mittlere Unternehmen (KMU) erleichtern, auf kleine Midcap-Unternehmen ausgeweitet, um kleinere Unternehmen weiter zu unterstützen.

Hinsichtlich personenbezogener Daten trat am 25. Mai 2018 die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung, DSGVO) in Kraft; sie enthält unionsweite Standards, Vorschriften und Garantien für die Verarbeitung personenbezogener Daten von Einzelpersonen, die Rechte betroffener Personen sowie einen allgemeinen Rechtsrahmen für jene, die personenbezogene Daten verarbeiten. Einerseits hielten die Interessenträger die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) im Allgemeinen für ausgewogen und solide und nach wie vor für zweckmäßig, allerdings äußerten einige Einrichtungen, insbesondere kleinere Unternehmen und Verbände mit nur wenigen, nicht intensiven und häufig risikoarmen Datenverarbeitungsvorgängen gewisse Bedenken über die Anwendung einiger Verpflichtungen aus der Verordnung. Einige dieser Bedenken lassen sich durch eine kohärentere und einheitlichere Auslegung und Durchsetzung in den Mitgliedstaaten ausräumen, aber andere Bedenken erfordern gezielte Änderungen der Rechtsvorschriften. In diesem Zusammenhang soll mit den Änderungen dieses Vorschlags den Bedenken Rechnung getragen werden und es sollen insbesondere bestimmte wichtige Begriffsbestimmungen präzisiert werden, z. B. „personenbezogene Daten“. ferner soll die Einhaltung der Vorschriften erleichtert werden, etwa durch Unterstützung der (für die Datenverarbeitung) Verantwortlichen hinsichtlich der Kriterien und Mittel zur Feststellung, ob Daten, die sich aus der Pseudonymisierung ergeben, personenbezogene Daten sind oder nicht; das gilt bezüglich Informationsanforderungen und Meldungen von Datenschutzverstößen an die Aufsichtsbehörden. Außerdem sollen diese Änderungen bestimmte Aspekte der Datenverarbeitung zur Entwicklung und zum Training von KI klären. Darüber hinaus behandeln die vorgeschlagenen Änderungen die mangelnde Klarheit über die Bedingungen für die wissenschaftliche Forschung: Sie definieren den Begriff „wissenschaftliche Forschung“ und sie stellen klar, dass die weitere Datenverarbeitung für wissenschaftliche Zwecke mit dem ursprünglichen Verarbeitungszweck vereinbar ist und dass wissenschaftliche Forschung ein berechtigtes Interesse darstellt. Ferner wird vorgeschlagen, die Ausnahmen von der Informationspflicht über die Datenverarbeitung auszuweiten. An den relevanten Punkten gibt dieser Vorschlag die Änderungen der Datenschutz-Grundverordnung gemäß der Verordnung (EU) 2018/1725 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union wieder.

Außerdem erfordert die Verbreitung von Cookies-Bannern und die diesbezügliche „Einwilligungsmüdigkeit“ eine längst überfällige regulatorische Lösung. Die zuletzt 2009 überarbeite Richtlinie 2002/58/EG (im Folgenden „Datenschutzrichtlinie für elektronische Kommunikation“) bietet einen Rahmen für den Schutz der vertraulichen Kommunikation und präzisiert die Verordnung (EU) 2016/679 (im Folgenden „Datenschutz-Grundverordnung“ oder „DSGVO“) bezüglich der Verarbeitung personenbezogener Daten in der elektronischen Kommunikation. Außerdem schreibt sie den Schutz jener Endeinrichtungen vor, die ausgenutzt werden können, um die Privatsphäre ihrer Nutzer zu verletzen und Informationen über diese Nutzer zu sammeln. Der Konsum von Inhalten und die Nutzung von Online-Diensten bilden einen wesentlichen Anteil der Nutzung von Endeinrichtungen wie Telefonen und PCs. Viele dieser Online-Dienste sind auf die Einnahmen aus Werbung angewiesen, einschließlich personalisierter Werbung. Das gilt auch für Mediendienste. Online-Diensteanbieter stützen sich auf sogenannte Cookies oder ähnliche Techniken, welche die Verarbeitungs- und Speicherfunktionen von Endeinrichtungen nutzen und so zum Beispiel auf

Informationen zugreifen, die dort gespeichert sind oder von dort ausgesendet werden. Diese Techniken dienen vielfältigen Zwecken wie dem optimierten Erbringen der Dienstleistung für die jeweilige Endeinrichtung. Sie gewährleisten die Sicherheit der Endeinrichtung und des gesamten Dienstes, aber sie dienen auch zur Verfolgung des Verhaltens von Einzelpersonen und ihrer Interaktion mit diversen Online-Diensten, um personalisierte Werbung anzubieten.

Die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) fordert die Einwilligung zum Einsatz solcher Techniken, wenn dies für die Speicherung oder für den Zugang zum alleinigen Zweck der Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz technisch nicht notwendig ist, und auch dann, wenn dies strikt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich verlangten Dienst der Informationsgesellschaft zur Verfügung zu stellen. In der Regel wird mit Pop-up-Bannern auf der Website oder in der mobilen Anwendung um eine solche Einwilligung gebeten. Derartige Banner enthalten Informationen über die Zwecke der Datenverarbeitung. Häufig geht es darin um Datenempfänger und Arten von Cookies, was für Einzelpersonen nicht immer leicht verständlich ist. Solche Banner erfüllen daher möglicherweise nicht ihr Ziel, die Einzelnen zu informieren und ihnen die Kontrolle über den Schutz ihrer Privatsphäre und die Verarbeitung ihrer personenbezogenen Daten zu geben, sondern werden von den Internetnutzern eher als Belästigung wahrgenommen. Gleichzeitig entstehen den Anbietern von Online-Diensten erhebliche Kosten für die Gestaltung rechtskonformer Banner.

Weitere Komplexität erzeugt Artikel 5 Absatz 3 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) über das Setzen von Cookies oder die Verwendung ähnlicher Techniken, um Informationen aus dem Endgerät eines Nutzers zu erhalten. Die anschließende Verarbeitung personenbezogener Daten unterliegt der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Eine Einwilligung ist zwar erforderlich, um die Kontrolle der betroffenen Personen zu gewährleisten, jedoch ist sie nicht immer die am besten geeignete Rechtsgrundlage der anschließenden Datenverarbeitung – etwa dann, wenn eine nicht als Dienst der Informationsgesellschaft eingeordnete Leistung zu erbringen ist. Das hat Rechtsunsicherheit und höhere Befolgungskosten für die Verantwortlichen verursacht, die aus Endgeräten erhaltene personenbezogene Daten verarbeiten. Darüber hinaus führte die doppelte Datenschutzregelung – nach der e-Datenschutzrichtlinie und nach der Datenschutz-Grundverordnung – dazu, dass mehrere nationale Behörden für die Überwachung der Vorschriften der beiden Rechtsrahmen zuständig sind.

Daher lautet der Vorschlag, das Zusammenwirken der geltenden Vorschriften unverzüglich zu vereinfachen. Ausschließlich die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) sollte die Verarbeitung personenbezogener Daten in und von Endeinrichtungen regeln; das umfasst auch die klar erforderliche Einwilligung zum Zugriff auf die Endeinrichtung einer natürlichen Person bei der Erhebung personenbezogener Daten. Die vorgeschlagenen Änderungen sehen auch vor, dass bei bestimmten Zwecken keine Einwilligung erforderlich sein sollte und die anschließende Datenverarbeitung als rechtmäßig zu betrachten sein sollte, was insbesondere bei nur geringem Risiko für die Rechte und Freiheiten der betroffenen Personen gilt, und wenn der Einsatz solcher Techniken zum Erbringen eines von dieser Person verlangten Dienstes erforderlich ist.

Sobald entsprechende Normen verfügbar sind, ebnet der Vorschlag schließlich den Weg für automatisierte und maschinenlesbare Angaben zu individuellen Wahlentscheidungen und die Befolgung derartiger Angaben seitens der Anbieter von Websites, mobilen und Mobiltelefon-

Anwendungen. Das baut auf der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und ihrer Änderung aus dem Jahr 2009 auf (vgl. Erwägungsgrund 66 der Richtlinie 2009/136/EG), in denen bereits angeregt wurde, die Einwilligung des Nutzers durch geeignete Einstellungen eines Browsers oder einer anderen Anwendung zu ermöglichen, sofern technisch möglich und wirksam; außerdem stützt sich der Vorschlag auf Artikel 21 Absatz 5 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) sowie auf den Vorschlag der Kommission von 2017 zu einer Verordnung über Privatsphäre und elektronische Kommunikation (COM(2017) 10), in dem es um Webbrowser-Einstellungen zum Management der Nutzerpräferenzen ging. Daraus folgt für die Kommission das Mandat, die Normungsgremien mit der Entwicklung einer Normenreihe über Folgendes zu beauftragen: die Kodierung automatisierter und maschinenlesbarer Angaben zur Präferenz und Wahl seitens der betroffenen Personen und die Übermittlung dieser Wahlentscheidungen von Browsern an Websites und von Mobiltelefon-Anwendungen an Webdienste. Sobald diese Normen verfügbar sind und nach Ablauf eines sechsmonatigen Übergangszeitraums sind die Verantwortlichen, die ihre Dienste über Websites und mobile Anwendungen erbringen, verpflichtet, diese codierten automatisierten und maschinenlesbaren Angaben zu beachten. Für Verantwortliche, die gewährleisten, dass ihre Websites oder Mobiltelefon-Anwendungen diesen Normen entsprechen, sollte eine Konformitätsvermutung gelten. Auf dieser Grundlage wird davon ausgegangen, dass für die Browser auch die betreffenden Einstellungen entwickelt werden. Die Bestimmungen sind technologieneutral formuliert, sodass auch andere Instrumente, z. B. agentische KI, die Nutzer bei ihren Einwilligungsentscheidungen unterstützen könnten, sofern sie die Anforderungen der DSGVO sicher erfüllen können. Angesichts der Bedeutung von Online-Einnahmen für den unabhängigen Journalismus als unverzichtbare Säule einer demokratischen Gesellschaft sollten Mediendiensteanbieter im Sinne der Verordnung (EU) 2024/1083 (Europäisches Medienfreiheitsgesetz) nicht verpflichtet sein, solche Signale zu beachten, und es sollte ihnen gestattet sein, die Nutzer in direkter Interaktion zu informieren und ihnen so die Einwilligungsentscheidungen zu ermöglichen.

Die vorgeschlagenen Änderungen dieser Verordnung sehen eine zentrale Anlaufstelle vor, **über die Einrichtungen ihre Meldepflichten für Vorfälle gemäß mehreren Rechtsakten erfüllen können**. Eine solche Anlaufstelle soll den Grundsatz „einmal melden, mehrfach benachrichtigen“ (*report once, share many*) fördern und damit den Verwaltungsaufwand für die Einrichtungen verringern und einen wirksamen und sicheren Informationsfluss über Sicherheitsvorfälle an die in den jeweiligen Rechtsvorschriften festgelegten Empfänger gewährleisten.

Der Vorschlag verpflichtet die ENISA dazu, die zentrale Anlaufstelle aufzubauen; gemäß der Verordnung (EU) 2024/2847 (Cyberresilienzverordnung) ist dabei die einheitliche Meldeplattform für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle zu berücksichtigen. Diese Verordnung gibt spezifische Anforderungen an das Instrument als sicheren Kanal für Informationen vor, die von den meldenden Einrichtungen zu den zuständigen Behörden gelangen. Dabei bleiben die zugrunde liegenden rechtlichen Anforderungen an die Meldung von Vorfällen unverändert, der Arbeitsablauf und die von den Einrichtungen benötigten Ressourcen werden jedoch erheblich optimiert.

Außerdem schreibt der Vorschlag die Nutzung der zentralen Anlaufstelle für einige eng miteinander verknüpfte Meldepflichten für Vorfälle gemäß folgenden Rechtsvorschriften vor: Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Verordnung (EU) 2016/679 (DSGVO), Verordnung (EU) 2022/2554 (DORA), Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) und Richtlinie (EU) 2022/2557 (CER-Richtlinie). Auch für weitere sektorspezifische Berichterstattungspflichten, wie sie im Rahmen des Netzkodex für Aspekte der

Cybersicherheit bei grenzüberschreitenden Stromflüssen (NCCS) und in den einschlägigen Instrumenten des Luftverkehrssektors festgelegt sind, wird die zentrale Anlaufstelle gelten: In den Änderungen der jeweiligen delegierten Rechtsakte und Durchführungsrechtsakte sind die Berichterstattungspflichten in diesen Rahmen vorgegeben.

Der Vorschlag zielt auch darauf ab, die gemeldeten Informationsinhalte zu straffen: Befugnisse für diverse Rechtsakte sollen eingeführt werden, sofern es noch keine gibt. Ferner wird im Vorschlag Folgendes klargestellt: Bei der Entwicklung gemeinsamer Meldevorlagen gemäß den Richtlinien (EU) 2022/2555 und 2022/2557 oder der Verordnung (EU) 2016/679 sollte die Kommission ihre Erfahrungen und die unter der Verordnung (EU) 2022/2554 (DORA) entwickelten gemeinsamen Vorlagen gebührend berücksichtigen, um Kohärenz zu gewährleisten, Synergien zu fördern und die von den Unternehmen auszufüllenden Datenfelder zu minimieren, was ihren Verwaltungsaufwand verringert.

Über diese zentrale Änderungen hinaus wird mit dem Vorschlag die Gelegenheit zur Aufhebung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (im Folgenden „Platform-to-Business-Verordnung“ oder „P2B-Verordnung“) genutzt. Diese seit dem 12. Juli 2020 geltende Verordnung war der erste Schritt hin zu einem umfassenden Rechtsrahmen für die Plattformwirtschaft. Seit ihrem Inkrafttreten sind jedoch weitere EU-Rechtsakte hinzugekommen, die Online-Vermittlungsdienste und Online-Plattformen regulieren. Hierzu zählen die Verordnungen (EU) 2022/1925 (Gesetz über digitale Märkte) und (EU) 2022/2065 (Gesetz über digitale Dienste), die die Bestimmungen der P2B-Verordnung weitgehend überholen. Ausgewählte Bestimmungen der P2B-Verordnung bleiben in Kraft, um Rechtssicherheit für Rechtsakte zu gewährleisten, die Querverweise auf diese Bestimmungen enthalten, zum Beispiel die Richtlinie (EU) 2023/2831 zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit. Im Allgemeinen wird der vereinfachte Rechtsrahmen für Online-Plattformen die wegen mehrschichtiger und sich überschneidender Vorschriften gegebenen Befolgungskosten senken, wie von den Interessenträgern gefordert. Die Anbieter von Online-Vermittlungsdiensten werden von klareren Rechtsvorschriften profitieren. Ihre Durchsetzung wird gezielter erfolgen.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Dem Vorschlag liegt ein zweiter Vorschlag zur Änderung der Verordnung (EU) 2024/1689 (KI-Verordnung) bei; zusammen bilden sie das Digital-Omnibus-Paket, das den ersten unmittelbaren Schritt zur Vereinfachung des digitalen Regelwerks darstellt. Neben dem Digital-Omnibus-Paket wird auch der Überarbeitungsvorschlag für die Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit) unter anderem das aktualisierte Mandat der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie Maßnahmen zur vereinfachten Einhaltung der Cybersicherheitsanforderungen umfassen.

Das Digital-Omnibus-Paket ist Teil einer umfassenden Strategie zur Vereinfachung der Rechtsvorschriften, wie im Digitalpaket angekündigt und im einleitenden Abschnitt dieser Begründung ausführlich dargelegt.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Der Vorschlag gehört zur Agenda der Kommission zur Vereinfachung des EU-Rechtsrahmens. Das breite Spektrum der geänderten Rechtsakte zeigt eindeutig das Potenzial für Vereinfachungen im Zusammenspiel verschiedener Vorschriften, auch wenn sie zu verschiedenen Politikbereichen gehören. Ein solcher Fall ist zum Beispiel die digitale Vereinfachung durch die Meldung von Sicherheitsvorfällen an die zentrale Anlaufstelle; sie

lässt die zugrunde liegenden regulatorischen Verpflichtungen unberührt, führt aber Cybersicherheitsvorschriften für wesentliche Einrichtungen oder für den Finanzsektor, Datenschutzvorschriften usw. in derselben Schnittstelle zusammen.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Der Vorschlag stützt sich auf die Artikel 114 und 16 des Vertrags über die Arbeitsweise der Europäischen Union, denn diese bildeten auch die Rechtsgrundlage der nun geänderten Rechtsakte. Die angemessene Rechtsgrundlage für die Bestimmungen zur Änderung der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und der Verordnung (EU) 2018/1725 ist Artikel 16 des Vertrags. Da sich alle anderen geänderten Rechtsakte auf Artikel 114 des Vertrags stützen, ist dieselbe Rechtsgrundlage auch für die entsprechenden Änderungsbestimmungen dieser Verordnung angemessen.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Die geänderten Vorschriften sind Unionsvorschriften und lassen sich daher nur auf Unionsebene ändern. Die in dieser Verordnung dargelegten technischen Anpassungen bewahren die Logik der Subsidiarität, die den geänderten Rechtsakten zugrunde liegt.

Hinsichtlich der Verordnung (EU) 2023/2854 (Datenverordnung) stärken die Änderungen das Ziel der Verordnung, Hindernisse im Binnenmarkt für die datengesteuerte Wirtschaft zu beseitigen. Hierfür werden mit den Änderungen bereits anderweitig bestehende Vorschriften in die Verordnung aufgenommen. Die gezielten Änderungen dieser Vorschriften zielen auf Vereinfachung und Klarheit ab und sollen den Verwaltungsaufwand im Privatsektor und für die nationalen Behörden verringern. Sie greifen nicht in die Zuständigkeit der Mitgliedstaaten oder der EU-Organe ein.

Gleiches gilt für die Aufhebung der Richtlinie (EU) 2019/1024 (über offene Daten): Ihre materiellrechtlichen Vorschriften gehen in die Verordnung (EU) 2023/2854 (Datenverordnung) über, ohne die den Mitgliedstaaten übertragenen Zuständigkeiten wesentlich zu ändern. Ein erheblicher Teil der Daten des öffentlichen Sektors unterliegt bereits heute der unmittelbar geltenden Durchführungsverordnung (EU) 2023/138 über hochwertige Datensätze[12]. Ihre Umwandlung in eine Verordnung wird die einheitliche Anwendung der vorgeschlagenen Änderungen in allen Mitgliedstaaten erleichtern. So unterstützt die Verordnung insbesondere öffentliche Verwaltungen, die im Besitz von Daten des öffentlichen Sektors sind, aber auch Weiterverwender solcher Daten: Sie strafft Verfahren und verringert den Verwaltungsaufwand bei der Auslegung und Umsetzung unterschiedlicher nationaler Rechtsvorschriften. Damit wird die Durchsetzung direkt anwendbarer Vorschriften wahrscheinlich kohärenter. Der Vorschlag ändert die nationalen Zugangsregelungen nicht und soll hinreichende Flexibilität für nationale Lösungen bieten – die Mitgliedstaaten unterstreichen dieses Vorrecht.

---

[12] Durchführungsverordnung (EU) 2013/138.

Bezüglich der Verordnungen (EU) 2016/679 (Datenschutz-Grundverordnung) und (EU) 2018/1725 sollen die vorgeschlagenen Änderungen Rechtsklarheit und Vorhersehbarkeit bei der Anwendung der bestehenden Vorschriften schaffen und den Verwaltungsaufwand nach Möglichkeit verringern, ohne das hohe Datenschutzniveau gemäß der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und der Verordnung (EU) 2018/1725 zu untergraben. Ebenso bleiben die Zuständigkeiten der Mitgliedstaaten und der Organe und Einrichtungen der EU unverändert.

Die Einführung der zentralen Anlaufstelle zur Meldung von Vorfällen gehört zum Vorschlag einer europaweiten Lösung mit einem einzigen Kanal, über den die Unternehmen mehrere rechtliche Meldepflichten, die im Wesentlichen dieselben Vorfälle betreffen, erfüllen können. Diese Lösung ändert in keiner Weise die Rechte und Zuständigkeiten der nationalen Behörden, solche Meldungen entgegenzunehmen. Stattdessen schafft sie mit der zentralen Anlaufstelle als benutzerfreundliche Schnittstelle Anreize zum Einreichen von Berichten und kommt außerdem mehreren rechtlichen Verpflichtungen entgegen. Da viele der betreffenden Dienstleistungen grenzüberschreitend erbracht werden und die Anbieter in mehreren Mitgliedstaaten präsent sind, ist eine europäische Lösung erforderlich.

- **Verhältnismäßigkeit**

Die technischen Änderungen des Vorschlags sind erforderlich, um die Ziele des geringeren Verwaltungsaufwands und der Rechtsklarheit zu erreichen und die zugrunde liegenden Ziele der geänderten Rechtsvorschriften zu wahren und zu optimieren. Die Änderungen sind verhältnismäßig, denn sie erlegen den Unternehmen und Behörden, wenn überhaupt, vernachlässigbare Übergangs- und Anpassungskosten auf, ermöglichen aber in den nächsten Jahren hohe Kosteneinsparungen.

Mehrere der in dieser Verordnung vorgelegten Änderungen dienen der Vereinfachung, in erster Linie durch das Schaffen von Rechtssicherheit und das Klären der Anwendung der Vorschriften – zum Beispiel Klarstellungen für Dateninhaber zum Schutz von Geschäftsgeheimnissen in der Verordnung (EU) 2023/2854 (Datenverordnung) oder zum Trainieren von KI-Modellen und KI-Systemen, die personenbezogene Daten enthalten, gemäß der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), oder zum Begriff „personenbezogene Daten“ in den Verordnungen (EU) 2016/679 und (EU) 2018/1725. Mit einigen Bestimmungen sollen Auslegungen des Gerichtshofs der Europäischen Union als Vorschriften aufgenommen werden, etwa hinsichtlich der in der Verordnung (EU) 2016/679 weiter präzisierten Pseudonymisierung personenbezogener Daten. Daher handelt es sich um sehr gezielte Änderungen der Vorschriften, und es wird eine große Wirkung auf die Rechtssicherheit für Unternehmen und Investoren erwartet.

Die in dieser Verordnung vorgeschlagenen Änderungen zielen auch darauf ab, die direkten Kosten für Unternehmen und Behörden zu senken, wobei dieselben regulatorischen Ziele unter Wahrung der Verhältnismäßigkeit der Vorschriften mit geringeren Belastungen erreichbar sind. So wird beispielsweise die in der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) vorgesehene verbindliche Regelung für Datenvermittlungsdienste in der Verordnung (EU) 2023/2854 (Datenverordnung) in eine freiwillige, vertrauensbildende Regelung umgewandelt.

Anhand der Ausweitung bestimmter für kleine und mittlere Unternehmen geltender Bestimmungen auf kleine Midcap-Unternehmen sollen die zielgerichteten Vereinfachungsmaßnahmen den Umfang dieser Verpflichtungen nur minimal ändern, aber einem breiteren Spektrum von Unternehmen mit hohem Potenzial zur Förderung der EU-

Wettbewerbsfähigkeit Rechtssicherheit bieten. Der Vorschlag beschränkt sich auf die notwendigen Änderungen, um zu gewährleisten, dass kleine Midcap-Unternehmen von demselben Rechtsrahmen profitieren wie KMU.

Die zentrale Anlaufstelle zur Meldung von Vorfällen und Datenschutzverletzungen ermöglicht Unternehmen hohe Kosteneinsparungen und geht das allgemeine Problem der unzureichenden Meldungen an. Diese Lösung ist nicht nur verhältnismäßig, sondern sie bringt auch eine wichtige Vereinfachung mit einem digitalen Instrument und unterstützt die Wirksamkeit der bestehenden Meldepflichten gegenüber der Anlaufstelle.

Die Aufhebung der Verordnung (EU) 2019/1150 (P2B-Verordnung) ist erforderlich, um Doppelregelungen zu beseitigen. Die Verordnung hat so nur noch einen geringen Restwert, und im Hinblick auf einen verhältnismäßigen Ansatz für die Regulierung von Online-Plattformen ist es notwendig, doppelte Verpflichtungen zu beseitigen.

- **Wahl des Instruments**

Aufgrund der Art der betroffenen Vorschriften werden die Änderungen als Verordnung vorgeschlagen. Bei der Änderung von Richtlinien richten sich die Bestimmungen an europäische Stellen, oder es erfolgen gezielte Änderungen, insbesondere zur Gestaltung und Weiterentwicklung von Bestimmungen zu Verordnungen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Die meisten der in diesem Vorschlag behandelten Rechtsvorschriften sind relativ neu und unterliegen einer fortlaufenden Bewertung der Ergebnisse. Die wichtigsten Feststellungen sind in der beigefügten Arbeitsunterlage der Kommissionsdienststellen zusammengefasst.

Eine Ausnahme bildet die vorläufige Überprüfung der Verordnung (EU) 2019/1150 (Platform-to-Business-Verordnung, P2B[13]) aus dem Jahr 2023. Der Bericht nannte erste positive Auswirkungen, zum Beispiel auf die vertragliche Transparenz für gewerbliche Nutzer und die ordnungsgemäße Behandlung von Beschwerden. Aus dem Bericht ging jedoch auch eine mangelnde Bewusstheit unter gewerblichen Nutzern sowie Anbietern von Online-Vermittlungsdiensten und Online-Suchmaschinen hinsichtlich ihrer jeweiligen Rechte und Pflichten gemäß der Verordnung (EU) 2019/1150 (P2B-Verordnung) hervor. Das war auch mit einer unzureichenden Einhaltung der Verordnung (EU) 2019/1150 (P2B) verbunden und führte zur mangelnden Umsetzung. Bis 2023 gingen nur sehr wenige Beschwerden gemäß der Verordnung (EU) 2019/1150 (P2B-Verordnung) ein. Im Bericht wurde der Schluss gezogen, dass „das Potenzial der Verordnung (EU) 2019/1150 (P2B) derzeit nicht voll ausgeschöpft“

[13] Arbeitsunterlage der Kommissionsdienststellen, Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die erste vorläufige Überprüfung der Durchführung der Verordnung (EU) 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten {SWD(2023) 300 final}.

wurde. Inzwischen sind die Verordnungen (EU) 2022/2065 (Gesetz über digitale Dienste) und (EU) 2022/1925 (Gesetz über digitale Märkte) vollständig in Kraft getreten und haben die Bestimmungen der Verordnung (EU) 2019/1150 (P2B-Verordnung) weitgehend überholt.

- **Konsultation der Interessenträger**

Zur Ausarbeitung des Vorschlags wurden mehrere Konsultationen durchgeführt. Diese waren als einander ergänzend konzipiert worden und befassten sich mit unterschiedlichen aktuellen Aspekten oder mit diversen Interessengruppen.

Im Frühjahr 2025 wurden drei öffentliche Konsultationen und Aufforderungen zur Stellungnahme zu den wichtigsten Säulen des Vorschlags veröffentlicht. Eine Konsultation vom 9. April bis zum 4. Juni behandelte die Strategie „KI anwenden“[14], eine weitere vom 11. April bis zum 20. Juni beschäftigte sich mit der Überarbeitung der Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit)[15] und eine dritte Konsultation vom 23. Mai bis zum 20. Juli betraf die Strategie für eine Europäische Datenunion[16]. Jeder Fragebogen enthielt einen eigenen Abschnitt (zuweilen auch mehrere) über Belange der Umsetzung und Vereinfachung in direktem Zusammenhang mit den Überlegungen zum Digital-Omnibus-Paket. Im Rahmen dieser ersten Konsultation gingen insgesamt 718 Einzelantworten ein.

Ferner wurde vom 16. September bis zum 14. Oktober 2025 eine Aufforderung zur Stellungnahme zum Digital-Omnibus-Paket veröffentlicht[17]. Damit sollten die Interessenträger die Möglichkeit erhalten, zu einem konsolidierten Vorschlag über den Anwendungsbereich des Digital-Omnibus-Pakets Stellung zu nehmen. Von diversen Interessengruppen gingen 513 Antworten ein, nicht zuletzt von Unternehmen und Unternehmensverbänden, der Zivilgesellschaft, Wissenschaftlern, Behörden sowie individuelle Beiträge von Bürgerinnen und Bürgern.

Exekutiv-Vizepräsidentin Henna Virkkunen veranstaltete zwei Umsetzungsdialoge über die wichtigsten Themen des Digital-Omnibus-Pakets: den ersten Dialog über die Datenpolitik[18] (1. Juli 2025) und den zweiten Dialog über die Cybersicherheitspolitik[19] (15. September).

Kommissionsmitglied McGrath veranstaltete am 16. Juli 2025 einen Umsetzungsdialog über die Anwendung der DSGVO.

Außerdem führten die Kommissionsdienststellen mehrere „Realitätschecks“ durch: Vom 15. September bis zum 6. Oktober 2025 wurden in Fokusgruppen mit Unternehmen und

---

14 Europäische Kommission (2025), Call for evidence on the Apply AI Strategy. Abrufbar unter: Strategie „KI anwenden“ – Stärkung des KI-Kontinents.

15 Europäische Kommission (2025), Call for evidence on the revision of the Cybersecurity Act. Abrufbar unter: Der EU-Rechtsakt zur Cybersicherheit.

16 Europäische Kommission (2025), Call for evidence on the European Data Union Strategy. Abrufbar unter: Strategie für eine europäische Datenunion.

17 Europäische Kommission (2025), Aufforderung zur Stellungnahme – Omnibusvorschriften für den Digitalbereich. Abrufbar unter: Vereinfachung – Digitalpaket und -omnibus.

18 Europäische Kommission (2025), Implementation dialogue – data policy. Abrufbar unter: Umsetzungsdialog – Datenpolitik – Europäische Kommission.

19 Europäische Kommission (2025), Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen. Abrufbar unter: Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen - Europäische Kommission.

Vertretern der Zivilgesellschaft die praktischen Herausforderungen der Umsetzung erörtert und die Befolgungskosten abgeschätzt.

Um insbesondere kleine und mittlere Unternehmen (KMU) zu befragen und ihre Rückmeldungen einzuholen, fand vom 4. September bis zum 16. Oktober 2025 ein spezielles KMU-Panel über das Enterprise Europe Network (EEN)[20] statt.

Abschließend erhielten die Kommissionsdienststellen zahlreiche Positionspapiere und veranstalteten bilaterale Treffen mit einer Vielzahl von Interessenträgern. Außerdem arbeiteten die Dienststellen der Kommission mit den Mitgliedstaaten an Gesprächen am Runden Tisch oder im Kontext diverser Arbeitsgruppen des Rates zusammen.

Insgesamt stimmten die Rückmeldungen der Interessenträger hinsichtlich der notwendigen vereinfachten Anwendung einiger digitaler Vorschriften überein. Die Interessenträger begrüßten den Schwerpunkt auf der Kohärenz und Konsolidierung der Vorschriften und auf der Optimierung der Befolgungskosten.

Es wurde eindeutig gefordert, den Besitzstand im Bereich des Datenschutzes zu straffen und die Vorschriften zu konsolidieren. Der Vorschlag behandelt diesen Punkt neben gezielten, von den Interessenträgern unterstützten Änderungen, unter anderem hinsichtlich der Datenschutz-Grundverordnung und der Ermüdung aufgrund der Cookie-Banner. Darüber hinaus wiesen Unternehmen auf weitere Bewertungen des Zusammenspiels zwischen den Datenvorschriften hin, die eine eingehendere Analyse anhand der Instrumente für eine bessere Rechtsetzung rechtfertigen – insbesondere die bevorstehende digitale Eignungsprüfung.

Unternehmen aus verschiedenen Sektoren wiesen auch auf die ungerechtfertigten Belastungen hin, die sich aus der doppelten Meldung von Vorfällen in mehreren Rechtsrahmen ergeben. Mit dem Vorschlag einer zentralen Anlaufstelle zur Meldung von Vorfällen wird auf diesen Handlungsaufruf eingegangen.

Hinsichtlich der Verordnung über künstliche Intelligenz wiesen die Interessenträger auf die notwendige Rechtssicherheit bei der Anwendung der Vorschriften hin und betonten insbesondere, dass vor der Anwendung der Vorschriften verfügbare Standards und Leitlinien erforderlich sind. Mit dem gesonderte Regulierungsvorschlag im Rahmen des Digital-Omnibus-Pakets wird auf ihre Bedenken eingegangen.

Schließlich äußerten sich die Interessenträger nicht zu den Auswirkungen der P2B-Verordnung; sie bestätigten aber die Ergebnisse des Zwischenbewertungsberichts, nach dem die Vorschriften weder bekannt sind noch ihre Ziele wirksam erreichen. Mit dieser Verordnung wird eine Aufhebung der Vorschriften für die Beziehungen zwischen Plattformen und Unternehmen vorgeschlagen, insbesondere angesichts ihrer Überschneidung mit aktuelleren Vorschriften.

Ein detaillierter Überblick über diese Konsultationen der Interessenträger und ihre Berücksichtigung im Vorschlag ist der Arbeitsunterlage der Kommissionsdienststellen zur Unterstützung des Digital-Omnibus-Pakets zu entnehmen.

---

[20] Das EEN ist das weltweit größte Unterstützungsnetz für kleine und mittlere Unternehmen; die Europäische Exekutivagentur für den Innovationsrat und für KMU der Europäischen Kommission betreut dieses Netz.

- **Einholung und Nutzung von Expertenwissen**

Zusätzlich zu den oben dargelegten Konsultationen stützte sich die Kommission für diesen Vorschlags hauptsächlich auf interne Analysen. Außerdem wurden zwei unterstützende Studien zur Analyse der Datenkapitel des Vorschlags in Auftrag gegeben. Die erste Studie konzentrierte sich auf die Umsetzung der Verordnung (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten), der Richtlinie (EU) 2019/1024 (über offene Daten) und der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt). Die zweite Studie ist enger mit der Mitteilung über die Strategie für die Datenunion verknüpft (zusammen mit dem Digital-Omnibus-Vorschlag im gleichen Vereinfachungspaket angenommen). Sie konzentrierte sich auf datenpolitische Entwicklungen im Zusammenhang mit generativer KI, die Einhaltung von Rechtsvorschriften und die internationalen Dimensionen. Beide Studien werden derzeit fertiggestellt und zu einem späteren Zeitpunkt veröffentlicht.

Die Dienststellen der Kommission haben auch eine Studie über das Zusammenspiel der Verordnung (EU) 2022/2065 (Gesetz über digitale Dienste) mit anderen Rechtsakten durchgeführt, unter anderem mit der Verordnung (EU) 2019/1150 (P2B-Verordnung). Als Teil des Digitalpakets veröffentlichte die Kommission den Bericht, der gemäß der Anforderung in Artikel 91 der Verordnung (EU) 2022/2065 (Gesetz über digitale Dienste) das Zusammenspiel derselben Verordnung (EU) 2022/2065 mit verwandten Vorschriften beschreibt.

- **Folgenabschätzung**

Die in dieser Verordnung vorgeschlagenen Änderungen sind zielgerichtet und technischer Art. Sie sollen eine effizientere Durchführung der Vorschriften gewährleisten. Diese Änderungen neigen nicht zu mehreren politischen Optionen, die sich sinnvoll testen und vergleichen ließen, und werden daher im Einklang mit den Leitlinien für eine bessere Rechtsetzung nicht durch eine vollständige Folgenabschätzung diese Änderungen untermauert.

In der beigefügten Arbeitsunterlage der Kommissionsdienststellen wird ausführlich auf die Interventionslogik der Änderungen und auf die Ansichten der Interessenträger über die diversen Maßnahmen eingegangen und es wird die Kosten-Nutzen-Analyse der Vorschläge vorgelegt, einschließlich der erzielten Kosteneinsparungen und anderer Auswirkungen. Vielfach baut diese Unterlage auf den jeweiligen, ursprünglich für die verschiedenen Rechtsakte vorgenommenen Folgenabschätzungen auf.

- **Effizienz der Rechtsetzung und Vereinfachung**

Die vorgeschlagene Verordnung verringert den Verwaltungsaufwand für Unternehmen, öffentliche Verwaltungen und Bürger sehr deutlich. Erste Schätzungen ergeben mögliche Einsparungen von jährlich mindestens 1 Mrd. EUR ab Inkrafttreten sowie zusätzliche Einsparungen von 1 Mrd. EUR bei einmaligen Kosten; über drei Jahre, bis 2029, ergibt das insgesamt mindestens 5 Mrd. EUR. Es werden auch umfangreiche nicht quantifizierbare Vorteile erwartet, insbesondere aufgrund des gestrafften Regelwerks, das ihre Beachtung und Einhaltung erleichtern wird. Die Berechnungen lassen auch die vom vorgeschlagenen Regulierungsansatz hervorgebrachten Geschäftsmöglichkeiten unberücksichtigt.

Eine Reihe von Bestimmungen in den mit dem Digital-Omnibus-Paket geänderten Rechtsakten enthalten bereits Ausnahmen für kleine und mittlere Unternehmen (KMU); im Bereich des Cloud-Wechsels werden aber weitere Unterstützungsmaßnahmen vorgeschlagen.

Im Kapitel über die harmonisierten Vorschriften für den Datenaustausch werden einige, den KMU bereits gewährte Ausnahmen auf kleine Midcap-Unternehmen ausgeweitet.

Außerdem steht der Vorschlag voll und ganz im Einklang mit dem „Digitalcheck“ der Kommission, der eine angemessene Abstimmung der politischen Vorschläge auf das digitale Umfeld gewährleisten soll. Weitere Einzelheiten hierzu sind Kapitel 4 des beigefügten Finanz- und Digitalbogen zu Rechtsakten zu entnehmen.

- **Grundrechte**

Die vorgeschlagenen Änderungen unterstützen die Innovationsmöglichkeiten für Unternehmen im Binnenmarkt und fördern somit das Grundrecht auf unternehmerische Freiheit in der Union.

Einige Bestimmungen beziehen sich auch auf den Schutz und die Förderung anderer Grundrechte, insbesondere auf das Recht auf Privatsphäre und den Schutz personenbezogener Daten; so sind diese Bestimmungen so eingerichtet, dass ein Höchstmaß an Schutz gewahrt bleibt, Einzelpersonen Unterstützung zur wirksamen Ausübung ihrer Rechte erhalten, ferner sollen sie die Kosten optimieren und weitere Innovationsmöglichkeiten schaffen. Damit folgt der Vorschlag strikt dem in Artikel 52 der Charta verankerten Grundsatz der Verhältnismäßigkeit.

Im besonderen Fall der Verordnungen (EU) 2016/679 (Datenschutz-Grundverordnung) und (EU) 2018/1725 würden die vorgeschlagenen zielgerichteten Änderungen die Anforderungen an Verarbeitungen mit geringem Risiko vereinfachen, bestimmte Normen harmonisieren und wichtige Konzepte dieser Verordnungen (EU) 2016/679 und (EU) 2018/1725 präzisieren, die den Verantwortlichen die Einführung wirksamerer Datenschutzstrategien ermöglichen. So könnten die Verantwortlichen ihre Ressourcen auf datenintensive und riskante Tätigkeiten konzentrieren, wo die Maßnahmen zum Schutz personenbezogener Daten am kritischsten sind.

In Bezug auf den Schutz der Privatsphäre in der Kommunikation wahrt der Vorschlag ein Höchstmaß an Schutz, einschließlich des auf Einwilligung gegründeten Zugangs zu Endeinrichtungen. Die Änderung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ändert nichts am umfassenden Schutz. Die Vorschriften für die Verarbeitung personenbezogener Daten in und von Endeinrichtungen werden an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) angeglichen. Hinsichtlich der Verarbeitung nicht-personenbezogener Daten bleiben die Vorschriften über die Integrität der Endeinrichtungen gemäß der Richtlinie bestehen.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Auswirkungen der Einrichtung und Aufrechterhaltung der zentralen Anlaufstelle zur Meldung von Vorfällen seitens der Agentur der Europäischen Union für Cybersicherheit (ENISA) auf den Haushalt sind in der Überarbeitung der Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit) unter den Ressourcen für die ENISA im Einzelnen dargelegt.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

NICHT ZUTREFFEND

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Änderung der Verordnung (EU) 2023/2854 (Datenverordnung)

Die Bestimmungen der Verordnungen (EU) 2018/1807 (über den freien Datenverkehr), (EU) 2022/868 (Daten-Governance-Rechtsakt) und der Richtlinie (EU) 2019/1024 (über offene Daten) werden im geänderten Rechtsrahmen über Daten in robust gestraffter Weise in der Verordnung (EU) 2023/2854 (Datenverordnung) konsolidiert. Kapitel I enthält auch gezielte Änderungen zur Anpassung der geltenden Vorschriften der Verordnung (EU) 2023/2854 (Datenverordnung).

Artikel 1 enthält Änderungen der Verordnung (EU) 2023/2854 (Datenverordnung) über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828.

In Artikel 1:

In Nummer 1 wird der Anwendungsbereich der Verordnung (EU) 2023/2854 (Datenverordnung) aktualisiert, zudem werden, wie nachfolgend erläutert, neue Kapitel darin eingefügt.

In Nummer 2 werden Begriffsbestimmungen geändert und neue Bestimmungen eingefügt.

In Nummer 3 wird eine neue Vorschrift nach Artikel 4 Absatz 8 der Verordnung (EU) 2023/2854 (Datenverordnung) eingeführt, die es Dateninhabern gestattet, einem Nutzer die Offenlegung von Geschäftsgeheimnissen zu verweigern, wenn ein hohes Risiko des rechtswidrigen Erwerbs oder der rechtswidrigen Nutzung oder Offenlegung gegenüber Drittländern oder unter ihrer Kontrolle stehenden Unternehmen vorliegt, die Rechtsordnungen mit einem schwächeren Schutz als in der Union unterliegen.

In Nummer 5 wird dieselbe Vorschrift für Artikel 5 Absatz 11 der Verordnung (EU) 2023/2854 (Datenverordnung) bezüglich Dateninhabern eingeführt, die Geschäftsgeheimnisse gegenüber Dritten offenlegen.

In den Nummern 5 bis 19 wird der Anwendungsbereich von Kapitel V von „außergewöhnlicher Notwendigkeit“ auf „öffentliche Notstände“ beschränkt. Ferner werden die Artikel 14 und 15 gestrichen, und der neue Artikel 15a wird zum einzigen Artikel für Verlangen bei öffentlichen Notfällen im Rahmen der B2G-Regelung der Verordnung (EU) 2023/2854 (Datenverordnung). Ein Verlangen ist demnach möglich, wenn es zur Bewältigung eines öffentlichen Notstands (Artikel 15a Absatz 2) oder zur Abmilderung der Lage oder zur Unterstützung der Erholung von einem öffentlichen Notstand (Artikel 15a Absatz 3) erforderlich ist. Querverweise werden entsprechend angepasst und ihr Wortlaut wird vereinfacht und präzisiert. In Artikel 1 Nummer 21 wird ein neuer Artikel 22a eingeführt, welcher die Beschwerderegelungen in Kapitel V enthält und vormals wiederholte Bestimmungen zusammenfasst.

Die Nummern 20 bis 22 enthalten bestimmte Ausnahmen von Kapitel VI der Verordnung (EU) 2023/2854 (Datenverordnung) (Wechsel zwischen Datenverarbeitungsdiensten): In Artikel 31 wird eine weniger strenge Sonderregelung für maßgeschneiderte Datenverarbeitungsdienste eingeführt, die nicht handelsüblich sind und ohne vorherige Anpassung an die Bedürfnisse und das Ökosystem des Nutzers nicht funktionieren würden. Das gilt, sofern sich die Leistungen auf vor dem 12. September 2025 abgeschlossene Verträge

gründen. In ähnlicher Weise wird in Artikel 31 eine neue, weniger strenge Sonderregelung für Datenverarbeitungsdienste eingeführt, die KMU und kleine Midcap-Unternehmen anhand von vor dem 12. September 2025 abgeschlossenen Verträgen erbringen, und es wird klargestellt, dass diese Anbieter Vertragsstrafen für vorzeitige Kündigung in befristete Verträge aufnehmen können.

Die Nummern 23 bis 25 enthalten Änderungen in Artikel 32 der Verordnung (EU) 2023/2854 (Datenverordnung), die sich aus der Einbeziehung von Stellen ergeben, die derzeit unter die Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) fallen, in die Verordnung (EU) 2023/2854.

Nummer 26 bezweckt die Aufhebung der Verpflichtungen der Anbieter intelligenter Verträge, die grundlegenden Anforderungen zu erfüllen, und überträgt der Kommission die Befugnis, harmonisierte Normen anzunehmen.

Nummer 27 umfasst zwei derzeit noch in der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) enthaltene rechtliche Regelungen; diese Verordnung wird aufgehoben, sobald die Digital-Omnibus-Verordnung in Kraft tritt. Darin werden die gegenwärtigen Vorschriften der Kapitel III und IV des Daten-Governance-Rechtsaktes reformiert; diese Vorschriften enthalten eine obligatorische Registrierungsregelung für Anbieter von Datenvermittlungsdiensten und eine freiwillige Registrierungsregelung für datenaltruistische Organisationen. Diese beiden Regelungen werden als neues Kapitel VIIa in die Verordnung (EU) 2023/2854 (Datenverordnung) eingefügt. Angesichts des neu entstehenden Marktes für Datenvermittlungsdienste werden die Verpflichtungen der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) flexibler gestaltet, damit dieser Markt wachsen kann: Erstens wird die Regelung für Anbieter von Datenvermittlungsdiensten in eine freiwillige Regelung umgewandelt. Zweitens wird die Verpflichtung, Datenvermittlungsdienste rechtlich von allen anderen Diensten zu trennen, die ein Unternehmen anbieten möchte – die kritischste Verpflichtung –, durch eine Verpflichtung ersetzt, die Dienste funktional getrennt zu halten und mit zusätzlichen Bedingungen zu versehen. Abschließend wird die Liste der Verpflichtungen drastisch gekürzt. Für datenaltruistische Organisationen werden die Berichterstattungs- und Transparenzpflichten aufgehoben – ebenso wird die Idee aufgegeben, die Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) in einem „Datenaltruismus-Regelwerk“ durch noch detailliertere Vorschriften zu ergänzen.

Das neue Kapitel VIIb fügt das Verbot von Datenlokalisierungsauflagen für nicht-personenbezogene Daten in der Union in die Verordnung (EU) 2023/2854 (Datenverordnung) ein; vorher war dieses Verbot in der aufzuhebenden Verordnung (EU) 2018/1807 (über den freien Verkehr nicht-personenbezogener Daten) enthalten. Die Verpflichtung zur Mitteilung an die Kommission bleibt bestehen, jedoch wird die nationale einheitliche Online-Informationsstelle abgeschafft, bei der die Mitgliedstaaten die geltenden Datenlokalisierungsauflagen veröffentlichen sollten.

In den Nummern 4 und 33 bis 58 werden die zusammengelegten Bestimmungen über die Weiterverwendung von Daten und Dokumenten im Besitz öffentlicher Stellen gemäß Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) und der Richtlinie (EU) 2019/1024 (Richtlinie über offene Daten) eingeführt:

- In Nummer 4 werden in die Verordnung (EU) 2023/2854 (Datenverordnung) aufgenommene Begriffsbestimmungen eingeführt, mit denen die Definitionen von

Daten und Dokumenten mittels einer strengen Abgrenzung zwischen digitalen Inhalten (Daten) und nicht digitalen Inhalten (Dokumenten) harmonisiert werden.

- Darin wird das neue Kapitel VIIc über die Weiterverwendung von Daten und Dokumenten im Besitz öffentlicher Stellen eingeführt.
- In einem neu eingefügten Abschnitt 1 werden die allgemeinen Grundsätze des neu eingefügten Kapitels dargelegt.
- Gegenstand und Anwendungsbereich des vereinten Kapitels werden dort eingeführt: Es ist eine Kombination der gemeinsamen Vorschriften des Kapitels II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) und der Richtlinie (EU) 2019/1024 (über offene Daten).
- In diesem Kapitel wird der gemeinsame Grundsatz der Nichtdiskriminierung festgelegt, er gilt für die gemeinsame Nutzung offener staatlicher Daten und für bestimmte Kategorien geschützter Daten.
- Es enthält das Verbot von Ausschließlichkeitsvereinbarungen – dieses ist der Regelung für offene staatliche Daten und bestimmten Kategorien geschützter Daten gemeinsam.
- Außerdem führt es allgemeine Grundsätze über die Abgeltung der Weiterverwendung offener staatlicher Daten oder bestimmter Kategorien geschützter Daten ein. Nach der neuen Regel müssen öffentliche Stellen sicherstellen, dass alle Entgelte oder Gebühren auch online über weithin verfügbare grenzüberschreitende Zahlungsdienste entrichtet werden können, ohne die Weiterverwendung offener staatlicher Daten zu diskriminieren. Das erweitert eine Vorschrift, die sich zuvor nur auf die Weiterverwendung geschützter Daten bestimmter Kategorien gemäß Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) bezog.
- So gewährt die erweiterte Vorschrift den Weiterverwendern offener staatlicher Daten und geschützter Daten bestimmter Kategorien das Recht auf Informationen über die verfügbaren Rechtsbehelfe bezüglich Entscheidungen oder Praktiken, die sie betreffen.
- Ein Abschnitt über die Vorschriften für die Weiterverwendung offener staatlicher Daten wird eingefügt – dabei handelt es sich um die ehemaligen Vorschriften der Richtlinie (EU) 2019/1024 (Richtlinie über offene Daten).
- Der Anwendungsbereich des Abschnitts wird festgelegt: Das allgemeine Kapitel über die Weiterverwendung von Daten und Dokumenten, die sich im Besitz öffentlicher Stellen befinden, bestimmt auch die Nichtanwendung auf geschützte Daten bestimmter Kategorien.
- Darin wird der allgemeine Grundsatz über die Weiterverwendung offener staatlicher Daten festgelegt.
- Der Abschnitt enthält die Vorschriften über die Bearbeitung von Anträgen auf Weiterverwendung offener staatlicher Daten, samt der eingefügten früheren Bestimmung der Richtlinie (EU) 2019/1024 (über offene Daten).
- Darin werden die Vorschriften über verfügbare Formate zur Weiterverwendung offener staatlicher Daten eingeführt, die zuvor in der Richtlinie (EU) 2019/1024 (über offene Daten) enthalten waren.

- Vorschriften über die Erhebung von Gebühren für offene staatliche Daten werden dort ebenfalls eingeführt; zuvor waren diese Fragen in der Richtlinie (EU) 2019/1024 (über offene Daten) geregelt. Nach dieser neuen Regel können öffentliche Stellen für die Weiterverwendung seitens sehr großer Unternehmen höhere Gebühren erheben. Derartige Gebühren müssen verhältnismäßig sein und ihre Höhe muss auf objektiven Kriterien beruhen.
- In diesen Abschnitten werden die Vorschriften über Standardlizenzen für die Weiterverwendung offener staatlicher Daten eingeführt, die zuvor in der Richtlinie (EU) 2019/1024 (über offene Daten) enthalten waren. Nach der neuen Regel können öffentliche Stellen besondere Bedingungen für sehr große Unternehmen vorsehen. Derartige Bedingungen müssen verhältnismäßig sein und auf objektiven Kriterien beruhen.
- Hier werden die Vorschriften über praktische Vorkehrungen eingeführt, die vorher in der Richtlinie (EU) 2019/1024 (über offene Daten) enthalten waren, um gemäß der Verordnung (EU) 2023/2854 (Datenverordnung) die Suche nach Daten oder Dokumenten, die zur Weiterverwendung zur Verfügung stehen, zu erleichtern.
- In diesen Abschnitten werden die Vorschriften über Forschungsdaten eingeführt, die zuvor in der Richtlinie (EU) 2019/1024 (über offene Daten) und in der Verordnung (EU) 2023/2854 (Datenverordnung) enthalten waren.
- Ferner werden die Vorschriften für hochwertige Datensätze eingeführt, die zuvor in der Richtlinie (EU) 2019/1024 (über offene Daten) in der Verordnung (EU) 20232854 (Datenverordnung) enthalten waren.
- Ein neuer Abschnitt über die Weiterverwendung geschützter Daten bestimmter Kategorien enthält ein Kapitel mit den früheren Vorschriften aus Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt). Hier wird der Anwendungsbereich dieses dritten Abschnitts dargelegt: Ausgenommen sind jene Daten und Dokumente, die unter Abschnitt zwei über die Regelung für die Weiterverwendung offener staatlicher Daten fallen. Weitere Dokumente werden in einer neuen Regel in den Anwendungsbereich dieses Abschnitts aufgenommen.
- Darin wird der allgemeinen Grundsatz über die Weiterverwendung bestimmter Kategorien geschützter Daten ausgeführt. Es handelt sich um den in Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) festgelegten Grundsatz, dass der Abschnitt die öffentlichen Stellen nicht dazu verpflichtet, die Weiterverwendung geschützter Daten zu gestatten, vielmehr legt er Mindestbedingungen für den Fall fest, dass öffentliche Stellen beschließen, solche Daten zur Weiterverwendung bereitzustellen.
- Dadurch werden in vereinfachter und gestraffter Form die Vorschriften über die Bedingungen der Weiterverwendung geschützter Daten bestimmter Kategorien eingeführt, die vorher in Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) vorlagen. Das umfasst eine Klarstellung, welche Vorschriften für anonymisierte personenbezogene Daten gelten. Die Anforderungen an die Übertragung nicht-personenbezogener Daten in Drittländer bleiben erhalten, sind jedoch in einen neuen Artikel unter Nummer 54 aufgeteilt.
- Im eingangs genannten Artikel werden die Vorschriften über die Erhebung von Gebühren, die früher zu Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) gehörten, in die Verordnung (EU) 2023/2854

(Datenverordnung) aufgenommen. Nach der neuen Regel können öffentliche Stellen höhere Gebühren für die Weiterverwendung durch sehr große Unternehmen vorsehen. Diese Gebühren müssen verhältnismäßig sein und auf objektiven Kriterien beruhen. Die besondere Erwägung zugunsten von Anreizen für die Weiterverwendung durch kleine und mittlere Unternehmen (KMU) wird auf kleine Midcap-Unternehmen ausgeweitet.

- Ferner gehen die Vorschriften über die zuständigen Stellen, die früher zu Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) gehörten, in die Verordnung (EU) 2023/2854 (Datenverordnung) über. Die zuständigen Stellen sollen öffentliche Stellen bei der Bearbeitung von Anträgen auf Weiterverwendung von Daten und Dokumenten gemäß Abschnitt 3 unterstützen.
- Außerdem werden die Vorschriften über die zentrale Informationsstelle, die früher zu Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) gehörten, in die Verordnung (EU) 2023/2854 (Datenverordnung) aufgenommen. Zentrale Informationsstellen sollen Weiterverwendern helfen, Informationen über die Weiterverwendung bestimmter Kategorien geschützter Daten einfach zu finden.
- Nach dem genannten Artikel gehen die Verfahrensregelungen für Anträge auf Weiterverwendung geschützter Daten bestimmter Kategorien, die zuvor in Kapitel II der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt) geregelt waren, in die Verordnung (EU) 2023/2854 (Datenverordnung) über.

Absatz 57 enthält die grundlegenden Vorschriften über den Europäischen Dateninnovationsrat (EDIB) – diese Gruppe berät die Kommission bei der einheitlichen Durchsetzung der Datenverordnung und dient als Koordinierungsforum für die Politikgestaltung in der Datenwirtschaft. Demgemäß werden die Grundregeln in die Datenverordnung integriert. Diese Änderungen ermöglichen es der Kommission, die relevanten Gründungsdokumente des EDIB zu ändern (Beschluss der Kommission vom 20. Februar 2023 – C(2023) 1074 final) und die Mitgliedschaft über die zuständigen Behörden hinaus auf Vertreter der nationalen Politikgestaltung zu erweitern.

Die Nummern 61 bis 65 enthalten Änderungen der Verordnung (EU) 2023/2854 (Datenverordnung) über das Ausschussverfahren und die Übertragung von Befugnissen; Nummer 66 enthält Änderungen der Verordnung (EU) 2022/868 (Daten-Governance-Rechtsakt), die erforderlich sind, um die Vorschriften derselben Verordnung (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (über offene Daten) in die Verordnung (EU) 2023/2854 (Datenverordnung) aufzunehmen.

In Nummer 68 wird das besondere Augenmerk auf die KMU im Kontext der Bewertung auf kleine Midcap-Unternehmen erweitert; Nummer 69 führt die Bewertung der neu in die Verordnung (EU) 2023/2854 (Datenverordnung) aufgenommenen Vorschriften ein.

Mit **Artikel 2** werden die einschlägigen Verweise auf Datenvermittlungsdienste und Datenaltruismus im Anhang bezüglich der „Gründung, Erneuerung und Schließung eines Unternehmens“ in die Verordnung (EU) 2018/1724 aufgenommen.

Änderungen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie 2002/58/EG

Mit Artikel 3 des Vorschlags würden gezielte Änderungen der Verordnung (EU) 2016/679 („Datenschutz-Grundverordnung“) eingeführt.

In Artikel 3:

In Nummer 1 würde die Definition des Begriffs „personenbezogene Daten“ nach Artikel 4 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) präzisiert: Demnach gelten in einer bestimmten Einrichtung Informationen dann nicht als personenbezogene Daten, wenn sie nach vernünftigem Ermessen nicht zur Identifizierung der natürlichen Person, auf die sie sich beziehen, dienen können. Folglich fiele eine solche Einrichtung grundsätzlich nicht in den Anwendungsbereich der genannten Verordnung.

Absatz 2 sähe zwei zusätzliche Ausnahmen von der Verarbeitung besonderer Datenkategorien vor: Eine Ausnahme vom allgemeinen Verbot der Verarbeitung biometrischer Daten wäre gegeben, sofern die Verarbeitung zur Bestätigung der Identität der betroffenen Person erforderlich ist und wenn die Daten und Mittel für eine solche Überprüfung der alleinigen Kontrolle dieser Person unterliegen. Eine weitere Ausnahme bestünde demnach für die restliche Verarbeitung besonderer Kategorien personenbezogener Daten für die Entwicklung und den Betrieb eines KI-Systems oder KI-Modells unter bestimmten Bedingungen, darunter geeignete organisatorische und technische Maßnahmen, um die Erhebung besonderer Kategorien personenbezogener Daten und die Entfernung solcher Daten zu vermeiden.

Nummer 3 würde die Situation nach Artikel 12 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) klären: Darin geht es um betroffene Personen, die das Auskunftsrecht für andere Zwecke als den Schutz ihrer personenbezogenen Daten missbrauchen. Demnach könnte der Verantwortliche sich weigern, der Aufforderung nachzukommen, oder eine angemessene Gebühr erheben. Darüber hinaus wären im genannten Absatz die Bedingungen für den Nachweis geklärt, dass ein Zugangsantrag exzessiv war.

Nummer 4 würde sich auf die Verpflichtung der Verantwortlichen konzentrieren, die betroffenen Personen gemäß Artikel 13 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) über die Verarbeitung ihrer personenbezogenen Daten zu unterrichten; darin wäre diese Verpflichtung dann aufgehoben, wenn hinreichende Gründe für die Annahme bestehen, dass die betroffene Person bereits über die Informationen verfügt, es sei denn, der Verantwortliche übermittelt die Daten an andere Empfänger oder Empfänger-Kategorien oder an ein Drittland, führt eine automatisierte Entscheidungsfindung durch oder die Verarbeitung birgt wahrscheinlich ein hohes Risiko für die Rechte der betroffenen Person.

In Nummer 5 wären die Anforderungen an die automatisierte Entscheidungsfindung im Einzelfall gemäß Artikel 22 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) bei Abschluss oder Ausführung eines Vertrags der betroffenen Person mit einem Verantwortlichen klargestellt; insbesondere wäre darin geklärt, dass die „Erforderlichkeit“ unabhängig davon gilt, ob die Entscheidung nur mit automatisierten Mitteln oder auch auf andere Weise getroffen werden könnte.

Nummer 6 würde die Verpflichtung des Verantwortlichen zur Meldung von Datenschutzverletzungen an die zuständige Aufsichtsbehörde gemäß Artikel 33 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) mit seiner Verpflichtung zur diesbezüglichen Meldung an die betroffenen Personen in Einklang bringen: Demnach wäre die Meldung nur dann erforderlich, wenn eine Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte der betroffenen Person darstellt. Außerdem wäre die Meldefrist auf 96 Stunden verlängert. Ferner wird vorgeschlagen, dass die Verantwortlichen die zentrale Anlaufstelle zur Meldung von Datenschutzverletzungen an die Datenschutzbehörde nutzen sollen. Darüber hinaus wäre der Europäische Datenschutzausschuss verpflichtet, einen Vorschlag eines gemeinsamen Musters für die Meldung von Datenschutzverletzungen auszuarbeiten und der Kommission vorzulegen, die nach einer Überprüfung, falls nötig, befugt wäre, das Muster mittels eines Durchführungsrechtsaktes anzunehmen.

In Nummer 7 wären die Listen der Verarbeitungstätigkeiten, die eine Datenschutz-Folgenabschätzung erfordern oder nicht erfordern, harmonisiert: Er enthält eine einzige Liste der Verarbeitungstätigkeiten beider Arten auf EU-Ebene und trägt somit zur Harmonisierung des Begriffs „hohes Risiko“ bei. Der Europäische Datenschutzausschuss wäre verpflichtet, Vorschläge für solche Listen auszuarbeiten. Außerdem wäre der Ausschuss verpflichtet, einen Vorschlag eines gemeinsamen Musters und einer gemeinsame Methodik für die Durchführung von Datenschutz-Folgenabschätzungen auszuarbeiten; nach einer Überprüfung, falls nötig, wäre die Kommission befugt, den Vorschlag mittels eines Durchführungsrechtsaktes anzunehmen.

In Nummer 8 wird festgelegt, dass die Kommission gemeinsam mit dem Europäischen Datenschutzausschuss die Verantwortlichen bei der Beurteilung, ob sich aus der Pseudonymisierung ergebende Daten personenbezogen sind, unterstützen kann; sie kann die für eine solche Beurteilung relevanten Mittel und Kriterien festlegen, einschließlich des Stands der verfügbaren Techniken und Kriterien zur Bewertung des Risikos einer erneuten Identifizierung...

In Absatz 12 wird die rechtliche Regelung der Verarbeitung personenbezogener Daten in oder von Endeinrichtungen („vernetzte Geräte“) reformiert, die gegenwärtig zur Richtlinie 2002/58/EG (e-Datenschutzrichtlinie) gehört. Ein in die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) eingefügter neuer Artikel 88a legt die Einwilligungspflicht für die Speicherung von oder den Zugriff auf personenbezogene Daten in Endeinrichtungen natürlicher Personen fest; ferner überträgt dieser Artikel die Verarbeitung personenbezogener Daten in und von Endeinrichtungen in den Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Ein neuer Artikel 88b der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) betrifft automatisierte und maschinenlesbare Angaben zu individuellen Wahlentscheidungen und die Befolgung dieser Angaben seitens der Website-Anbieter, sobald Normen verfügbar sind.

In Artikel 4:

In Artikel 4 des Vorschlags würden gezielte Änderungen der Verordnung (EU) 2018/1725 eingeführt, um ihren Wortlaut an die in Artikel 3 eingeführten Änderungen der Verordnung (EU) 2016/679 anzupassen.

In Artikel 5:

Artikel 5 sieht Änderungen der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (e-Datenschutzrichtlinie) vor. Artikel 4 der genannten Richtlinie wird aufgehoben. Das Hinzufügen von Artikel 5 Absatz 3 der genannten Richtlinie ermöglicht die Übernahme der Vorschriften über die Speicherung personenbezogener Daten und den Zugriff am Endgerät einer natürlichen Person in die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung); das geschieht durch das Einfügen des neuen Artikels 88a der Verordnung (EU) 2016/679, wie oben beschrieben.

Zentrale Anlaufstelle zur Meldung von Vorfällen

In **Artikel 6**:

In den Nummern 1 und 2 wird die zentrale Anlaufstelle zur Meldung von Vorfällen eingerichtet: Sie enthalten auch spezifische Anforderungen an die ENISA. Darüber hinaus

wird darin festgelegt, dass die Meldung von Vorfällen gemäß der NIS-2-Richtlinie bei der neuen zentralen Anlaufstelle erfolgen sollte.

In **Artikel 7**: Die zentrale Anlaufstelle ist auch für die Meldung von Vorfällen gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) zuständig.

In Artikel 8: Die zentrale Anlaufstelle ist auch für die Verordnung (EU) 2022/2554 (DORA) zuständig.

In **Artikel 9**: Die zentrale Anlaufstelle ist auch für die Richtlinie (EU) 2022/2557 (CER) zuständig.

Darüber hinaus ist in Artikel 3 Absatz 6 vorgesehen, dass die Meldung von Datenschutzverletzungen auch gemäß der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) über die zentrale Anlaufstelle erfolgen muss. In Artikel 5 Absatz 1 werden die Meldepflichten gemäß der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) aufgehoben, denn angesichts der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) sind sie hinfällig.

Aufhebungen von Rechtsakten und Schlussbestimmungen

In **Artikel 10**:

In Nummer 1 wird die Verordnung (EU) 2019/1150 (P2B-Verordnung) aufgehoben, die angesichts der jüngsten Vorschriften, die weitgehend dieselben Fragen abdecken, nur noch wenig Bedeutung hat. Hiervon abweichend betrifft Nummer 2 jegliche Querverweise auf die Verordnung (EU) 2019/1150 (P2B-Verordnung) in anderen Rechtsinstrumenten: Solche Verweise bleiben bis zur Änderung in ihren ursprünglichen Rechtsakten in Kraft, längstens jedoch bis zum 31. Dezember 2032, um Rechtsunsicherheiten zu vermeiden.

In Nummer 3 werden die in die Verordnung (EU) 2023/2854 (Datenverordnung) übernommenen Rechtstexte aufgehoben.

Artikel 11 enthält die Schlussbestimmungen der Änderungsverordnung.

2025/0360 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[21],

nach Stellungnahme der Europäischen Zentralbank[22],

nach Stellungnahme des Ausschusses der Regionen[23],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) In ihrer Mitteilung „Ein einfacheres und schnelleres Europa“[24] kündigte die Kommission ihr Engagement für ein ehrgeiziges Programm zur Förderung zukunftsorientierter, innovativer Strategien an, die die Wettbewerbsfähigkeit der Union stärken, den Regelungsaufwand für die Menschen, Unternehmen und Verwaltungen drastisch verringern und höchste Standards bei der Förderung der Werte der Union wahren sollen. Folglich räumte die Kommission dem Vorschlag sofortiger Anpassungen der Gesetzgebung Vorrang ein, einschließlich der Rechtsvorschriften für den digitalen Bereich, damit die Union die Herausforderungen der Wettbewerbsfähigkeit bewältigt.

(2) Das Unionsrecht für digitalen Bereich setzt hohe Standards in der Union und kann Unternehmen, die sich an die Vorschriften halten, starke Wettbewerbsvorteile

---

21 ABl. C […] vom […], S. […].

22 ABl. C […] vom […], S. […].

23 ABl. C […] vom […], S. […].

24 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Ein einfacheres und schnelleres Europa: Mitteilung über die Umsetzung und Vereinfachung, COM(2025) 47 final, 11. Februar 2025.

verschaffen, denn es steht für weltweit führende Qualität, Sicherheit und Vertrauenswürdigkeit. Die Digitalvorschriften geben klare Spielregeln für verantwortungsvolle Unternehmen in der Union vor, gewährleisten Fairness und Transparenz in den Geschäftsbeziehungen von Unternehmen, regen innovative Geschäftsmodelle an und gewährleisten ein hohes Maß an Schutz und Sicherheit der Verbraucher und den Schutz der Grundrechte, nicht zuletzt auch der Privatsphäre und des Datenschutzes.

(3) Als Reaktion auf den rasch wachsenden Fußabdruck digitaler Technologien in der Wirtschaft und auf die gesellschaftliche Dynamik in der Union haben sich ihre Rechtsvorschriften für den digitalen Bereich in den letzten Jahren Schritt für Schritt weiterentwickelt – das gilt auch hinsichtlich der neuen Herausforderungen und der Förderung von Geschäftsmöglichkeiten in der EU. Die Kommission verpflichtete sich zum systematischen „Stresstest" der Digitalvorschriften. Dieser Test könnte zusammen mit anderen Unionsvorschriften zu weiteren regulatorischen Anpassungen führen, insbesondere nach der bevorstehenden digitalen Eignungsprüfung oder nach anderen gezielten Bewertungen der Digitalvorschriften; dessen ungeachtet sind sofortige regulatorische Änderungen erforderlich. Folglich enthält diese Verordnung den Vorschlag für eine erste Reihe von Änderungen des Rechtsrahmens im digitalen Bereich, die unverzüglich regulatorische Fragen klären, Innovationen auf dem Unionsmarkt fördern, die administrativen Befolgungskosten insbesondere für Unternehmen senken und die Aufsichts- und Verwaltungskosten für Aufsichtsbehörden und beratende Einrichtungen straffen sollen. Die Änderungen zielen auch darauf ab, Einzelpersonen Klarheit zu verschaffen.

(4) Angesichts der grundlegenden Rolle von Daten als Motor der Wertschöpfung in der digitalen Wirtschaft und gemäß den Zielen der Mitteilung über die Strategie für eine europäische Datenunion sollen die in dieser Verordnung vorgelegten Änderungen des Rechtsrahmens für Daten einen kohärenten und einenden Rechtsrahmen für die Verfügbarkeit und Nutzung von Daten schaffen; gleichzeitig sollen die Änderungen den Rechtsrahmen für Daten straffen und in nur zwei Rechtsakten zusammenfassen, nämlich den Verordnungen (EU) 2016/679[25] und (EU) 2023/2854[26] des Europäischen Parlaments und des Rates, gegenüber den derzeit fünf verschiedenen anwendbaren Rechtsakten. Mit diesen Änderungen sollen unnötige Verwaltungskosten gesenkt werden und es soll die Verfügbarkeit von Daten als Voraussetzung für die Unterstützung wettbewerbsfähiger digitaler Unternehmen in der Union gefördert werden; dabei sind das höchste Maß an Schutz der Privatsphäre und personenbezogener Daten sowie faire Geschäftspraktiken zu wahren und zentrale Regulierungsziele, darunter die Einhaltung des EU- und nationalen Wettbewerbsrechts, zu gewährleisteten.

---

[25] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[26] VERORDNUNG (EU) 2023/2854 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

(5) Angesichts der iterativen Entwicklung horizontaler und sektorspezifischer Vorschriften ist es unerlässlich, auch Überschneidungen spezifischer Bestimmungen anzugehen, die den Verwaltungsaufwand unnötig vervielfachen. Solche Überschneidungen liegen bei Anforderungen in mehreren Vorschriften über die Meldung von Cybersicherheitsvorfällen und verwandten Vorfällen vor; diesbezüglich können digitale Lösungen, wie in dieser Verordnung vorgeschlagen, Unternehmen in allen betroffenen Sektoren sofortige Entlastung bieten.

(6) In ähnlicher Weise hat die iterative Regulierung von Online-Plattformen in den letzten Jahren in den neueren Vorschriften einen klareren und ehrgeizigeren Rahmen geschaffen als einige alte, damit nun hinfällige Vorschriften. Daher muss sich der Rechtsrahmen notwendigerweise weiterentwickeln und unnötige, die rechtliche Komplexität erhöhende Überschneidungen beseitigen.

(7) In der Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates[27] sind Vorschriften für Vermittlerfunktionen in drei verschiedenen Umgebungen festgelegt: a) Funktionen zur Unterstützung der Weiterverwendung geschützter Daten, die sich im Besitz öffentlicher Stellen befinden, unter kontrollierten Bedingungen, b) Datenvermittlungsdienste, die eine Datenweitergabe zwischen betroffenen Personen, Dateninhabern und Datennutzern erleichtern, c) datenaltruistische Organisationen, welche die Nutzung von Daten unterstützen, die betroffene Personen oder Dateninhaber in altruistischer oder philanthropischer Weise zur Verfügung stellen. Die Funktionen zur Unterstützung der Weiterverwendung geschützter Daten im Besitz des öffentlichen Sektors hängen eng mit den Vorschriften der Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates[28] zusammen. Ihr Zusammenwirken hat insbesondere bei öffentlichen Stellen zu Verwirrung geführt. Daher ist es notwendig, die beiden Regelwerke zusammenzuführen. Die Bewertung der Vorschriften für Datenvermittlungsdienste hat gezeigt, dass die Begriffsbestimmung „Anbieter von Datenvermittlungsdiensten“ Schwächen aufweist und dass die Vorschriften für die Diensteanbieter zu streng sind, um ein nachhaltiges Finanzmodell zu finden. Daher ist es auch notwendig, diese Regelungen zu straffen. Hinsichtlich des Datenaltruismus erscheinen bestimmte Vorschriften der Verordnung (EU) 2022/868 unnötig, insbesondere die Verpflichtung der Mitgliedstaaten zur Aufstellung nationaler Datenaltruismus-Strategien, die Erstellung eines „Regelwerks“ und die Entwicklung eines europäischen Einwilligungsformulars für Datenaltruismus, was auch vor dem Hintergrund der laufenden Arbeiten des Europäischen Datenschutzausschusses gemäß Artikel 68 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des

---

[27] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) (ABl. L 152 vom 3.6.2022, S. 1, ELI: https://data.europa.eu/eli/reg/2022/868/oj).

[28] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172 vom 26.6.2019, S. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

Rates[29] über Leitlinien zur Verarbeitung personenbezogener Daten in der wissenschaftlichen Forschung gilt.

(8) Die Bedeutung von Datenvermittlungsdiensten ist im Kontext vieler Initiativen zur Unterstützung der Datenweitergabe und Zusammenarbeit anerkannt; dennoch sollten die Vorschriften der Verordnung (EU) 2022/868 über Anbieter von Datenvermittlungsdiensten präzisiert werden. Insbesondere wäre die Begriffsbestimmung solcher Anbieter zu präzisieren. Elemente, die lediglich als Beispiele und nicht als Ausnahmen dienten, wären daraus zu entfernen. Darüber hinaus sollten Schlupflöcher geschlossen werden, die sich aus mehrdeutigen Formulierungen ergeben, insbesondere bezüglich des Begriffs „geschlossene Gruppe". Es sollte nicht möglich sein, nur von einer geschlossenen Gruppe von Unternehmen genutzte Dienste als Datenvermittlungsdienste zu registrieren, sofern nur diese Gruppe und nicht der Diensteanbieter eine Ausweitung dieser Unternehmensgruppe beschließen kann. Noch wichtiger ist, dass die verbindliche Regelung dieses aufstrebenden Marktes unnötige Befolgungskosten verursacht hat. In diesem Stadium der Marktentwicklung erscheint eine freiwillige Regelung, die es neutralen Akteuren ermöglicht, sich von anderen Akteuren zu unterscheiden, ausreichend. Um nachhaltige Geschäftsmodelle zu ermöglichen, wäre die Regelung zudem weniger streng zu gestalten. So sollte die erforderliche rechtliche Trennung von Datenvermittlungsdiensten und anderen Mehrwertdiensten, die angeboten werden dürfen, abgeschafft und durch eine funktionale Trennung ersetz werden, wobei bestimmte Garantien beibehalten werden sollten. Das System der Verwaltungsüberwachung sollte vereinfacht werden. Anstelle nationaler Register und öffentlicher Unionsregister für Anbieter von Datenvermittlungsdiensten und datenaltruistischen Organisationen sollte es nur öffentliche Unionsregister geben, nämlich eines für Anbieter von Datenvermittlungsdiensten und eines für datenaltruistische Organisationen. Bei dieser Aufgabe sollten die zuständigen Behörden, welche die Vergabe des Siegels und die Einhaltung der Anforderungen zu seiner Erlangung seitens der Einrichtungen überwachen, unabhängig sein. Das ist so zu verstehen, dass die Behörden rechtlich und funktional von einem Datenvermittlungsdienst oder einer datenaltruistischen Organisation unabhängig sind, auch auf ihrer obersten Leitungsebene. Regierungsstellen sollten die Möglichkeit haben, Datenvermittlungsdienste oder datenaltruistische Organisationen finanziell zu unterstützen, insbesondere angesichts ihres neu entstehenden Charakters, sofern es sich um rechtlich getrennte Einrichtungen handelt. Damit anerkannte Einrichtungen in der gesamten Union leicht als solche erkennbar sind, erließ die Kommission die Durchführungsverordnung (EU) 2023/1622 über die Ausgestaltung gemeinsamer Logos für die in der Union anerkannten Anbieter von Datenvermittlungsdiensten und datenaltruistischen Organisationen.

(9) Mit der Verordnung (EU) 2023/2854 werden Hindernisse beim Datenzugang und der Datennutzung beseitigt, ihr Inhalt erschließt datengesteuerte Innovation, fördert die

---

[29] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

Wettbewerbsfähigkeit und schützt die Anreize jener, die in Datentechnologien investieren.

(10) Gemäß Kapitel II der Verordnung (EU) 2023/2854 müssen Dateninhaber den Nutzern und den von diesen ausgewählten Dritten Daten zur Verfügung stellen; dies umfasst auch als Geschäftsgeheimnisse geschützte Daten, sofern die vom Dateninhaber festgelegten Vertraulichkeitsmaßnahmen eingehalten werden. Diese Anforderung der Wahrung der Vertraulichkeit ergänzt die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates[30], die die Standards für den Schutz von Geschäftsgeheimnissen in der Union vorgibt. Jedoch erhöht die Offenlegung von Geschäftsgeheimnissen gegenüber Rechtsträgern aus Drittländern möglicherweise die Risiken für die Integrität und Vertraulichkeit der Daten, falls es sich um Rechtsordnungen mit unzureichendem Schutz oder schwieriger realer Durchsetzung handelt, was zu unbefugter Nutzung, wirtschaftlichem Schaden und Rechtsunsicherheit führen kann.

(11) Es ist notwendig, die Verordnung (EU) 2023/2854 zu stärken, nämlich durch die Einführung eines zusätzlichen Rechtsgrundes für Dateninhaber, die Offenlegung von Geschäftsgeheimnissen zu verweigern; dies würde bestehende Bestimmungen ergänzen, die Dateninhabern eine solche Verweigerung gestatten, sofern sie einen sehr wahrscheinlichen schweren wirtschaftlichen Schaden nachweisen können. Nach der neuen Bestimmung können Dateninhaber die Offenlegung von Geschäftsgeheimnissen verweigern, wenn sie ein hohes Risiko des rechtswidrigen Erwerbs oder der rechtswidrigen Nutzung oder Offenlegung zugunsten von Einrichtungen oder Systemen mit unzureichenden Schutz nachweisen, deren schützender Rechtsrahmen schwächer ist als die geltenden Unionsvorschriften – oder diesen nicht gleichwertig ist. Die neue Bestimmung deckt auch Fälle von theoretisch soliden oder über die Unionsvorschriften hinausgehenden Drittstaats-Rechtsrahmen ab, die aber in der Praxis nicht angemessen durchgesetzt werden. Derartige Risiken unterstreichen den möglichen Erwerb und die mögliche Nutzung oder Offenlegung von Geschäftsgeheimnissen unter Verstoß gegen das Unionsrecht, was die Integrität und Vertraulichkeit von Geschäftsgeheimnissen gefährden könnte.

(12) Die Nutzung des Verweigerungsmechanismus sollte freiwillig bleiben, und der Nachweis sollte erst nach seiner Inanspruchnahme zu erbringen sein. Zur Begründung der Weigerung, Daten weiterzugeben oder Geschäftsgeheimnisse offenzulegen, sollten die Dateninhaber nicht verpflichtet sein, eine umfassende Analyse vorzulegen oder den Grad des Schutzes von Geschäftsgeheimnissen in Drittländern oder bei Einrichtungen in Drittländern nachzuweisen. In einem solchen Nachweis können die Dateninhaber diverse Faktoren berücksichtigen, wie unzureichende oder unangemessene Rechtsnormen, mangelnde oder willkürliche Durchsetzung, historische Verstöße, mit dem Unionsrecht kollidierende ausländische Offenlegungspflichten, begrenzte Rechtsmittel oder Rechtsbehelfe für Einrichtungen

---

[30] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.6.2016, S. 1).

der Union, strategischen Missbrauch von Verfahrenstaktiken zum Schwächen von Wettbewerbern oder unzulässige politische Einflussnahme. Angesichts der diversen beteiligten Einrichtungen, Drittländer und Datenweitergabeszenarien sollten sich die Dateninhaber bei ihrer Bewertung und Demonstration auf maßgebliche Risiken konzentrieren und entsprechend handeln; so können sie unter anderem geeignete Schutzvorkehrungen treffen oder den Verweigerungsmechanismus in Kraft setzen. Verweigerungen der Datenweitergabe sollten klar, verhältnismäßig und auf die besonderen Umstände des Einzelfalls zugeschnitten sein; demnach sind sie nicht systematisch oder allgemein in einem Drittland anzuwenden.

(13) Ein unzureichender Schutz von Geschäftsgeheimnissen und die Herausforderungen ihrer Durchsetzung in Drittländern können europäischen Unternehmen einen nicht wiedergutzumachenden Schaden zufügen. Daher lautet das Ziel, zur Stärkung der Schutzvorkehrungen für Geschäftsgeheimnisse ihre Weitergabe an natürliche oder juristische Personen zu verhindern, die in Ländern oder Gebieten ansässig sind, in denen solche Risiken bestehen. Das schließt Unternehmen mit Sitz in der Union ein, die von Rechtsträgern aus Drittländern kontrolliert werden und bösgläubig oder getarnt zugunsten solcher Rechtsträger handeln können. Ein weiteres Ziel ist, direkte Risikopositionen gegenüber in der Union tätigen Unternehmen aus Drittländern, die solchen Rechtsordnungen unterliegen, zu vermeiden. Der Hoheitsgewalt eines Drittlands zu unterstehen, bedeutet für eine natürliche oder juristische Person, rechtlich den Gesetzen einer Regulierungsbehörde oder der Kontrolle eines Drittlands zu unterliegen oder anderweitig an diese gebunden zu sein. Tochterunternehmen oder verbundene Unternehmen von Muttergesellschaften aus Drittländern können diese Rechtsordnungen ausnutzen, um das Unionsrecht zu umgehen. Der Begriff der direkten oder indirekten Kontrolle bezieht sich auf das Ausüben eines bestimmenden oder beherrschenden Einflusses auf die Geschäftsführung oder strategische Entscheidungen eines anderen Unternehmens, sei es durch Eigentum an Kapital, Stimmrechte, finanzielle Beteiligung, vertragliche Vereinbarungen oder zwischengeschaltete Stellen. Das Ausüben von Kontrolle kann direkt oder aber auf andere Weise erfolgen, auch ohne Mehrheitsbeteiligung. Die Dateninhaber sollten sich nach Kräften bemühen, die einschlägigen Informationen zu erhalten – möglicherweise mittels Suchabfragen in öffentlichen Registern oder direkter Informationsanforderung beim Nutzer oder einer Drittpartei, wobei ein angemessenes, nicht intrusives Vorgehen zu gewährleisten ist.

(14) Der Schutz von Geschäftsgeheimnissen ist angesichts dieser Schwachstellen für die europäische Industrie unverzichtbar, um ihre Marktposition und ihren Wettbewerbsvorteil zu erhalten. Dateninhaber verfügen zwar über einen Ermessensspielraum beim Schutz ihrer Geschäftsgeheimnisse, jedoch sollten sie die Verweigerung von Datenweitergaben auf gerechtfertigte außergewöhnliche Umstände beschränken und so die Ziele der Verordnung (EU) 2023/2854 zur Förderung datengetriebener Innovation und einer florierenden digitalen Wirtschaft in der Union wahren. Die Schutzmaßnahmen gegen den Missbrauch des Verweigerungsmechanismus sollten bestehen bleiben, einschließlich der Verpflichtung des Dateninhabers, hinreichend begründet nachzuweisen, dass eine Offenlegung ein hohes Risiko darstellt, und der Verpflichtung, die zuständigen Behörden zu benachrichtigen. Dieser Nachweis ist dem Datennutzer oder Dritten unverzüglich schriftlich vorzulegen und muss dem betreffenden Fall angemessenen sein. Alle beteiligten Parteien sollten eine derartige Entscheidung und den unterstützenden Nachweis vertraulich behandeln, um die Vertraulichkeit der betroffenen Geschäftsgeheimnisse zu wahren. Nutzer und gegebenenfalls Dritte

können die Entscheidung des Dateninhabers bei der zuständigen Behörde, vor Gericht oder über Streitbeilegungsgremien anfechten.

(15) Um den Rahmen der gemeinsamen Datennutzung zwischen Unternehmen und Behörden gemäß der Verordnung (EU) 2023/2854 zu vereinfachen und Unklarheiten über die den Unternehmen zuvor auferlegten, umfassenderen Verpflichtungen zu klären, ist es erforderlich, den Anwendungsbereich des Kapitels V der genannten Verordnung von „außergewöhnlicher Notwendigkeit“ auf „öffentliche Notstände“ zu beschränken. So gewährleistet der in Artikel 2 Nummer 29 der Verordnung (EU) 2023/2854 definierte Begriff des „öffentlichen Notstands“, dass die in diesem Kapitel festgelegten Verpflichtungen nur in genau definierten, dringenden Situationen greifen, was die technischen, administrativen und rechtlichen Herausforderungen, die sich den Unternehmen unter der vorherigen Regelung stellten, verringert. Das würde gewährleisten, dass die Datenanfragen relevant und verhältnismäßig sind und mit ihnen auf öffentliche Notstände reagiert wird, diese abgemildert werden oder die diesbezügliche Erholung unterstützt wird. Da der aktualisierte Unionsrahmen für europäische Statistiken gemäß der Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates[31] nicht auf öffentliche Notstände abstellt, ist es wichtig, die Rolle amtlicher Statistiken gemäß Kapitel V der Verordnung (EU) 2023/2854 zu wahren, um in solchen Situationen für Eindeutigkeit und Wirksamkeit zu sorgen. Außerdem ist es notwendig, die Ausgleichsregelung für Situationen zu präzisieren, in denen Kleinstunternehmen und kleine Unternehmen Daten zur Bewältigung eines öffentlichen Notstands bereitstellen müssen – in solchen Fällen dürfen diese Unternehmen eine Gegenleistung beantragen.

(16) Um Rechtsunsicherheiten zu mindern, die innovative Geschäftsmodelle behindern könnten, ist es erforderlich, den erheblichen Aufwand und die wesentlichen Unklarheiten in Bezug auf die Einhaltung anzugehen, die hinsichtlich der Bestimmungen über intelligente Verträge zur Ausführung von Datenweitergabevereinbarungen gemäß Artikel 36 der Verordnung (EU) 2023/2854 bestehen. Es fehlen harmonisierte Normen und klare Definitionen für wichtige Begriffe wie „Robustheit“, „Zugangskontrolle“ und „Kohärenz bezüglich der Vertragsbedingungen“, ferner ist die Anforderung eines „sicheren Beendigungs- oder Unterbrechungsmechanismus“ möglicherweise unvereinbar mit dezentralen oder öffentlichen Blockchain-Architekturen, die auf unveränderlichen Journalen beruhen, was für Innovatoren aus der Sicht der Kosten und Möglichkeiten problematisch war. Darüber hinaus besteht die Gefahr, dass die Mehrdeutigkeit hinsichtlich der Durchführung der Konformitätsbewertung gemäß Artikel 36 Absatz 2 der genannten Verordnung unverhältnismäßige Belastungen mit sich bringt. Daher würde die Streichung des Artikels 36 der Verordnung (EU) 2023/2854 die Entwicklung und

---

[31] Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften (ABl. L 87 vom 31.3.2009, S. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

Markteinführung neuer Geschäftsmodelle fördern, Innovationen erleichtern und Hindernisse für neu entstehende Technik abbauen.

(17) Bestimmte Datenverarbeitungsdienste fallen nicht unter das Bereitstellungsmodell „Infrastruktur als Dienstleistung“ (IaaS) und sind vielmehr auf die Bedürfnisse oder das Ökosystem eines Kunden zugeschnitten. Die Erbringung solcher Datenverarbeitungsdienste beruht auf zeitintensiven vorvertraglichen und vertraglichen Verhandlungen, in denen die spezifischen Anforderungen des Kunden und die technischen Bemühungen zur Anpassung des Datenverarbeitungsdienstes für eine maßgeschneiderte Lösung festgelegt werden. Dabei handelt es sich um Dienste, die nicht standardmäßig erbracht werden und die auf die Bedürfnisse eines Kunden zugeschnitten sind, um eine maßgeschneiderte Lösung zu bieten, bei der die Mehrzahl der Merkmale und Funktionen des Datenverarbeitungsdienstes vom Anbieter an die spezifischen Bedürfnisse des Kunden angepasst wurde, wobei die Mehrzahl der Merkmale und Funktionen für einen Kunden ohne vorherige Anpassung durch den Anbieter nicht nutzbar wäre. Derartige Dienste unterscheiden sich von kundenspezifischen Datenverarbeitungsdiensten gemäß Artikel 31 Absatz 1 der Verordnung (EU) 2023/2854. Datenverarbeitungsdienste gelten als kundenspezifisch, wenn der Anbieter die meisten Hauptmerkmale individuell an die besonderen Bedürfnisse eines einzelnen Kunden anpasst oder wenn der Anbieter diese Dienste nicht im größeren kommerziellen Maßstab in seinem Dienstleistungskatalog anbietet. Um bei der notwendigen Wiedereröffnung und Neuaushandlung von Verträgen, die bis zum 12. September 2025 abgeschlossen wurden, zusätzliche Kosten und Verwaltungsaufwand zu vermeiden, ist Folgendes klarzustellen: Kundenspezifische Dienste, die aufgrund bis zum 12. September 2025 geschlossener Verträge erbracht werden, mit Ausnahme der Verpflichtung, Wechsel- und Ausstiegsgebühren zu senken und letztlich abzuschaffen, sollten nicht in den Anwendungsbereich von Kapitel VI der Verordnung (EU) 2023/2854 fallen.

(18) Aus Gründen der Finanzplanung und der Anziehung von Investitionen bevorzugen Anbieter von Datenverarbeitungsdiensten, insbesondere KMU und kleine Midcap-Unternehmen, eventuell Verträge mit fester Laufzeit und bieten solche Verträge an. Es ist klarzustellen, dass Anbieter von Datenverarbeitungsdiensten Bestimmungen über verhältnismäßige Sanktionen für eine vorzeitige Kündigung in solche Verträge aufnehmen dürfen, solange diese Sanktionen kein Hindernis für einen Wechsel darstellen. Darüber hinaus belastet die notwendige Anpassung bestehender Verträge über die Erbringung von Datenverarbeitungsdiensten an die Verordnung (EU) 2023/2854 kleine Midcap-Unternehmen und KMU als Anbieter von Datenverarbeitungsdiensten besonders. Daher ist es erforderlich, eine besondere Regelung für solche Anbieter zu schaffen, die andere Datenverarbeitungsdienste als IaaS auf der Grundlage bis zum 12. September 2025 abgeschlossener Verträge erbringen. Unter Berücksichtigung des Ziels der Verordnung (EU) 2023/2854, den Wechsel zwischen Datenverarbeitungsdiensten zu ermöglichen, und angesichts der Tatsache, dass Wechselentgelte, einschließlich Ausstiegsentgelten, ein schwerwiegendes Hindernis für den Wechsel darstellen, sollten die neuen, weniger strengen, maßgeschneiderten oder von KMU oder kleinen Midcap-Unternehmen aufgestellten Regelungen für Datenverarbeitungsdienste die schrittweise erfolgende Abschaffung dieser Entgelte nicht erschweren. Diesem Ziel zuwiderlaufende vertragliche Bestimmungen sollten als nichtig angesehen werden, wenn sie in vertraglichen Vereinbarungen über die Erbringung von Dienstleistungen enthalten sind, die in den Anwendungsbereich dieser beiden neuen, spezifischen Regelungen fallen.

(19) In der Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates[32] wurde ein zentraler Grundsatz zur Unterstützung der datengesteuerten Wirtschaft in der Union eingeführt, der die Niederlassungsfreiheit und die Dienstleistungsfreiheit konkret untermauert. Der mit dem Verbot von Datenlokalisierungsauflagen präzisierte „freie Datenverkehr“ in der Union ist nach wie vor ein Grundprinzip, das Unternehmen Rechtssicherheit bietet, und sollte in der Verordnung (EU) 2023/2854 beibehalten werden. Diese Bestimmung berührt die Datenverarbeitung nicht, soweit sie im Rahmen einer Tätigkeit erfolgt, die gemäß Artikel 4 des Vertrags über die Europäische Union nicht in den Anwendungsbereich des Unionsrechts fällt, insbesondere im Hinblick auf die nationale Sicherheit. Gleichzeitig ersetzen neuere Vorschriften einige andere Bestimmungen der Verordnung (EU) 2018/1807. Insbesondere wird mit Kapitel VI der Verordnung (EU) 2023/2854 ein moderner horizontaler Rechtsrahmen eingeführt, der den Wechsel zwischen Datenverarbeitungsdiensten regelt und Artikel 6 der Verordnung (EU) 2018/1807 praktisch hinfällig macht. Das Nebeneinander dieser Bestimmungen hat die rechtliche Komplexität für die Unternehmen erhöht. Deshalb sollte die Verordnung (EU) 2018/1807 aufgehoben werden.

(20) Der Begriff der öffentlichen Sicherheit im Sinne von Artikel 52 AEUV und gemäß der Auslegung durch den Gerichtshof bezieht sich sowohl auf die innere als auch die äußere Sicherheit eines Mitgliedstaats sowie auf Fragen der Sicherheit der Bevölkerung, um insbesondere die Untersuchung, Aufdeckung und Verfolgung von Straftaten zu erleichtern. Er setzt die Existenz einer tatsächlichen erheblichen Gefahr voraus, die ein Grundinteresse der Gesellschaft berührt, wie eine Bedrohung für das Funktionieren der Institutionen, der grundlegenden öffentlichen Dienstleistungen und das Überleben der Bevölkerung sowie die Gefahr einer erheblichen Störung der Außenbeziehungen, der friedlichen Koexistenz der Nationen oder eine Bedrohung der militärischen Interessen. Gemäß dem Grundsatz der Verhältnismäßigkeit sollten Datenlokalisierungsauflagen, die aus Gründen der öffentlichen Sicherheit gerechtfertigt sind, zur Erreichung der damit verfolgten Ziele geeignet sein und nicht über das dafür Notwendige hinausgehen.

(21) In der Richtlinie (EU) 2019/1024 und in Kapitel II der Verordnung (EU) 2022/868 ist die Weiterverwendung von Informationen des öffentlichen Sektors zu Innovationszwecken geregelt. Das Zusammenspiel der beiden Regelwerke hat vor allem bei öffentlichen Stellen zu Rechtsunsicherheit geführt. Deshalb ist eine Angleichung der Vorschriften in einem einzigen Rechtsinstrument erforderlich, um für mehr rechtliche Kohärenz und Rechtssicherheit zu sorgen.

(22) Sowohl die Richtlinie (EU) 2019/1024 als auch die Verordnung (EU) 2022/868 sollen die Weiterverwendung von Informationen des öffentlichen Sektors fördern, und um die Vorschriften aus der Sicht der öffentlichen Stellen und der Weiterverwender von Informationen des öffentlichen Sektors zu vereinfachen, ist es sinnvoll, die Richtlinie (EU) 2019/1024 und die Verordnung (EU) 2022/868 aufzuheben, die beiden

---

[32] Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (ABl. L 303 vom 28.11.2018, S. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

Regelungen aneinander anzugleichen und die betreffenden Vorschriften in einem einzigen Kapitel der vorliegenden Verordnung zu konsolidieren. Das wird diese Vorschriften in der Union verstärkt harmonisieren, den Verwaltungsaufwand bei der Auslegung und Umsetzung nationaler Rechtsvorschriften verringern und Unternehmen die Entwicklung grenzüberschreitender Dienstleistungen und Produkte erleichtern. Bei der Benennung der zuständigen Stellen sollten die Mitgliedstaaten letztlich alle relevanten Sektoren erfassen – das gilt auch für die Benennung sektorspezifischer zuständiger Stellen. Die Änderungen in dieser Verordnung sind so zu verstehen, dass sie die Auslegung der diversen Definitionen und Begriffe nur dann ändern, wenn dies klar angegeben ist.

(23) Daten und Dokumente, die sich zur Weiterverwendung öffentlich zugänglich machen lassen, sowie jene, die aufgrund von Geschäftsgeheimnissen geschützt sind, darunter Betriebs-, Berufs- und Unternehmensgeheimnisse, statistische Geheimhaltung sowie Schutz des geistigen Eigentums Dritter und von personenbezogenen Daten, sind häufig im Besitz derselben öffentlichen Stellen. Daher ist es notwendig, die für alle Informationen des öffentlichen Sektors geltenden Begriffsbestimmungen und gemeinsamen Grundsätze anzugleichen und Fragen zum Zusammenspiel der beiden Regelwerke zu behandeln.

(24) Die bestehenden Vorschriften sollten im Interesse der Klarheit und Kohärenz gestrafft werden. Dennoch sollten die beiden Weiterverwendungsregelungen unterschiedlich bleiben, und ihre Anwendungsbereiche sollten weiterhin von den jeweiligen Merkmalen der Daten oder Dokumente und vom Kontext ihrer Weiterverwendung abhängen. Öffentliche Stellen sollten die Regelung für offene Daten anwenden, wann immer es möglich ist. Nur dann, wenn sie feststellen, dass Daten oder Dokumente Informationen bestimmter geschützter Kategorien enthalten, sollten sie deren öffentliche Verfügbarkeit einschränken und erwägen, sie zur Weiterverwendung als geschützte Daten zur Verfügung zu stellen.

(25) Start-up-Unternehmen, kleine Unternehmen und Unternehmen, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG[33] der Kommission als mittlere Unternehmen einzustufen sind, sowie Unternehmen aus Branchen mit weniger entwickelten digitalen Fähigkeiten tun sich schwer mit der Weiterverwendung von Daten und Dokumente. Gleichzeitig sind aufgrund der Anhäufung und Aggregation gewaltiger Datenmengen und der nötigen technischen Infrastruktur für ihre Monetarisierung in der digitalen Wirtschaft wenige sehr große Unternehmen mit beträchtlicher wirtschaftlicher Macht entstanden. Hierzu zählen sehr große Unternehmen, die zentrale Plattformdienste erbringen und die gemäß der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates[34] als Torwächter benannt sind und besonderen Verpflichtungen bezüglich des Ausgleichs von Ungleichgewichten

---

33 Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

34 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

unterliegen. Um derartige Ungleichgewichte zu beheben und Wettbewerb und Innovation zu stärken, sollten öffentliche Stellen in der Lage sein, besondere Bedingungen in Lizenzen zur Weiterverwendung von Daten und Dokumenten durch sehr große Unternehmen einzuführen. Solche Bedingungen sollten verhältnismäßig sein, auf objektiven Kriterien beruhen und die Wirtschaftskraft des Unternehmens, seine Fähigkeit zum Datenerwerb oder seine Benennung als Torwächter gemäß der Verordnung (EU) 2022/1925 sowie gegebenenfalls andere derartige Kriterien berücksichtigen. Unter anderem können sich solche besonderen Bedingungen auf Gebühren und Entgelte oder auf die Zwecke der Weiterverwendung beziehen.

(26) Im Sinne der Innovationsförderung und um einen fairen Wettbewerb auf dem digitalen Markt der Union zu wahren, müssen der Zugang zu Daten des öffentlichen Sektors und ihre Weiterverwendung unbedingt einem breiten Spektrum von Marktteilnehmern zugutekommen und dürfen bestehende marktbeherrschende Stellungen nicht unbeabsichtigt verstärken. Sehr große Unternehmen – insbesondere gemäß der Verordnung (EU) 2022/1925 benannte Torwächter – üben beträchtliche Macht und erheblichen Einfluss auf den Binnenmarkt aus. Damit solche Unternehmen ihre erheblichen Mittel nicht zum Nachteil des fairen Wettbewerbs und der Innovation ausnutzen, sollten öffentliche Stellen höhere Entgelte und Gebühren für die Weiterverwendung offener staatlicher und geschützter Daten festlegen können. Solche höheren Entgelte und Gebühren sollten verhältnismäßig sein und auf objektiven Kriterien beruhen. Dabei sind die Wirtschaftskraft des Unternehmens und seine Fähigkeit, Daten zu erwerben, zu berücksichtigen. Diese Maßnahme soll kleineren Unternehmen und neuen Marktteilnehmern die Möglichkeit sichern, in der digitalen Wirtschaft innovativ und wettbewerbsfähig zu sein.

(27) Mit dieser Verordnung wird eine Reihe gezielter Änderungen an der Verordnung (EU) 2016/679 vorgeschlagen, um eine Klarstellung und Vereinfachung zu bewirken und dabei das gleiche Datenschutzniveau zu wahren. Nach Artikel 4 der Verordnung (EU) 2016/679 sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle hinreichend wahrscheinlich genutzten Mittel zu ihrer direkten oder indirekten Identifizierung berücksichtigt werden. Unter Beachtung der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union zur Definition personenbezogener Daten ist eingehender zu klären, wann eine natürliche Person als identifizierbar gelten sollte. Zusätzliche vorliegende Informationen, welche die Identifizierung der betroffenen Person ermöglichen, bedeuten für sich genommen nicht, dass pseudonymisierte Daten für die Zwecke der Anwendung der Verordnung (EU) 2016/679 in allen Fällen und für jede Person oder Stelle als personenbezogene Daten anzusehen sind. Insbesondere wäre klarzustellen, dass Informationen für eine bestimmte Einrichtung nicht als personenbezogene Daten gelten, wenn diese Einrichtung über keine Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person dienen, auf die sich die Informationen beziehen. Bei einer eventuellen späteren Übermittlung dieser Informationen an Dritte, die ihrerseits nach vernünftigem Ermessen über Mittel verfügen, um die natürliche Person, auf die sich die Informationen beziehen, zu identifizieren, etwa durch einen Abgleich mit anderen ihnen zur Verfügung stehenden Daten, werden diese Angaben nur für jene Dritten, die solche Mittel besitzen, zu personenbezogenen Daten. Eine Einrichtung, für die bestimmte Informationen keine personenbezogenen Daten sind, fällt grundsätzlich nicht in den Anwendungsbereich der Verordnung (EU) 2016/679. Diesbezüglich hat der Gerichtshof der Europäischen Union Folgendes festgestellt: Der Einsatz eines

Mittels zur Identifizierung der betroffenen Person ist nicht hinreichend wahrscheinlich, wenn die wirkliche Gefahr der Identifizierung unbedeutend erscheint, da diese gesetzlich verboten oder in der Praxis unmöglich ist, zum Beispiel wegen unverhältnismäßigen Aufwands hinsichtlich Zeit, Kosten und Arbeit. Ein Beispiel des Verbots der erneuten Identifizierung findet sich in den Pflichten der Gesundheitsdatennutzer in Artikel 61 Absatz 3 der Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates[35]. Die Kommission sollte gemeinsam mit dem Europäischen Datenschutzausschuss die Verantwortlichen bei der Anwendung dieser aktualisierten Begriffsbestimmung unterstützen, indem sie in einem Durchführungsrechtsakt technische Kriterien festlegt.

(28) Bei der Beurteilung, ob Forschung die Bedingungen der wissenschaftlichen Forschung für die Zwecke dieser Verordnung erfüllt, können Elemente wie der in der Forschung im betreffenden Bereich angewandte methodische und systematische Ansatz berücksichtigt werden. Forschung und technologische Entwicklung sollten in akademischen, industriellen und sonstigen Umfeldern erfolgen, darunter auch in kleinen und mittleren Unternehmen (Artikel 179 Absatz 2 AEUV), stets von hoher Qualität sein und den Grundsätzen der Zuverlässigkeit, Ehrlichkeit, Achtung und Rechenschaftspflicht (Nachprüfbarkeit) entsprechen.

(29) Folgendes wäre zu bekräftigen: Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. In solchen Fällen ist es nicht erforderlich, anhand von Artikel 6 Absatz 4 dieser Verordnung zu prüfen, ob der Zweck der Weiterverarbeitung mit dem ursprünglichen Erhebungszweck der personenbezogenen Daten vereinbar ist.

(30) Eine vertrauenswürdige KI ist entscheidend, um Wirtschaftswachstum zu schaffen und Innovationen mit sozial günstigen Ergebnissen zu unterstützen. Die Entwicklung und Nutzung von KI-Systemen und der ihnen zugrunde liegenden Modelle, darunter großer Sprachmodelle und generativer Videomodelle, beruhen auf Daten, auch personenbezogenen Daten; das gilt für mehrere Phasen des KI-Lebenszyklus, wie Training, Test und Validierung. In einigen Fällen verbleiben die Daten in dem KI-System oder KI-Modell. Daher kann die Verarbeitung personenbezogener Daten in diesem Kontext zu einem Ziel des berechtigten Interesses im Sinne des Artikels 6 der Verordnung (EU) 2016/679 erfolgen. Dies berührt nicht die Verpflichtung des Verantwortlichen, dafür zu sorgen, dass die Entwicklung oder der Einsatz (die Einführung) von KI in einem bestimmten Kontext oder für bestimmte Zwecke mit anderen Rechtsvorschriften der Union oder der Mitgliedstaaten im Einklang steht, oder die Rechtsbefolgung zu gewährleisten, falls die Verwendung ausdrücklich gesetzlich verboten ist. Ebenso wenig wird seine Verpflichtung berührt, zu gewährleisten, dass alle anderen Bedingungen des Artikels 6 Absatz 1 Buchstabe f der

---

[35] Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847 (ABl. L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj).

Verordnung (EU) 2016/679 sowie alle anderen Anforderungen und Grundsätze der genannten Verordnung erfüllt sind.

(31) Im risikobasierten Ansatz, der die Skalierbarkeit der Verpflichtungen gemäß dieser Verordnung angibt, wägt der Verantwortliche der Datenverarbeitung das berechtigte Interesse, das er selbst oder ein Dritter verfolgt, und die Interessen, Rechte und Freiheiten der betroffenen Person gegeneinander ab, wobei zu prüfen wäre, ob das vom Verantwortlichen verfolgte Interesse der betroffenen Person und der Gesellschaft insgesamt zugutekommt, was zum Beispiel der Fall sein kann, wenn die Verarbeitung personenbezogener Daten erforderlich ist, um systematische Verzerrungen aufzudecken und zu beseitigen und so die betroffenen Personen vor Diskriminierung zu schützen, oder dann, wenn die Datenverarbeitung genaue und sichere Ergebnisse für eine vorteilhafte Nutzung gewährleisten soll, etwa die Zugänglichkeit bestimmter Dienste verbessern soll. Ferner wäre unter anderem Folgendes zu berücksichtigen: die angemessenen Erwartungen der betroffenen Person gemäß ihrer Beziehung zum Verantwortlichen, geeignete Garantien, um die Auswirkungen auf die Rechte der betroffenen Personen zu minimieren, wie etwa mehr Transparenz für die betroffenen Personen, ein bedingungsloses Recht auf Widerspruch gegen die Verarbeitung der personenbezogenen Daten, die Einhaltung technischer Angaben in einem Dienst, der die Datennutzung zur KI-Entwicklung durch Dritte beschränkt, der Einsatz anderer moderner Verfahren zum Schutz der Privatsphäre beim KI-Training und geeignete technische Maßnahmen zur wirksamen Minimierung der Risiken, die sich beispielsweise aus Rückflüssen, Datenverlusten und anderen beabsichtigten oder vorhersehbaren Abläufen ergeben.

(32) Die Verarbeitung personenbezogener Daten für die wissenschaftliche Forschung und die Anwendung der Bestimmungen der DSGVO über die wissenschaftliche Forschung hängen gemäß Artikel 89 Absatz 1 DSGVO von geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen ab. Hierzu wägt die DSGVO das Recht auf den Schutz personenbezogener Daten gemäß Artikel 8 der EU-Grundrechtecharta gegen die Freiheit der Wissenschaft gemäß Artikel 13 dieser Charta ab. Somit verfolgt die Verarbeitung personenbezogener Daten für wissenschaftliche Forschung ein berechtigtes Interesse im Sinne von Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679, sofern diese Forschung nicht gegen das Unionsrecht oder das Recht der Mitgliedstaaten verstößt. Dies gilt unbeschadet der Verpflichtung des Verantwortlichen, zu gewährleisten, dass alle anderen Bedingungen von Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 sowie alle anderen Anforderungen und Grundsätze der genannten Verordnung eingehalten werden.

(33) Die Entwicklung bestimmter KI-Systeme und KI-Modelle kann die Erhebung großer Datenmengen umfassen, einschließlich personenbezogener Daten und besonderer Kategorien derselben. Personenbezogene Daten besonderer Kategorien können in den Trainings-, Test- oder Validierungs-Datensätzen verbleiben oder im KI-System oder im KI-Modell gespeichert bleiben, obwohl Daten dieser Art für die Zwecke der Verarbeitung nicht erforderlich sind. Um die Entwicklung und den Betrieb von KI nicht unverhältnismäßig zu behindern und unter Berücksichtigung der Fähigkeiten des Verantwortlichen, personenbezogene Daten besonderer Kategorien zu ermitteln und zu entfernen, sollten Ausnahmen vom Verbot der Verarbeitung von Daten solcher Kategorien gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 zulässig sein. Ausnahmen sollten nur dann gelten, wenn der Verantwortliche geeignete technische und organisatorische Maßnahmen wirksam eingeführt hat, um die Verarbeitung solcher Daten zu vermeiden, geeignete Maßnahmen während des gesamten

Lebenszyklus eines KI-Systems oder KI-Modells ergreift und solche Daten nach der Ermittlung wirksam entfernt. Falls die Datenentfernung einen unverhältnismäßigen Aufwand bedeuten würde, insbesondere dann, wenn das Entfernen von Daten besonderer Kategorien, die in einem KI-System oder KI-Modell gespeichert sind, eine Umgestaltung desselben erfordern würde, sollte der Verantwortliche diese Daten wirksam vor der Nutzung zum Ableiten von Ergebnissen schützen, sowie vor ihrer Offenlegung oder jeder sonstigen Bereitstellung für Dritte. Diese Ausnahmeregelung sollte nicht gelten, wenn die Verarbeitung von personenbezogenen Daten besonderer Kategorien gemäß dem Zweck ihrer Verarbeitung erforderlich ist. In diesem Fall sollte sich der Verantwortliche auf die Ausnahmen nach Artikel 9 Absatz 2 Buchstaben a bis j der Verordnung (EU) 2016/679 stützen.

(34) Biometrische Daten nach der Begriffsbestimmung in Artikel 4 Nummer 14 der Verordnung (EU) 2016/679 sind bestimmte, mit spezifischen technischen Mitteln verarbeitete Merkmale einer natürlichen Person, die ihre eindeutige Identifizierung ermöglichen oder bestätigen. Der Begriff der biometrischen Daten umfasst zwei unterschiedliche Funktionen, nämlich die Identifizierung einer natürlichen Person oder die Verifizierung (Authentifizierung) ihrer behaupteten Identität. Beide Funktionen beruhen auf unterschiedlichen technischen Verfahren. Das Identifizierungsverfahren beruht auf einem Eins-zu-viele-Abgleich (1:n-Abgleich) der biometrischen Daten der betroffenen Person in einer Datenbank, während das Überprüfungsverfahren auf einem Eins-zu-eins-Abgleich (1:1-Abgleich) der biometrischen Daten beruht, die von der betroffenen Person, die damit ihre Identität geltend macht, bereitgestellt werden. Ausnahmen vom Verbot der Verarbeitung biometrischer Daten gemäß Artikel 9 Absatz 1 der Verordnung sollten auch dann zulässig sein, wenn die Überprüfung der behaupteten Identität der betroffenen Person für einen vom Verantwortlichen verfolgten Zweck erforderlich ist, sofern geeignete Garantien bestehen, die der betroffenen Person die alleinige Kontrolle über den Überprüfungsprozess ermöglichen. Wenn die biometrischen Daten zum Beispiel ausschließlich bei der betroffenen Person oder aber beim Verantwortlichen in verschlüsselter Form nach dem neuesten Stand der Technik sicher gespeichert sind und nur die betroffene Person den Schlüsselcode oder ein gleichwertiges Mittel besitzt, birgt diese Datenverarbeitung wahrscheinlich keine erheblichen Risiken für ihre Grundrechte und Freiheiten. Dabei erlangt der Verantwortliche keine Kenntnis der biometrischen Daten oder er erlangt diese nur für sehr kurze Zeit während des Überprüfungsprozesses.

(35) Artikel 15 der Verordnung (EU) 2016/679 gibt der betroffenen Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten, die sie betreffen, verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Zugang zu diesen Daten und auf bestimmte zusätzliche Auskünfte. Das Auskunftsrecht sollte es der betroffenen Person ermöglichen, sich der Rechtmäßigkeit der Datenverarbeitung bewusst zu sein und diese zu prüfen, und es sollte der Person ermöglichen, ihre anderen Rechte gemäß der Verordnung (EU) 2016/679 auszuüben. Hingegen wäre in Artikel 12 der Verordnung klarzustellen, dass keine betroffene Person das von Anfang an zu ihren Gunsten gültige Auskunftsrecht zu anderen Zwecken als zum Schutz ihrer Daten missbrauchen darf. Zum Beispiel wäre ein solcher Missbrauch des Auskunftsrechts gegeben, wenn die betroffene Person beabsichtigt, den Verantwortlichen zur Ablehnung eines Auskunftsantrags zu veranlassen, um anschließend eine Entschädigungszahlung zu verlangen, möglicherweise unter Androhung eines Schadensersatzanspruchs. Ein Missbrauch liegt beispielsweise auch dann vor, wenn eine betroffene Person übermäßig von ihrem Auskunftsrecht Gebrauch macht, mit der alleinigen Absicht, dem Verantwortlichen

einen Schaden zuzufügen, oder wenn eine Einzelperson ein Verlangen stellt und gleichzeitig anbietet, dieses gegen eine bestimmte Form der Vorteilgewährung seitens des Verantwortlichen zurückzuziehen. Um die Belastungen der Verantwortlichen angemessen zu halten, sollte außerdem die von ihnen zu erbringende Beweislast bezüglich eines exzessiven Verlangens geringer sein als bezüglich eines offensichtlich unbegründeten Antrags. Der Grund hierfür ist Folgender: Ein offensichtlich unbegründetes Verlangen hängt von Tatsachen ab, die hauptsächlich im Verantwortungsbereich des Verantwortlichen liegen, aber ein exzessives Verlangen betrifft möglicherweise das missbräuchliche Verhalten einer betroffenen Person, das vorwiegend außerhalb des Einflussbereichs des Verantwortlichen liegt. Somit kann der Verantwortliche einen solchen Missbrauch möglicherweise nur in einem zumutbaren Umfang nachweisen. In jedem Fall sollte die betroffene Person, wenn sie Zugang gemäß Artikel 15 der Verordnung (EU) 2016/679 verlangt, so spezifisch wie möglich sein. Zu weit gefasste und undifferenzierte Auskunftsverlangen sind ebenfalls als exzessiv anzusehen.

(36) Nach Artikel 13 der Verordnung (EU) 2016/679 ist der Verantwortliche verpflichtet, der betroffenen Person bestimmte Informationen über die Verarbeitung ihrer personenbezogenen Daten sowie bestimmte weitere erforderliche Informationen zur Verfügung zu stellen, um eine faire und transparente Verarbeitung gemäß den Absätzen 1, 2 und 3 dieser Bestimmung zu gewährleisten. Gemäß Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 gilt diese Verpflichtung nicht, wenn und sofern die betroffene Person bereits über diese Informationen verfügt. Um den Aufwand für die Verantwortlichen weiter zu verringern, ohne die Möglichkeiten der betroffenen Personen zur Ausübung ihrer Rechte nach Kapitel III der Verordnung zu beeinträchtigen, sollte diese Ausnahmeregelung auf folgende Situationen erweitert werden: immer dann, wenn die Datenverarbeitung wahrscheinlich nicht zu einem hohen Risiko im Sinne des Artikels 35 der Verordnung führt, und wenn angesichts des Kontexts der Erhebung der personenbezogenen Daten hinreichende Gründe für die Annahme bestehen, dass die betroffene Person bereits über die in Absatz 1 Buchstaben a und c genannten Informationen verfügt. Das gilt insbesondere hinsichtlich der Beziehung der betroffenen Person zum Verantwortlichen. In diesen Situationen sollte der Kontext der Beziehung des Verantwortlichen zur betroffenen Person sehr klar und begrenzt sein, und die Tätigkeit des Verantwortlichen sollte nicht datenintensiv sein, wie z. B. die Beziehung eines Handwerkers zu seinen Kunden, in der sich die Datenverarbeitung auf das zum Erbringen der Dienstleistung erforderliche Mindestmaß beschränkt. Die Tätigkeit des Verantwortlichen ist nicht datenintensiv, wenn er personenbezogene Daten in geringem Umfang erhebt und seine Verarbeitungsvorgänge nicht komplex sind, wie beispielsweise im Beschäftigungsbereich. Unter solchen Umständen, also dann, wenn der Verantwortliche eine geringe Menge personenbezogener Daten auf nicht datenintensive und nicht komplexe Weise verarbeitet, sollte vernünftigerweise erwartet werden, dass die betroffene Person z. B. über die Identitäts- und Kontaktdaten des Verantwortlichen verfügt und den Zweck der Verarbeitung kennt, sofern diese zur Erfüllung eines Vertrags erfolgt und die betroffene Person Vertragspartei ist, oder dann, wenn die betroffene Person im Einklang mit der Verordnung (EU) 2016/679 ihre Einwilligung zu dieser Verarbeitung erteilt hat. Gleiches sollte für Vereine und Sportvereine gelten, wo sich die Verarbeitung personenbezogener Daten auf die Verwaltung der Mitgliedschaft, die Kommunikation mit den Mitgliedern und die Organisation von Aktivitäten beschränkt. Diese Ausnahme von den Pflichten nach Artikel 13 lässt jedoch die unabhängigen Pflichten des Verantwortlichen nach

Artikel 15 der genannten Verordnung unberührt, die gelten, wenn die betroffene Person aufgrund der letztgenannten Bestimmung Zugang beantragt. Dort, wo die Ausnahme von den Pflichten nach Artikel 13 nicht gilt, können die Verantwortlichen beim Bereitstellen der erforderlichen Informationen in einem mehrstufigen Ansatz die Anforderungen der Vollständigkeit und des einfachen Verständnisses für die betroffene Person gegeneinander abwägen, insbesondere indem sie den Nutzern das Navigieren zu weiteren Informationen gestatten.

(37) Wenn die Datenverarbeitung der wissenschaftlichen Forschung dient und sich das Unterrichten der betroffenen Person als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden wäre, sollte das Bereitstellen der Informationen gemäß Artikel 13 dieser Verordnung nicht erforderlich sein. Dann sollte der Verantwortliche angemessene Anstrengungen unternehmen, um Kontaktdaten zu erhalten, falls diese ohne Weiteres verfügbar sind und ihre Beschaffung keinen unverhältnismäßigen Aufwand erfordern würde. Die Bereitstellung der Informationen wäre insbesondere dann ein unverhältnismäßiger Aufwand, wenn der Verantwortliche zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht wusste oder nicht vorhersah, dass er solche Daten später zur wissenschaftlichen Forschung verarbeiten würde. In diesem Fall verfügt er möglicherweise nicht über leicht zugängliche Kontaktdaten der betroffenen Personen. In solchen Situationen sollte der Verantwortliche die betroffenen Personen indirekt informieren, indem er z. B. die Informationen öffentlich zugänglich macht. Diese Informationen sind so bereitzustellen, dass möglichst viele betroffene Personen erreicht werden. Die erforderlichen Mittel zur Veröffentlichung der Informationen wären abhängig vom Kontext des Forschungsprojekts und von den betroffenen Personen festzulegen.

(38) Artikel 22 der Verordnung (EU) 2016/679 enthält Vorschriften über die Verarbeitung personenbezogener Daten, wenn der Verantwortliche Entscheidungen, die sich rechtlich oder in ähnlicher Weise erheblich auf die betroffene Person auswirken, ausschließlich anhand automatisierter Verarbeitung trifft. Im Interesse der Rechtssicherheit wäre klarzustellen, dass unter bestimmten Bedingungen ausschließlich auf automatisierter Verarbeitung beruhende Entscheidungen gemäß der Verordnung (EU) 2016/679 zulässig sind. Außerdem wäre Folgendes klarzustellen: Bei der Bewertung, ob eine Entscheidung für den Abschluss oder die Erfüllung eines Vertrags der betroffenen Person mit einem Verantwortlichen gemäß Artikel 22 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 notwendig ist, sollte es nicht erforderlich sein, dass sich die Entscheidung ausschließlich durch automatisierte Verarbeitung treffen lässt. Folglich hindert die Tatsache, dass auch ein Mensch die Entscheidung treffen könnte, den Verantwortlichen nicht daran, die Entscheidung nur mittels automatisierter Verarbeitung zu treffen, und wenn mehrere gleich wirksame automatisierte Verarbeitungsmöglichkeiten gegeben sind, sollte der Verantwortliche die weniger intrusive Lösung verwenden.

(39) Um den Aufwand für die Verantwortlichen der Verarbeitung zu verringern und gleichzeitig sicherzustellen, dass die Aufsichtsbehörden Zugang zu den einschlägigen Informationen haben und bei Verstößen gegen die Verordnung tätig werden können, sollte die Schwelle für die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäß Artikel 33 der Verordnung (EU) 2016/679 an die Schwelle für die Meldung von Verletzungen des Schutzes personenbezogener Daten an eine betroffene Person gemäß Artikel 34 der genannten Verordnung angeglichen werden. Im Falle einer Verletzung des Schutzes

personenbezogener Daten, die voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, sollte der Verantwortliche nicht verpflichtet sein, die zuständige Aufsichtsbehörde zu benachrichtigen. Die höhere Schwelle für die Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde berührt weder die Verpflichtung des Verantwortlichen, die Verletzung gemäß Artikel 33 Absatz 5 der Verordnung (EU) 2016/679 zu dokumentieren, noch seine Verpflichtung, gemäß Artikel 5 Absatz 2 der genannten Verordnung nachweisen zu können, dass er die genannte Verordnung einhält. Um den Verantwortlichen die Einhaltung der Vorschriften und einen harmonisierten Ansatz in der Union zu erleichtern, sollte der Ausschuss ein gemeinsames Muster für die Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde und eine gemeinsame Liste der Umstände erstellen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten einer natürlichen Person führt. Die Kommission sollte den vom Ausschuss ausgearbeiteten Vorschlag gebührend berücksichtigen und ihn erforderlichenfalls vor seiner Annahme überprüfen. Um neuen Bedrohungen der Informationssicherheit Rechnung zu tragen, sollten die gemeinsame Vorlage und die Liste mindestens alle drei Jahre überprüft und erforderlichenfalls aktualisiert werden. Das Fehlen einer gemeinsamen Liste von Umständen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person zur Folge hat, sollte die Pflicht der Verantwortlichen zur Meldung solcher Verletzungen unberührt lassen.

(40) Nach Artikel 35 der Verordnung (EU) 2016/679 müssen Verantwortliche der Datenverarbeitung eine Datenschutz-Folgenabschätzung durchführen, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die gemäß der genannten Verordnung zuständigen Aufsichtsbehörden erstellen eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlichen diese. Die Verordnung regelt des Weiteren, dass Aufsichtsbehörden eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen können, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Um wirksam zum Erreichen des Ziels des Zusammenwachsens der Volkswirtschaften beizutragen und den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten wirksam zu gewährleisten, die Rechtssicherheit zu erhöhen, den Verantwortlichen der Datenverarbeitung die Einhaltung der Vorschriften zu erleichtern und eine harmonisierte Auslegung des Begriffs „hohes Risiko für die Rechte und Freiheiten der betroffenen Personen“ zu gewährleisten, sollte auf EU-Ebene eine einheitliche Liste der Verarbeitungsvorgänge erstellt werden, die die bestehenden nationalen Listen ersetzt. Darüber hinaus sollte die Veröffentlichung einer Liste der Arten von Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist, verbindlich vorgeschrieben werden, was derzeit fakultativ ist. Die Listen der Verarbeitungsvorgänge sollten vom Ausschuss erstellt und von der Kommission als Durchführungsrechtsakt erlassen werden. Um den für die Verarbeitung Verantwortlichen die Einhaltung der Vorschriften zu erleichtern, sollte der Ausschuss auch eine gemeinsame Vorlage und eine gemeinsame Methodik für die Durchführung von Datenschutz-Folgenabschätzungen ausarbeiten, die von der Kommission als Durchführungsrechtsakt angenommen werden sollen. Die Kommission sollte die vom Ausschuss ausgearbeiteten Vorschläge gebührend berücksichtigen und sie erforderlichenfalls vor ihrer Annahme überprüfen. Um den technologischen Entwicklungen Rechnung zu tragen, sollten die Listen sowie die

gemeinsame Vorlage und Methodik mindestens alle drei Jahre überprüft und erforderlichenfalls aktualisiert werden.

(41) Die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[36] gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[37] findet auf die Verarbeitung personenbezogener Daten durch zuständige Behörden für die Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung Anwendung. Die Verordnung (EU) 2018/1725 und die Richtlinie (EU) 2016/680 sollten an die mit der vorliegenden Verordnung eingeführten Änderungen der Verordnung (EU) 2016/679 angeglichen werden.

(42) Wie in Erwägungsgrund 5 der Verordnung (EU) 2018/1725 klargestellt, sollten in Fällen, in denen die Bestimmungen der Verordnung (EU) 2018/1725 denselben Grundsätzen folgen wie die Bestimmungen der Verordnung (EU) 2016/679, die Bestimmungen dieser Verordnungen nach der Rechtsprechung des Gerichtshofs der Europäischen Union einheitlich ausgelegt werden. Der Rahmen der Verordnung (EU) 2018/1725 sollte als gleichwertig mit dem Rahmen der Verordnung (EU) 2016/679 verstanden werden. Daher werden mit dieser Verordnung auch jene Bestimmungen der Verordnung (EU) 2018/1725 angepasst, die von den Änderungen der Verordnung (EU) 2016/679 betroffen sind, soweit letztere Änderungen auch im Zusammenhang mit der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union relevant sind.

(43) Um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu schaffen, sollten die erforderlichen Anpassungen der Richtlinie (EU) 2016/680 und aller anderen Rechtsakte der Union, die für eine solche Verarbeitung personenbezogener Daten gelten, im Anschluss an den Erlass dieser Verordnung erfolgen, damit sie so nah wie möglich am Geltungsbeginn der Änderungen der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 angewandt werden können.

(44) Die Speicherung personenbezogener Daten oder der Zugriff auf bereits in einer Endeinrichtung gespeicherte personenbezogene Daten und die anschließende Verarbeitung dieser Daten sollten in einem einzigen Rechtsrahmen, nämlich dem der Verordnung (EU) 2016/679, geregelt werden, wenn es sich bei dem Teilnehmer des elektronischen Kommunikationsdienstes oder dem Nutzer der Endeinrichtung um eine

---

[36] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

[37] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

natürliche Person handelt. Die in dieser Verordnung vorgeschlagenen Änderungen bieten weiterhin das höchste Schutzniveau für personenbezogene Daten und vereinfachen gleichzeitig die Modalitäten für betroffene Personen, ihre Rechte auszuüben und ihre Wahlentscheidungen im Internet auszudrücken. Die Änderungen betreffen insbesondere die Speicherung von Informationen in diesen Geräten, den Zugang zu oder die anderweitige Erhebung von Informationen aus diesen Geräten, was die Verarbeitung personenbezogener Daten durch Cookies oder ähnliche Technologien zur Gewinnung von Informationen aus den Endeinrichtungen mit sich bringt. Die einschlägigen Vorschriften sollten auch unabhängig davon gelten, ob die Endeinrichtung Eigentum der natürlichen Person oder einer anderen juristischen oder natürlichen Person ist.

Die Speicherung personenbezogener Daten oder der Zugang zu bereits in einer Endeinrichtung gespeicherten personenbezogenen Daten sollte weiterhin nur mit Einwilligung gestattet sein. Ähnlich wie bei der Richtlinie 2002/58/EG sollte diese Anforderung die Speicherung personenbezogener Daten oder den Zugang zu personenbezogenen Daten, die bereits in der Endeinrichtung einer natürlichen Person gespeichert sind, nicht ausschließen, wenn dies auf dem Unionsrecht oder dem Recht der Mitgliedstaaten im Sinne des Artikels 6 der Verordnung (EU) 2016/679 beruht und alle in dieser Bestimmung festgelegten Voraussetzungen für die Rechtmäßigkeit erfüllt und für die in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 festgelegten Ziele erfolgt.

Um den Aufwand für die Befolgung der Vorschriften zu verringern und Rechtsklarheit für die Verantwortlichen zu schaffen, und angesichts der Tatsache, dass bestimmte Verarbeitungszwecke ein geringes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen oder dass eine solche Verarbeitung erforderlich sein kann, um einen von der betroffenen Person verlangten Dienst zu erbringen, ist es erforderlich, eine erschöpfende Liste der Zwecke festzulegen, zu denen die Verarbeitung ohne Einwilligung zulässig sein sollte. In Bezug auf die Speicherung personenbezogener Daten oder den Zugriff auf personenbezogene Daten, die bereits in einer Endeinrichtung gespeichert sind, und deren anschließende Verarbeitung, die für diese Zwecke erforderlich ist, sollte diese Verordnung daher vorsehen, dass die Verarbeitung rechtmäßig ist. Der Verantwortliche, z. B. ein Mediendiensteanbieter, kann einen Auftragsverarbeiter, z. B. ein Marktforschungsunternehmen, beauftragen, die Verarbeitung in seinem Namen durchzuführen.

Auf die anschließende Verarbeitung personenbezogener Daten zu anderen als den in der erschöpfenden Liste festgelegten Zwecken sollten Artikel 6 und gegebenenfalls Artikel 9 der Verordnung (EU) 2016/679 angewandt werden. Es ist Sache des Verantwortlichen, unter Berücksichtigung des Grundsatzes der Rechenschaftspflicht die geeignete Rechtsgrundlage für die beabsichtigte Verarbeitung zu wählen. Um sich auf ein berechtigtes Interesse nach Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 als Grund für die anschließende Verarbeitung personenbezogener Daten berufen zu können, muss der Verantwortliche nachweisen, dass er die berechtigten Interessen des Verantwortlichen oder Dritter verfolgt, dass die Verarbeitung zur Erreichung des Zwecks dieses berechtigten Interesses erforderlich ist und dass die Interessen oder Grundrechte der betroffenen Person die von dem Verantwortlichen verfolgten Interessen nicht überwiegen. In diesem Zusammenhang sollten die Verantwortlichen die folgenden Elemente in größtmöglichem Umfang berücksichtigen: ob es sich bei der betroffenen Person um ein Kind handelt, die vernünftigen Erwartungen der betroffenen Person, die Auswirkungen auf den

Einzelnen aufgrund des Umfangs der verarbeiteten Daten oder der Sensibilität der verarbeiteten Daten, den Umfang der betreffenden Verarbeitung in dem Sinne, dass die Verarbeitung weder aufgrund ihrer Menge noch aufgrund der Bandbreite der Datenkategorien besonders umfassend sein kann, dass die Verarbeitung auf Daten beruhen sollte, die auf das erforderliche Maß beschränkt sind, und nicht auf der Überwachung großer Teile der Online-Aktivitäten der betroffenen Personen beruhen darf; gegebenenfalls andere relevante Faktoren. Die Verarbeitung sollte nicht zu einer kontinuierlichen Überwachung des Privatlebens der betroffenen Person führen.

Kann sich der Verantwortliche nicht auf ein berechtigtes Interesse als Rechtsgrundlage für die anschließende Verarbeitung berufen, so sollte die Verarbeitung auf einem anderen Grund nach Artikel 6 Absatz 1 beruhen, insbesondere auf der Einwilligung gemäß den Artikeln 6 und 7 der Verordnung (EU) 2016/679, sofern alle Grundsätze der Verordnung (EU) 2016/679 eingehalten werden.

(45) Betroffene Personen, die eine Einwilligungsanfrage abgelehnt haben, werden häufig jedes Mal, wenn sie den Online-Dienst desselben Verantwortlichen erneut besuchen, mit einer erneuten Einwilligungsanfrage konfrontiert. Dies kann nachteilige Folgen für die betroffenen Personen haben, die womöglich ihre Einwilligung nur deshalb erteilen, weil sie die wiederholten Einwilligungsanfragen vermeiden möchten. Der Verantwortliche sollte daher verpflichtet sein, die Wahlentscheidung der betroffenen Person, eine Einwilligungsanfrage abzulehnen, für mindestens einen bestimmten Zeitraum zu respektieren.

(46) Betroffene Personen sollten die Möglichkeit haben, sich auf automatisierte und maschinenlesbare Angaben zu ihren Wahlentscheidungen zu stützen, um in die Verarbeitung von Daten einzuwilligen, eine Einwilligungsanfrage abzulehnen oder der Verarbeitung zu widersprechen. Diese Mittel sollten dem Stand der Technik entsprechen. Sie können in den Einstellungen eines Webbrowsers oder in der europäischen Brieftasche für die digitale Identität (EUDI-Brieftasche) gemäß der Verordnung (EU) Nr. 910/2014 oder mit anderen geeigneten Mitteln implementiert werden. Die in dieser Verordnung festgelegten Vorschriften sollten die Entwicklung marktorientierter Lösungen mit geeigneten Schnittstellen unterstützen. Der Verantwortliche sollte verpflichtet sein, automatisierte und maschinenlesbare Angaben zu den Wahlentscheidungen der betroffenen Person zu beachten, sobald entsprechende Normen verfügbar sind. Angesichts der Bedeutung des unabhängigen Journalismus in einer demokratischen Gesellschaft und um die wirtschaftliche Grundlage dafür nicht zu untergraben, sollten Mediendiensteanbieter nicht verpflichtet sein, maschinenlesbare Angaben zu Wahlentscheidungen der betroffenen Nutzer bei der Datenverarbeitung zu befolgen. Die Verpflichtung der Anbieter von Webbrowsern, betroffenen Personen die technischen Mittel zur Verfügung zu stellen, damit sie Wahlentscheidungen in Bezug auf die Verarbeitung treffen können, sollte die Möglichkeit der Mediendiensteanbieter, die Einwilligung der betroffenen Personen einzuholen, nicht beeinträchtigen.

(47) Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation („Datenschutzrichtlinie für elektronische Kommunikation“), die zuletzt im Jahr 2009 überarbeitet wurde, bietet einen Rechtsrahmen für den Schutz des Rechts auf Privatsphäre, einschließlich der Vertraulichkeit der Kommunikation. Ferner präzisiert sie die Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung personenbezogener Daten im Zusammenhang mit elektronischen Kommunikationsdiensten. Sie schützt die Privatsphäre und die Integrität der Endeinrichtungen der Nutzer oder Teilnehmer, die

für diese Kommunikation verwendet werden. Die derzeitige Bestimmung des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG sollte weiterhin gelten, sofern es sich bei dem Teilnehmer oder Nutzer nicht um eine natürliche Person handelt und die gespeicherten oder abgerufenen Informationen keine Verarbeitung personenbezogener Daten darstellen oder zu einer solchen Verarbeitung führen.

(48) Artikel 4 der Richtlinie 2002/58/EG sollte aufgehoben werden. Artikel 4 der Richtlinie 2002/58/EG enthält Anforderungen an Betreiber öffentlich zugänglicher Kommunikationsdienste in Bezug auf die Gewährleistung der Sicherheit ihrer Dienste und Meldepflichten. In der Folge wurden mit der Richtlinie (EU) 2022/2555 neue Anforderungen an Risikomanagementmaßnahmen im Bereich der Cybersicherheit und Meldepflichten in Bezug auf Sicherheitsvorfälle für diese Betreiber festgelegt. Damit sich Verpflichtungen für Einrichtungen im Bereich der elektronischen Kommunikation möglichst nicht überschneiden, sollte Artikel 4 der Richtlinie 2002/58/EG aufgehoben werden. In Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten gemäß Artikel 4 Absätze 1 und 1a dieser Richtlinie und die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Artikel 4 Absätze 3 bis 5 der Richtlinie 2002/58/EG enthält die Verordnung (EU) 2016/679 bereits umfassende und aktuelle Vorschriften. Diese Vorschriften sollten daher für Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste und Anbieter öffentlicher Kommunikationsnetze gelten, wodurch sichergestellt wird, dass für die Verantwortlichen und die Auftragsverarbeiter eine einzige Regelung gilt.

(49) In mehreren horizontalen oder sektorspezifischen Rechtsakten der Union ist die Meldung desselben Ereignisses an verschiedene Behörden unter Verwendung unterschiedlicher technischer Mittel und Kanäle vorgeschrieben. Die zentrale Anlaufstelle zur Meldung von Vorfällen sollte es den Einrichtungen ermöglichen, ihren Meldepflichten gemäß der Richtlinie (EU) 2022/2555, der Verordnung (EU) 2016/679, der Verordnung (EU) 2022/2554, der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2022/2557 nachzukommen, indem sie Meldungen an eine einzige Schnittstelle übermitteln. Darüber hinaus sollte die zentrale Anlaufstelle den Einrichtungen die Möglichkeit geben, Informationen abzurufen, die sie zuvor über diese Anlaufstelle übermittelt haben, um ihnen dabei zu helfen, die Einhaltung ihrer Meldepflichten im Zusammenhang mit bestimmten Vorfällen zu verfolgen.

(50) Um die Sicherheit der zentralen Anlaufstelle zu gewährleisten, sollte die ENISA geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der zentralen Anlaufstelle und der über die zentrale Anlaufstelle übermittelten oder verbreiteten Informationen zu beherrschen. Bei der Bewertung des Risikos sowie der Angemessenheit und Verhältnismäßigkeit dieser Maßnahmen sollte die ENISA die Sensibilität der gemäß den einschlägigen Rechtsakten der Union übermittelten oder verbreiteten Informationen berücksichtigen. Die ENISA sollte bei der Ausarbeitung der technischen, operativen und organisatorischen Maßnahmen zur Einrichtung, Wartung und dem sicheren Betrieb der zentralen Anlaufstelle die nach den einschlägigen Rechtsakten der Union zuständigen Behörden konsultieren, indem sie auf bestehende Kooperationsgruppen und Netzwerke der Mitgliedstaaten zurückgreift, die im Rahmen dieser Rechtsakte eingerichtet wurden.

(51) Bevor die ENISA die Meldung von Vorfällen ermöglicht, sollte sie die Funktionsweise der zentralen Anlaufstelle testen, was eine gründliche Prüfung der Besonderheiten und Anforderungen an die Meldungen für die einschlägigen Rechtsakte der Union umfassen sollte. Auf der Grundlage der Ergebnisse des

Pilotprojekts sollte die Kommission das ordnungsgemäße Funktionieren, die Zuverlässigkeit, die Integrität und die Vertraulichkeit der zentralen Anlaufstelle bewerten. Die Kommission sollte das CSIRTs-Netzwerk und die nach den einschlägigen Rechtsakten der Union zuständigen Behörden konsultieren und sich zur Durchführung der Bewertung an bestehende Kooperationsgruppen und Netzwerke der Mitgliedstaaten wenden, die gemäß diesen Rechtsakten eingerichtet wurden. Stellt die Kommission fest, dass die zentrale Anlaufstelle das ordnungsgemäße Funktionieren, die Zuverlässigkeit, die Integrität und die Vertraulichkeit gewährleistet, sollte sie eine entsprechende Bekanntmachung im *Amtsblatt der Europäischen Union* veröffentlichen. Ist die Kommission der Auffassung, dass das ordnungsgemäße Funktionieren, die Zuverlässigkeit, die Integrität und die Vertraulichkeit nicht gewährleistet sind, sollte die ENISA alle erforderlichen Korrekturmaßnahmen ergreifen, gefolgt von einer Neubewertung durch die Kommission.

(52) Um die Kontinuität und die Interoperabilität mit bestehenden nationalen technischen Lösungen zu gewährleisten, die die Meldung von Vorfällen erleichtern, sollte die ENISA diese nationalen technischen Lösungen so weit wie möglich bei der Ausarbeitung der Spezifikationen für die technischen, operativen und organisatorischen Maßnahmen berücksichtigen, die für die Einrichtung, die Wartung und den sicheren Betrieb der zentralen Anlaufstelle erforderlich sind. Darüber hinaus sollte die ENISA technische Protokolle und Instrumente wie Anwendungsprogramm-Schnittstellen (API) und maschinenlesbare Standards in Betracht ziehen, die es Einrichtungen ermöglichen, Meldepflichten in Geschäftsprozesse zu integrieren, und Behörden, die zentrale Anlaufstelle mit ihren nationalen Meldesystemen zu verbinden.

(53) Um sicherzustellen, dass die zentrale Anlaufstelle es den betreffenden Einrichtungen ermöglicht, die Art der Informationen und das Format zu übermitteln, die nach den einschlägigen Rechtsakten der Union erforderlich sind, sollte die ENISA die Kommission und die gemäß diesen Rechtsakten zuständigen Behörden konsultieren. Ist ein Rechtsakt der Union in Bezug auf die Art der Informationen und das Format der Meldungen nicht vollständig harmonisiert, so sollten die Mitgliedstaaten die ENISA über ihre nationalen Bestimmungen unterrichten.

(54) Auf der Grundlage der Verordnung (EU) 2022/2554 hat der Finanzsektor bei der Umsetzung eines harmonisierten, umfassenden und wirksamen Rahmens, auch in Bezug auf die Meldung von Sicherheitsvorfällen, eine Vorreiterrolle gespielt. Um die Einhaltung der Vorschriften zu vereinfachen, ist es angezeigt, den mit der Verordnung (EU) 2022/2554 geschaffenen Rahmen für die Meldung von Vorfällen an die zentrale Anlaufstelle anzugleichen und gleichzeitig die Kontinuität und Stabilität des bestehenden Rahmens für solche Meldungen zu gewährleisten, wobei zu berücksichtigen ist, dass die zentrale Anlaufstelle erst nach Feststellung ihres ordnungsgemäßen Funktionierens, ihrer Zuverlässigkeit, Integrität und Vertraulichkeit betriebsbereit wäre. Darüber hinaus wurden mit der Verordnung (EU) 2022/2554 standardisierte Vorlagen für Meldungen eingeführt, um Inhalte von Meldungen schwerwiegender IKT-bezogener Vorfälle für den Finanzsektor zu vereinheitlichen. Die bei der Einführung dieser Vorlagen gewonnenen Erfahrungen liefern wertvolle Erkenntnisse und bewährte Verfahren, die bei der Festlegung der Art der Informationen, des Formats und des Verfahrens einer Meldung für die Zwecke der Meldung an die zentrale Anlaufstelle gemäß der Richtlinie (EU) 2022/2555, der Richtlinie (EU) 2022/2557 oder der Verordnung (EU) 2016/679 gegebenenfalls berücksichtigt werden sollten. Zu diesem Zweck sollte die Kommission die gemäß der Verordnung (EU) 2022/2554 erlassenen technischen Regulierungsstandards gebührend

berücksichtigen, in denen die Inhalte der Erstmeldung sowie der Zwischen- und Abschlussmeldungen schwerwiegender IKT-bezogener Vorfälle festgelegt sind. Dieser Ansatz zielt darauf ab, Kohärenz zu gewährleisten, Synergien zu fördern und den Verwaltungsaufwand für Unternehmen durch weniger von ihnen auszufüllende Datenfelder zu verringern, wodurch effizientere und einheitlichere, gestraffte Meldeverfahren erleichtert werden.

(55) Nach den einschlägigen Rechtsakten der Union müssen bestimmte vorfallsbezogene Informationen zu einem späteren Zeitpunkt zwischen den zuständigen Behörden ausgetauscht werden, um eine wirksame Beaufsichtigung und Koordinierung zu erleichtern. Daher sollte die zentrale Anlaufstelle so konzipiert sein, dass sie den Informationsaustausch auf dieser Ebene für jeden einschlägigen Rechtsakt der Union ermöglicht und unterstützt, wobei sicherzustellen ist, dass eine angemessen sichere, zeitnahe und effiziente Datenübermittlung zwischen den Behörden ermöglicht wird, falls die Mitgliedstaaten beschließen, diese zusätzliche Funktion zu nutzen.

(56) Um sicherzustellen, dass die Meldung von Vorfällen künftig über eine zentrale Anlaufstelle erfolgt, sollten die Richtlinie (EU) 2022/2555, die Verordnung (EU) 2016/679, die Verordnung (EU) 2022/2554, die Verordnung (EU) Nr. 910/2014 sowie die Richtlinie (EU) 2022/2557 daher entsprechend geändert werden. Die zentrale Anlaufstelle sollte innerhalb von 18 Monaten nach Inkrafttreten dieser Verordnung für die Zwecke der Meldungen im Rahmen dieser Rechtsakte genutzt werden können. Wenn die Kommission die Bekanntmachungsmechanismen einleitet und den Geltungsbeginn damit auf 24 Monate nach Inkrafttreten der Verordnung verschiebt, sollten die entsprechenden Bestimmungen der Richtlinie (EU) 2022/2555, der Verordnung (EU) Nr. 910/2014, der Verordnung (EU) 2022/2554 und der Richtlinie (EU) 2022/2557 für die Zwecke der Erfüllung der in den Bestimmungen festgelegten Meldepflichten weiterhin gelten.

(57) In dem außergewöhnlichen Fall, dass die Übermittlung von Meldungen über Vorfälle über die zentrale Anlaufstelle technisch nicht möglich ist, sollten die Einrichtungen ihren Meldepflichten auf alternative Weise nachkommen. Zu diesem Zweck sollten die Adressaten von Meldungen über Vorfälle nach den einschlägigen Rechtsakten der Union sicherstellen, dass sie in der Lage sind, solche Meldungen von Vorfällen auf alternative Weise zu erhalten und Angaben zu diesen alternativen Übermittlungsformen öffentlich zugänglich machen.

(58) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[38] angehört und hat am [DATUM] seine Stellungnahme abgegeben. Der Europäische Datenschutzausschuss wurde gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 konsultiert und hat am [DATUM] eine Stellungnahme abgegeben.

---

[38] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(59) Mit der Verordnung (EU) 2019/1150 werden gezielte verbindliche Vorschriften auf Unionsebene festgelegt, um für ein faires, vorhersehbares, tragfähiges und vertrauenswürdiges Online-Geschäftsumfeld im Binnenmarkt zu sorgen. Die Verordnung (EU) 2022/2065 und die Verordnung (EU) 2022/1925 bieten einen umfassenden Regelungsrahmen für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld für alle Endnutzer von Online-Diensten und schaffen gleiche Wettbewerbsbedingungen für Unternehmen auf digitalen Märkten. Im Interesse der Vereinfachung der Rechtsvorschriften der Union im Bereich der Online-Vermittlungsdienste und Online-Plattformen und angesichts der Tatsache, dass die Ziele und wesentlichen Bestimmungen der Verordnung über die Beziehungen zwischen Online-Plattformen und Unternehmen weitgehend durch das Gesetz über digitale Dienste und das Gesetz über digitale Märkte abgedeckt sind, sollte die Verordnung (EU) 2019/1050 aufgehoben werden. Die Verordnung (EU) 2022/2065 und die Verordnung (EU) 2022/1925 tragen zu einem vollständig harmonisierten Rechtsrahmen für digitale Dienste und digitale Märkte bei, indem sie die nationalen Maßnahmen in Bezug auf die Anforderungen an Anbieter von Vermittlungsdiensten und die Bestreitbarkeit und Fairness der von Torwächtern erbrachten zentralen Plattformdienste angleichen. Aus Gründen der Rechtssicherheit bleiben ausgewählte Begriffsbestimmungen in Artikel 2, die Bestimmungen über Einschränkungen und Aussetzungen in Artikel 4 sowie über das interne Beschwerdemanagementsystem in Artikel 11 der Verordnung (EU) 2019/1150, auf die in anderen Rechtsakten, insbesondere in der Richtlinie (EU) 2023/2831 zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit und in Artikel 15 zur Gewährleistung der Durchsetzung, verwiesen wird, vorübergehend in Kraft, bis die ursprünglichen Rechtsakte geändert worden sind.

(60) Angesichts des technischen Charakters der in dieser Verordnung vorgeschlagenen Änderungen und der Dringlichkeit, einen vereinfachten Rechtsrahmen zu schaffen, sollte diese Verordnung unmittelbar nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft treten. Gegebenenfalls sollten den Mitgliedstaaten und den beaufsichtigten Unternehmen Übergangsfristen für die Anpassung an die Vorschriften eingeräumt werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Änderungen der Verordnung (EU) 2023/2854

Die Verordnung (EU) 2023/2854 wird wie folgt geändert:

1. Artikel 1 wird wie folgt geändert:

a) In Absatz 1 werden folgende Buchstaben eingefügt:

„ea) die freiwillige Eintragung von Datenvermittlungsdiensten,

eb) die freiwillige Eintragung von Einrichtungen, die für altruistische Zwecke zur Verfügung gestellte Daten sammeln und verarbeiten,

ec) die Einsetzung eines Europäischen Dateninnovationsrats,

ed) Datenlokalisierungsauflagen und die Verfügbarkeit von Daten für die zuständigen Behörden,

ee) die Weiterverwendung bestimmter Daten und Dokumente, die sich im Besitz öffentlicher Stellen oder bestimmter öffentlicher Unternehmen befinden, sowie von Forschungsdaten,“.

b) In Absatz 2 werden folgende Buchstaben angefügt:

„g) Kapitel VIIa gilt für alle personenbezogenen und nicht-personenbezogenen Daten;

h) Kapitel VIIb gilt für alle nicht-personenbezogenen Daten;

i) Kapitel VIIc gilt für personenbezogene und nicht-personenbezogene Daten, d. h.:

i) Dokumente im Besitz öffentlicher Stellen der Mitgliedstaaten, auf die Bezug genommen wird

1) in Artikel 32i Absatz 1 Buchstabe a oder von öffentlichen Unternehmen, auf die Bezug genommen wird,

2) in Artikel 32i Absatz 1 Buchstaben b;

ii) Forschungsdaten gemäß Artikel 32i Absatz 1 Buchstabe c,

iii) bestimmte Kategorien geschützter Daten gemäß Artikel 32i Absatz 1 Buchstabe a.“

c) Absatz 3 Buchstabe g erhält folgende Fassung:

„g) Teilnehmer an Datenräumen.“

d) Absatz 7 wird gestrichen.

e) Folgende Absätze 11, 12 und 13 werden angefügt:

„(11) Kapitel VIIb dieser Verordnung lässt Rechts- und Verwaltungsvorschriften, die sich auf die innere Organisation der Mitgliedstaaten beziehen und die Übertragung von Befugnissen und Zuständigkeiten für die Datenverarbeitung zwischen Behörden und Einrichtungen des öffentlichen Rechts ohne vertragliche Vergütung unter Privatrechtssubjekten regeln, sowie Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die die Wahrnehmung dieser Befugnisse und Zuständigkeiten regeln, unberührt.

(12) Müssen öffentliche Stellen, Anbieter von Datenvermittlungsdiensten oder anerkannte Einrichtungen, die Datenaltruismus-Dienste erbringen, aufgrund sektorspezifischen Unionsrechts oder nationalen Rechts bestimmte zusätzliche technische, administrative oder organisatorische Anforderungen einhalten, die sich auf die Kapitel VIIa und VIIb beziehen, einschließlich durch Genehmigungs- oder Zertifizierungsverfahren, so finden auch diese Bestimmungen des sektorspezifischen Unionsrechts oder nationalen Rechts Anwendung. Etwaige spezifische zusätzliche Anforderungen müssen nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein.“

(13) In Bezug auf Daten und Dokumente, die in den Anwendungsbereich von Kapitel VIIc Abschnitt II fallen, berührt Kapitel VIIc dieser Verordnung nicht die Möglichkeit der Mitgliedstaaten, ausführlichere oder strengere Vorschriften zu erlassen, sofern diese Vorschriften eine umfassendere Weiterverwendung von Daten und Dokumenten ermöglichen.“

2. Artikel 2 wird wie folgt geändert:

a) Folgende Nummern 4a, 4b und 4c werden eingefügt:

„4a. ‚Einwilligung' eine Einwilligung im Sinne des Artikels 4 Nummer 11 der Verordnung (EU) 2016/679;

4b. ‚Erlaubnis' das Recht auf Verarbeitung nicht-personenbezogener Daten, das Datennutzern eingeräumt wird;

4c. ‚Zugang' die Datennutzung im Einklang mit bestimmten technischen, rechtlichen oder organisatorischen Anforderungen, ohne dass Daten hierzu zwingend übertragen oder heruntergeladen werden müssen;"

b) Nummer 13 erhält folgende Fassung:

„13. ‚Dateninhaber' eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen oder bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat;"

c) Folgende Nummern 28a und 28b werden eingefügt:

„28a. ‚Einrichtungen des öffentlichen Rechts' Einrichtungen mit sämtlichen der folgenden Merkmale:

a) Sie wurden zu dem besonderen Zweck gegründet, im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen;

b) sie besitzen Rechtspersönlichkeit,

c) sie werden überwiegend vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts finanziert, oder sie unterstehen hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften oder Einrichtungen, oder sie haben ein Verwaltungs-, Leitungs- beziehungsweise Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts ernannt worden sind;

28b. ‚öffentliches Unternehmen' ein Unternehmen, auf das eine öffentliche Stelle aufgrund ihres Eigentums, ihrer finanziellen Beteiligung oder der für das Unternehmen geltenden Bestimmungen unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben kann. Von einem beherrschenden Einfluss der öffentlichen Stellen ist in jedem der folgenden Fälle auszugehen, in denen diese Stellen unmittelbar oder mittelbar

a) die Mehrheit des gezeichneten Kapitals des Unternehmens besitzen, oder

b) über die Mehrheit der Stimmrechte verfügen, die mit den von dem Unternehmen ausgegebenen Anteilen verbunden sind, oder

c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des Unternehmens ernennen können;"

d) Folgende Nummern 38a und 38b werden eingefügt:

„38a. ‚Datenvermittlungsdienst' einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen wirtschaftlicher Natur zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern und Datennutzern hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen, und

1) dessen Hauptzweck nicht die Vermittlung urheberrechtlich geschützter Inhalte ist,

2) der nicht von mehreren juristischen Personen gemeinsam zur ausschließlichen Verwendung unter ihnen bereitgestellt wird;

38b. ‚Datenaltruismus' die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht-personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse;"

e) Folgende Nummern 44 bis 63 werden angefügt:

„44. ‚mittleres Unternehmen' ein mittleres Unternehmen im Sinne des Artikels 2 des Anhangs I der Empfehlung 2003/361/EG;

45. ‚kleines Midcap-Unternehmen' ein Unternehmen mit mittlerer Kapitalisierung im Sinne des Artikels 2 des Anhangs der Empfehlung (EU) 2025/1099 der Kommission;

46. ‚Hochschule' eine öffentliche Stelle, die postsekundäre Bildungsgänge anbietet, die zu einem akademischen Grad führen;

47. ‚Standardlizenz' eine Reihe vorgegebener Bedingungen für die Weiterverwendung, die in digitalem Format vorliegen und vorzugsweise mit standardisierten online verfügbaren öffentlichen Lizenzen kompatibel sind;

48. ‚Dokument':

a) alle Inhalte, die nicht-digital sind, unabhängig von der Form des Datenträgers (auf Papier oder als Ton-, Bild- oder audiovisuelle Aufzeichnung), oder

b) einen beliebigen Teil eines solchen Inhalts;

50. ‚dynamische Daten' Daten und Dokumente in digitaler Form, die häufig oder in Echtzeit aktualisiert werden, insbesondere aufgrund ihrer Volatilität oder ihres raschen Veraltens; von Sensoren generierte Daten werden in der Regel als dynamische Daten angesehen;

51. ‚Forschungsdaten' Daten, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden;

52. ‚Weiterverwendung' die Nutzung – durch natürliche oder juristische Personen – von Dokumenten, die im Besitz

a) öffentlicher Stellen sind, für gewerbliche oder nichtgewerbliche Zwecke, die sich von dem ursprünglichen Zweck im Rahmen des öffentlichen Auftrags, für den die Dokumente erstellt wurden, unterscheiden, abgesehen vom Austausch von Dokumenten zwischen öffentlichen Stellen ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags, oder

b) öffentlicher Unternehmen nach Kapitel VIIc Abschnitt 2 für gewerbliche oder nichtgewerbliche Zwecke sind, die sich von dem ursprünglichen Zweck der Erbringung von Dienstleistungen von allgemeinem Interesse, für den die Dokumente erstellt wurden, unterscheiden, abgesehen vom Austausch von Dokumenten zwischen öffentlichen Unternehmen und öffentlichen Stellen ausschließlich im Rahmen der Erfüllung des öffentlichen Auftrags öffentlicher Stellen;

53. ‚hochwertige Datensätze' Daten und Dokumente, deren Weiterverwendung mit wichtigen Vorteilen für die Gesellschaft, die Umwelt und die Wirtschaft verbunden ist, insbesondere aufgrund ihrer Eignung für die Schaffung von Mehrwertdiensten, von Anwendungen und neuer, hochwertiger und menschenwürdiger Arbeitsplätze sowie aufgrund der Zahl der potenziellen Nutznießer der Mehrwertdienste und -anwendungen auf der Grundlage dieser Daten und Dokumente;

54. ‚bestimmte Kategorien geschützter Daten' Daten und Dokumente im Besitz öffentlicher Stellen, die geschützt sind aus folgenden Gründen:

a) geschäftliche Geheimhaltung, einschließlich Betriebsgeheimnissen, Berufsgeheimnissen, Unternehmensgeheimnissen;

b) statistische Geheimhaltung,

c) Schutz geistigen Eigentums Dritter oder

d) Schutz personenbezogener Daten, soweit diese Daten nicht in den Anwendungsbereich von Abschnitt 2 Kapitel VIIc fallen;

56. ‚sichere Verarbeitungsumgebung' die physische oder virtuelle Umgebung und die organisatorischen Mittel, mit denen die Einhaltung der Anforderungen des Unionsrechts, insbesondere im Hinblick auf die Rechte der betroffenen Personen, die Rechte des geistigen Eigentums und die geschäftliche und statistische Vertraulichkeit, die Integrität und die Verfügbarkeit, sowie des geltenden nationalen Rechts gewährleistet wird und die es der Einrichtung, die die sichere Verarbeitungsumgebung bereitstellt, ermöglichen, alle Datenverarbeitungsvorgänge zu bestimmen und zu beaufsichtigen, darunter

auch das Anzeigen, Speichern, Herunterladen und Exportieren von Daten und das Berechnen abgeleiteter Daten mithilfe von Rechenalgorithmen;

57. ‚Weiterverwender' eine natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten oder Dokumenten, die sich im Besitz einer öffentlichen Stelle oder eines öffentlichen Unternehmens befinden, gemäß Kapitel VIIc oder von Forschungsdaten oder bestimmten Kategorien geschützter Daten gewährt wurde;

58. ‚maschinenlesbares Format' ein Dateiformat, das so strukturiert ist, dass Softwareanwendungen konkrete Daten, einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur, leicht identifizieren, erkennen und extrahieren können;

59. ‚offenes Format' ein Dateiformat, das plattformunabhängig ist und der Öffentlichkeit ohne Einschränkungen, die der Weiterverwendung von Dokumenten hinderlich wären, zugänglich gemacht wird;

60 ‚formeller, offener Standard' einen schriftlich niedergelegten Standard, in dem die Anforderungen für die Sicherstellung der Interoperabilität der Software niedergelegt sind;

61. ‚angemessene Gewinnspanne' einen Prozentsatz der Gesamtkosten, der über den zur Deckung der einschlägigen Kosten erforderlichen Betrag hinausgeht, aber höchstens fünf Prozentpunkte über dem von der EZB festgesetzten Zinssatz liegt;

62. ‚Datenlokalisierungsauflage' eine Verpflichtung, ein Verbot, eine Bedingung, eine Beschränkung oder eine andere Anforderung, die in Rechts- oder Verwaltungsvorschriften eines Mitgliedstaats enthalten ist oder sich aus allgemeinen und einheitlichen Verwaltungspraktiken in einem Mitgliedstaat und Einrichtungen des öffentlichen Rechts, unbeschadet der Richtlinie 2014/24/EU auch im Bereich der Vergabe öffentlicher Aufträge, ergibt und die bestimmt, dass die Datenverarbeitung im Hoheitsgebiet eines bestimmten Mitgliedstaats stattfinden muss, oder die die Verarbeitung von Daten in einem anderen Mitgliedstaat behindert;

63. ‚Pseudonymisierung' eine Pseudonymisierung im Sinne von Artikel 4 Nummer 5 der Verordnung (EU) 2016/679."

3. Artikel 4 Absatz 8 erhält folgende Fassung:

„(8) Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Dritten gemäß Absatz 6 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird, oder dass die Offenlegung von Geschäftsgeheimnissen gegenüber dem Nutzer ein hohes Risiko des rechtswidrigen Erwerbs oder der rechtswidrigen Nutzung oder Offenlegung gegenüber Einrichtungen aus Drittländern oder in der Union niedergelassenen Einrichtungen, die unter der direkten oder indirekten Kontrolle solcher Einrichtungen stehen und Rechtsordnungen unterliegen, die einen schwächeren oder nicht gleichwertigen Schutz im Vergleich zu dem nach Unionsrecht bieten, birgt, kann er das Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, wie der Durchsetzbarkeit des Schutzes von

Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen. Er ist dem Nutzer unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.“

4. Artikel 5 Absatz 11 erhält folgende Fassung:

„(11) Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Dritten gemäß Absatz 9 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird, oder dass die Offenlegung von Geschäftsgeheimnissen gegenüber dem Nutzer ein hohes Risiko des rechtswidrigen Erwerbs oder der rechtswidrigen Nutzung oder Offenlegung gegenüber Einrichtungen aus Drittländern oder in der Union niedergelassenen Einrichtungen, die unter der direkten oder indirekten Kontrolle solcher Einrichtungen stehen und Rechtsordnungen unterliegen, die einen schwächeren oder nicht gleichwertigen Schutz im Vergleich zu dem nach Unionsrecht bieten, birgt, kann er das Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, wie der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen. Er ist dem Dritten unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.“

5. Die Überschrift des Kapitels V erhält folgende Fassung:

„BEREITSTELLUNG VON DATEN FÜR ÖFFENTLICHE STELLEN, DIE KOMMISSION, DIE EUROPÄISCHE ZENTRALBANK UND EINRICHTUNGEN DER UNION AUFGRUND EINES ÖFFENTLICHEN NOTSTANDS“

6. Die Artikel 14 und 15 werden gestrichen.

7. Folgender Artikel 15a wird eingefügt:

„Artikel 15a

Verpflichtung der Dateninhaber zur Bereitstellung von Daten aufgrund eines öffentlichen Notstands

(1) Weist eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union nach, dass eine außergewöhnliche Notwendigkeit besteht, bestimmte Daten zur Wahrnehmung ihrer gesetzlichen Aufgaben im öffentlichen Interesse zu nutzen, um auf einen öffentlichen Notstand zu reagieren, ihn abzumildern oder die Erholung nach einem öffentlichen Notstand zu unterstützen, so kann sie von Dateninhabern, bei denen es sich um juristische Personen handelt, die keine öffentlichen Stellen sind, verlangen, diese Daten, einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen Metadaten, zur Verfügung zu stellen. Auf ein solches hinreichend begründetes Verlangen stellen die Dateninhaber der verlangenden öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der Einrichtung der Union die

entsprechenden Daten und Metadaten zur Verfügung. Solche Verlangen können auch gestellt werden, wenn die Erstellung amtlicher Statistiken im Zusammenhang mit einem öffentlichen Notstand erforderlich ist.

(2) Sind die verlangten Daten zur Bewältigung eines öffentlichen Notstands erforderlich und ist die verlangende Stelle gemäß Absatz 1 nicht in der Lage, diese Daten auf andere Weise rechtzeitig und wirksam unter gleichwertigen Bedingungen zu erhalten, so darf das Verlangen nur nicht-personenbezogene Daten betreffen. Reicht die Bereitstellung nicht-personenbezogener Daten nicht aus, um den öffentlichen Notstand zu bewältigen, so können auch personenbezogene Daten vorbehaltlich geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung ihres Schutzes verlangt und nach Möglichkeit in pseudonymisierter Form zur Verfügung gestellt werden.

(3) Sind die verlangten Daten erforderlich, um die Auswirkungen eines öffentlichen Notstands abzumildern oder die Erholung nach einem öffentlichen Notstand zu unterstützen, so kann eine nach Absatz 1 verlangende Stelle, die auf der Grundlage des Unionsrechts oder des nationalen Rechts handelt, spezifische nicht-personenbezogene Daten verlangen, deren Fehlen sie daran hindert, die Auswirkungen eines öffentlichen Notstands zu abzumildern oder die Erholung nach einem öffentlichen Notstand zu unterstützen. Solche Verlangen werden nicht an Kleinst- und Kleinunternehmen gerichtet.“

8. Artikel 16 Absatz 2 erhält folgende Fassung:

„(2) Dieses Kapitel gilt nicht für Tätigkeiten öffentlicher Stellen, der Kommission, der Europäische Zentralbank und von Einrichtungen der Union in Bezug auf Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder die Strafvollstreckung oder die Zoll- oder Steuerverwaltung. Dieses Kapitel berührt nicht das für solche Tätigkeiten geltende Unionsrecht oder nationale Recht.“

9. Artikel 17 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

i) Der einleitende Teil erhält folgende Fassung:

„Öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union müssen in ihren Datenverlangen nach Artikel 15a“.

ii) Die Buchstaben b und c erhalten folgende Fassung:

„b) nachweisen, dass die Bedingungen für ein Verlangen nach Artikel 15a erfüllt sind;

c) den Zweck des Verlangens, die beabsichtigte Nutzung der verlangten Daten. gegebenenfalls auch durch einen Dritten gemäß Absatz 4, und die Dauer dieser Nutzung sowie gegebenenfalls die Art und Weise erläutern, wie die Verarbeitung personenbezogener Daten dem öffentlichen Notstand abhelfen soll;“

b) Absatz 2 wird wie folgt geändert:

i) Buchstabe c erhält folgende Fassung:

„c) im Hinblick auf den öffentlichen Notstand und den Umfang der verlangten Daten sowie die Häufigkeit des Zugangs zu den verlangten

Daten in einem angemessenen Verhältnis zu der außergewöhnlichen Notwendigkeit stehen und ausreichend begründet sein;“

ii) Buchstabe e wird gestrichen;

c) Die Absätze 5 und 6 werden gestrichen.

10. Artikel 18 wird wie folgt geändert:

a) In Absatz 2 erhält der einführende Wortlaut folgende Fassung:

„(2) Unbeschadet besonderer Erfordernisse bezüglich der Verfügbarkeit von Daten, die im Unionsrecht oder in nationalem Recht festgelegt sind, kann ein Dateninhaber Datenzugangsverlangen im Sinne dieses Kapitels unverzüglich und in jedem Fall innerhalb von fünf Arbeitstagen nach Eingang eines Datenverlangens gemäß Artikel 15a Absatz 2 sowie in anderen Fällen unverzüglich und in jedem Fall innerhalb von 30 Arbeitstagen nach Eingang eines Datenverlangens gemäß Artikel 15a Absatz 3 aus einem der folgenden Gründe ablehnen oder deren Änderung beantragen:“

b) Absatz 5 wird gestrichen.

11. Artikel 19 wird wie folgt geändert:

a) In Absatz 1 erhält der einführende Wortlaut folgende Fassung:

„Eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union, die Daten aufgrund eines Verlangens nach Artikel 15a erhalten hat,“

b) Absatz 3 erhält folgende Fassung:

„(3) Die Offenlegung von Geschäftsgeheimnissen gegenüber einer öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union gilt nur in dem Maße als erforderlich, in dem dies für den Zweck eines Verlangens gemäß Artikel 15a unerlässlich ist. In diesem Fall muss der Dateninhaber oder, falls es sich dabei nicht um dieselbe Person handelt, der Inhaber des Geschäftsgeheimnisses die Daten, die als Geschäftsgeheimnisse geschützt sind, einschließlich der einschlägigen Metadaten, identifizieren. Die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union treffen vor der Offenlegung von Geschäftsgeheimnissen alle erforderlichen und geeigneten technischen und organisatorischen Maßnahmen, um die Vertraulichkeit der Geschäftsgeheimnisse zu wahren, gegebenenfalls einschließlich der Verwendung von Mustervertragsbestimmungen, technischen Normen und der Anwendung von Verhaltenskodizes.“

12. Artikel 20 erhält folgende Fassung:

„Artikel 20

Gegenleistung für die Bereitstellung von Daten gemäß Kapitel V

(1) Dateninhaber stellen die zur Bewältigung eines öffentlichen Notstands nach Artikel 15a Absatz 2 erforderlichen Daten unentgeltlich bereit. Die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union, die die Daten erhalten haben, erkennen den Beitrag des Dateninhabers auf dessen Ersuchen hin öffentlich an.

(2) Der Dateninhaber hat Anspruch auf eine faire Gegenleistung für die Bereitstellung von Daten im Einklang mit einem Verlangen gemäß Artikel 15a Absatz 3. Diese Gegenleistung deckt mindestens die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, gegebenenfalls einschließlich der Kosten einer Anonymisierung, Pseudonymisierung, Aggregation und technischen Anpassung, und einer angemessenen Marge. Auf Verlangen der öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der Einrichtung der Union übermittelt der Dateninhaber Informationen über die Grundlage der Kostenberechnung und die angemessene Marge.

(3) Abweichend von Absatz 1 kann ein Dateninhaber, bei dem es sich um ein Kleinst- oder Kleinunternehmen handelt, für die Bereitstellung von Daten auf ein Verlangen gemäß Artikel 15a Absatz 2 unter den in Absatz 2 des vorliegenden Artikels festgelegten Bedingungen eine Gegenleistung verlangen.

(4) Dateninhaber haben kein Recht auf Gegenleistung für die Bereitstellung von Daten zur Erfüllung eines Verlangens gemäß Artikel 15a Absatz 3, falls die besondere Aufgabe im öffentlichen Interesse zur Erstellung amtlicher Statistiken durchgeführt wird und der Erwerb von Daten nach nationalem Recht nicht zulässig ist. Die Mitgliedstaaten unterrichten die Kommission, wenn der Erwerb von Daten für die Erstellung amtlicher Statistiken nach nationalem Recht nicht zulässig ist.“

13. Artikel 21 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„**Weitergabe von im Zusammenhang mit einem öffentlichen Notstand erhaltenen Daten an Forschungseinrichtungen oder statistische Ämter**“

b) Absatz 5 erhält folgende Fassung:

„(5) Beabsichtigt eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union, Daten gemäß Absatz 1 zu übermitteln oder bereitzustellen, so teilt sie dies dem Dateninhaber, von dem die Daten empfangen wurden, unverzüglich mit, unter Angabe

a) der Identität und der Kontaktdaten der die Daten empfangenden Organisation oder Einzelperson,

b) des Zwecks der Übermittlung oder Bereitstellung der Daten,

c) des Zeitraums, für den die Daten verwendet werden sollen, und der getroffenen technischen Schutzmaßnahmen,

d) der organisatorischen Maßnahmen, auch wenn personenbezogene Daten oder Geschäftsgeheimnisse betroffen sind.“

14. Folgender Artikel 22a wird vor Kapitel VI eingefügt:

„Artikel 22a

Beschwerderecht

Bei Streitigkeiten über ein Datenverlangen nach Artikel 15a, die dessen Ablehnung, Änderung, die Höhe der Gegenleistung oder die Übermittlung oder Bereitstellung von Daten betreffen, kann der Dateninhaber, die öffentliche

Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union bei der gemäß Artikel 37 benannten zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, Beschwerde einlegen.“

15. In Artikel 31 werden die folgenden Absätze 1a und 1b eingefügt:

„(1a) Die in Kapitel VI – mit Ausnahme des Artikels 29 – und in Artikel 34 festgelegten Pflichten gelten nicht für andere als die in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienste, bei denen die meisten Merkmale und Funktionen des Datenverarbeitungsdienstes vom Anbieter an die spezifischen Bedürfnisse des Kunden angepasst wurden, wenn die Erbringung dieser Dienste auf einem Vertrag beruht, der vor dem oder am 12. September 2025 geschlossen wurde.

Der Anbieter solcher Datenverarbeitungsdienste ist nicht verpflichtet, einen Vertrag über die Erbringung dieser Dienste vor dessen Ablauf neu auszuhandeln oder zu ändern, wenn dieser Vertrag vor dem oder am 12. September 2025 geschlossen wurde. Jede Vertragsklausel, die im Widerspruch zu Artikel 29 Absätze 1, 2 oder 3 steht, ist als nichtig anzusehen.

(1b) Ein Anbieter von Datenverarbeitungsdiensten kann in einen befristeten Vertrag über die Erbringung anderer als der in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienste Bestimmungen über verhältnismäßige Sanktionen bei vorzeitiger Kündigung aufnehmen.

Handelt es sich bei dem Anbieter von Datenverarbeitungsdiensten um ein kleines und mittleres Unternehmen oder ein kleines Midcap-Unternehmen, so gelten die in Kapitel VI – mit Ausnahme des Artikels 29 – und in Artikel 34 festgelegten Verpflichtungen nicht für andere als die in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienste, wenn die Erbringung dieser Dienste auf einem Vertrag beruht, der vor dem oder am 12. September 2025 geschlossen wurde.

Handelt es sich bei dem Anbieter eines Datenverarbeitungsdienstes um ein kleines und mittleres Unternehmen oder ein kleines Midcap-Unternehmen, so ist der Anbieter nicht verpflichtet, einen Vertrag über die Erbringung eines anderen als der in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienstes vor dessen Ablauf neu auszuhandeln oder zu ändern, wenn dieser Vertrag vor dem oder am 12. September 2025 geschlossen wurde. Jede vertragliche Bestimmung in diesem Vertrag, die im Widerspruch zu Artikel 29 Absätze 1, 2 oder 3 steht, ist als nichtig anzusehen.“

16. Artikel 32 wird wie folgt geändert:

a) Die Absätze 1 und 2 erhalten folgende Fassung:

„(1) Anbieter von Datenverarbeitungsdiensten, die öffentliche Stelle, die Daten oder Dokumente gemäß Kapitel VIIc Abschnitt 3 zur Verfügung stellt, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten oder Dokumenten gemäß Kapitel VIIc Abschnitt 3 gewährt wurde, ein Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation ergreifen unbeschadet der Absätze 2 oder 3 alle angemessenen technischen, organisatorischen und rechtlichen Maßnahmen, einschließlich Verträgen, um den staatlichen Zugang zu in der Union gespeicherten nicht-personenbezogenen Daten auf internationaler Ebene und in

Drittländern sowie deren Übermittlung zu verhindern, wenn eine solche Übermittlung oder ein solcher Zugang im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde.

(2) Entscheidungen und Urteile eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Anbieter von Datenverarbeitungsdiensten, einer öffentlichen Stelle, die Daten oder Dokumente gemäß Kapitel VIIc Abschnitt 3 bereitstellt, einer natürlichen oder juristischen Person, der das Recht auf Weiterverwendung von Daten oder Dokumenten gemäß Kapitel VIIc Absatz 3 gewährt wurde, einem Anbieter von Datenvermittlungsdiensten oder einer anerkannten datenaltruistischen Organisationen die Übertragung von in der Union gespeicherten nicht-personenbezogenen Daten im Anwendungsbereich dieser Verordnung oder der Zugang zu diesen Daten in der Union verlangt wird, werden nur dann anerkannt oder vollstreckbar, wenn sie auf eine in Kraft befindliche völkerrechtliche Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder auf eine solche Vereinbarung zwischen dem ersuchenden Drittland und einem Mitgliedstaat gestützt sind.“

b) In Absatz 3 Unterabsatz 1 erhält der Einleitungssatz folgende Fassung:

„(3) Wenn keine völkerrechtliche Übereinkunft gemäß Absatz 2 besteht und eine Entscheidung oder ein Urteil eines Gerichts eines Drittlandes oder eine Entscheidung einer Verwaltungsbehörde eines Drittlands, mit der die Übertragung nicht-personenbezogener Daten im Anwendungsbereich dieser Verordnung aus der Union oder der Zugang zu diesen Daten in der Union verlangt wird, an einen Anbieter von Datenverarbeitungsdiensten, an eine öffentliche Stelle, die Daten oder Dokumente gemäß Kapitel VIIc Abschnitt 3 bereitstellt, an eine natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten oder Dokumenten gemäß Kapitel VIIc Abschnitt 3 gewährt wurde, an einen Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation gerichtet ist und die Befolgung einer solchen Entscheidung oder eines solchen Gerichtsurteils den Adressaten in Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats bringen würde, erfolgt die Übertragung dieser Daten an die Behörde des Drittlands oder die entsprechende Zugangsgewährung nur dann, wenn“

c) Die Absätze 4 und 5 erhalten folgende Fassung:

„(4) Sind die in Absatz 2 oder 3 festgelegten Voraussetzungen erfüllt, so stellt der Anbieter von Datenverarbeitungsdiensten, die öffentliche Stelle, die Daten oder Dokumente gemäß Kapitel VIIc Abschnitt 3 bereitstellt, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten oder Dokumenten gemäß Kapitel VIIc Abschnitt 3 gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation die Mindestmenge an Daten bereit, die auf der Grundlage einer angemessenen Auslegung dieses Verlangens durch den Anbieter oder die in Absatz 3 Unterabsatz 2 genannte einschlägige nationale Stelle oder Behörde als Reaktion auf das Verlangen zulässig ist.

(5) Der Anbieter von Datenverarbeitungsdiensten, die öffentliche Stelle, die Daten oder Dokumente gemäß Kapitel VIIc Abschnitt 3 bereitstellt, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von

Daten oder Dokumenten gemäß Kapitel VIIc Abschnitt 3 gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation teilt der natürlichen oder juristischen Person, deren Rechte und Interessen beeinträchtigt werden könnten, mit, dass für ihre Daten ein Datenzugangsverlangen einer Behörde eines Drittlands vorliegt, bevor er das Verlangen erfüllt, außer in Fällen, in denen das Verlangen Strafverfolgungszwecken dient und solange zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahmen erforderlich.“

17. Artikel 36 wird gestrichen.

18. Folgende Kapitel VIIa, VIIb und VIIc werden eingefügt:

„**KAPITEL VIIa**
DATENVERMITTLUNGSDIENSTE UND DATENALTRUISTISCHE ORGANISATIONEN

Artikel 32a

Öffentliche Unionsregister

(1) Die Kommission führt und aktualisiert regelmäßig öffentliche Unionsregister von

a) anerkannten Anbietern von Datenvermittlungsdiensten und

b) anerkannten datenaltruistischen Organisationen.

(2) Anbieter von Datenvermittlungsdiensten, die im öffentlichen Unionsregister gemäß Absatz 1 Buchstabe a eingetragen sind, dürfen in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannter Anbieter von Datenvermittlungsdiensten“ sowie ein gemeinsames Logo gemäß Absatz 4 verwenden.

(3) Datenaltruistische Organisationen, die in dem in Absatz 1 Buchstabe b genannten öffentlichen Unionsregister eingetragen sind, dürfen in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ sowie das in Absatz 4 genannte gemeinsame Logo verwenden.

(4) Damit in der Union anerkannte Anbieter von Datenvermittlungsdiensten in der gesamten Union leicht erkennbar sind, wird der Kommission die Befugnis übertragen, im Wege von Durchführungsrechtsakten die Ausgestaltung eines gemeinsamen Logos festzulegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 46 Absatz 1a genannten Beratungsverfahren erlassen.

Artikel 32b

Für die Registrierung von Anbietern von Datenvermittlungsdiensten und datenaltruistischen Organisationen zuständige Behörden

(1) Jeder Mitgliedstaat benennt mindestens eine Stelle, die für die Umsetzung und Durchsetzung dieses Kapitels gemäß Artikel 37 Absatz 1 auf nationaler Ebene zuständig ist.

(2) Die zuständigen Behörden werden so eingerichtet, dass ihre Unabhängigkeit von anerkannten Anbietern von Datenvermittlungsdiensten oder anerkannten datenaltruistischen Organisationen gewährleistet ist.

Artikel 32c

Allgemeine Anforderungen an die Registrierung anerkannter Anbieter von Datenvermittlungsdiensten

Um in das in Artikel 32a Absatz 1 Buchstabe a genannte öffentliche Unionsregister eingetragen zu werden, muss der Anbieter von Datenvermittlungsdiensten alle folgenden Anforderungen erfüllen:

a) er verwendet die Daten, für die er Datenvermittlungsdienste erbringt, nicht für andere Zwecke, als um sie den Datennutzern zur Verfügung zu stellen;

b) er verwendet die Daten, die er in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zur Erbringung des Datenvermittlungsdienstes erhebt, einschließlich Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Datenvermittlungsdienst nutzenden Person hergestellt werden, nur für die Entwicklung dieses Datenvermittlungsdienstes;

c) wenn er Dateninhabern oder betroffenen Personen zusätzliche Instrumente und Dienste zum spezifischen Zweck der Erleichterung des Datenaustauschs wie Zwischenspeicherung, Aufbereitung, Umwandlung, Verschlüsselung, Anonymisierung und Pseudonymisierung anbietet, so dürfen diese Instrumente und Dienste nur auf ausdrückliche Veranlassung oder mit ausdrücklicher Zustimmung des Dateninhabers oder der betroffenen Person verwendet werden;

d) wenn Anbieter von Datenvermittlungsdiensten, bei denen es sich nicht um Kleinst- oder Kleinunternehmen handelt, ihren Kunden andere Mehrwertdienste als die unter Buchstabe c genannten Dienste anbieten, müssen sie die folgenden Voraussetzungen erfüllen:

   i) die Mehrwertdienste werden vom Nutzer ausdrücklich verlangt,

   ii) die Daten werden nicht für andere Zwecke als die Erbringung des Mehrwertdienstes verwendet,

   iii) die Mehrwertdienste werden über eine funktional getrennte Stelle angeboten,

   iv) das Unternehmen, das die Mehrwertdienste anbieten möchte, ist nicht als Torwächter gemäß Artikel 3 der Verordnung (EU) 2022/1925 benannt,

   v) die kommerziellen Bedingungen, einschließlich der Preisgestaltung, für die Erbringung von Datenvermittlungsdiensten für einen Dateninhaber oder Datennutzer sind nicht davon abhängig, ob der Dateninhaber oder Datennutzer andere Mehrwertdienste desselben Anbieters von Datenvermittlungsdiensten oder eines verbundenen Unternehmens nutzt;

e) der Anbieter von Datenvermittlungsdiensten, der Dienste für betroffene Personen anbietet, handelt bei der Erleichterung der Rechteausübung durch die betroffenen Personen im besten Interesse der betroffenen Personen; insbesondere informiert und – soweit erforderlich – berät er betroffene Personen in prägnanter, transparenter, verständlicher und leicht zugänglicher Weise über die beabsichtigte Nutzung der Daten durch Datennutzer und die üblichen Geschäftsbedingungen für solche Nutzungen, bevor die betroffenen Personen ihre Einwilligung erteilen.

Artikel 32d

Allgemeine Anforderungen an die Registrierung anerkannter datenaltruistischer Organisationen

Um in das öffentliche Unionsregister gemäß Artikel 32a Absatz 1 Buchstabe b eingetragen zu werden, muss eine datenaltruistische Organisation alle folgenden Anforderungen erfüllen:

a) sie führt datenaltruistische Tätigkeiten durch,

b) sie hat gemäß nationalem Recht Rechtspersönlichkeit, um gegebenenfalls gemäß dem nationalen Recht Ziele von allgemeinem Interesse zu erreichen,

c) sie ist selbst ohne Erwerbszweck tätig und rechtlich unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln,

d) sie übt die Datenaltruismus-Tätigkeiten über eine Struktur aus, die von ihren anderen Tätigkeiten funktionell getrennt ist.

Artikel 32e

Eintragung

(1) Anbieter von Datenvermittlungsdiensten, die die Anforderungen des Artikels 32c erfüllen, können bei der in Artikel 32b genannten zuständigen Behörde des Mitgliedstaats, in dem sie ihre Hauptniederlassung haben, einen Antrag auf Eintragung in das öffentliche Unionsregister der anerkannten Anbieter von Datenvermittlungsdiensten stellen.

Datenaltruistische Organisationen, die die Anforderungen des Artikels 32d erfüllen, können bei der in Artikel 32b genannten zuständigen Behörde des Mitgliedstaats, in dem sie ihre Hauptniederlassung haben, einen Antrag auf Eintragung in das öffentliche Unionsregister der anerkannten datenaltruistischen Organisationen stellen.

(2) Anbieter von Datenvermittlungsdiensten und datenaltruistische Organisationen, die keine Hauptniederlassung in der Union haben, benennen einen gesetzlichen Vertreter in einem der Mitgliedstaaten. Der gesetzliche Vertreter wird beauftragt, zusätzlich oder anstelle des Anbieters von Datenvermittlungsdiensten oder der datenaltruistischen Organisation als Anlaufstelle für zuständige Behörden oder betroffene Personen und Dateninhaber zu dienen. Der gesetzliche Vertreter arbeitet mit der zuständigen Behörde zusammen und legt ihr auf Verlangen umfassend dar, welche Maßnahmen und Vorkehrungen der Anbieter von Datenvermittlungsdiensten bzw. die datenaltruistische Organisation getroffen hat, um die Einhaltung dieser Verordnung sicherzustellen.

Der Anbieter von Datenvermittlungsdiensten bzw. die datenaltruistische Organisation unterliegt der rechtlichen Zuständigkeit des Mitgliedstaats, in dem sich der gesetzliche Vertreter befindet. Die Benennung eines gesetzlichen Vertreters erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Anbieter von Datenvermittlungsdiensten bzw. die datenaltruistische Organisation.

(3) Die zuständigen Behörden erstellen die erforderlichen Antragsformulare.

(4) Hat ein Anbieter von Datenvermittlungsdiensten alle erforderlichen Informationen gemäß Absatz 3 des vorliegenden Artikels vorgelegt und erfüllt er die Anforderungen des Artikels 32c, so entscheidet die zuständige Behörde innerhalb von 12 Wochen nach Eingang des Antrags auf Eintragung, ob der Anbieter die in

Artikel 32c festgelegten Kriterien erfüllt. Erfüllt der Anbieter die Kriterien, so übermittelt die zuständige Behörde die einschlägigen Informationen der Kommission, die sodann die Anbieter in das öffentliche Unionsregister als anerkannten Anbieter von Datenvermittlungsdiensten einträgt.

Unterabsatz 1 gilt auch, wenn eine datenaltruistische Organisation alle erforderlichen Informationen gemäß Absatz 2 vorgelegt hat und die Eintragungsanforderungen gemäß Artikel 32d erfüllt.

Die Eintragung in das öffentliche Unionsregister ist in allen Mitgliedstaaten gültig.

(5) Die zuständige Behörde kann nach Maßgabe des nationalen Rechts Gebühren für die Eintragung erheben. Diese Gebühren müssen verhältnismäßig und objektiv sein und auf den Verwaltungskosten im Zusammenhang mit der Überwachung der Einhaltung beruhen. Bei kleinen Midcap-Unternehmen, kleinen und mittleren Unternehmen und Start-up-Unternehmen kann die zuständige Behörde eine ermäßigte Gebühr erheben oder auf die Gebühr verzichten.

(6) Eingetragene Einrichtungen melden der zuständigen Behörde alle späteren Änderungen der Informationen, die während des Antragsverfahrens bereitgestellt wurden, oder wenn sie ihre Datenvermittlungs- oder Datenaltruismus-Tätigkeiten in der Union einstellen.

(7) Die zuständige Behörde unterrichtet die Kommission unverzüglich auf elektronischem Wege über jede Mitteilung gemäß Absatz 6. Die Kommission aktualisiert das öffentliche Unionsregister unverzüglich.

Artikel 32f

Pflichten anerkannter datenaltruistischer Organisationen

(1) Anerkannte datenaltruistische Organisationen informieren betroffene Personen oder Dateninhaber vor der Verarbeitung ihrer Daten auf klare und leicht verständliche Weise über Folgendes:

a) die Ziele von allgemeinem Interesse und gegebenenfalls den angegebenen, ausdrücklichen und rechtmäßigen Zweck der Verarbeitung personenbezogener Daten, für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt;

b) den Standort der Verarbeitung und die Ziele von allgemeinem Interesse, für die sie eine etwaige Verarbeitung in einem Drittland erlaubt, sofern die Verarbeitung von der anerkannten datenaltruistischen Organisation vorgenommen wird.

(2) Anerkannte datenaltruistische Organisationen verwenden die Daten nicht für andere als die Ziele von allgemeinem Interesse, für die die betroffene Person oder der Dateninhaber die Verarbeitung erlaubt hat. Die anerkannte datenaltruistische Organisation darf keine irreführenden Vermarktungspraktiken verwenden, um Daten zu erhalten.

(3) Anerkannte datenaltruistische Organisationen stellen elektronische Mittel für die Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten sowie für deren Widerruf bereit.

(4) Anerkannte datenaltruistische Organisationen unterrichten Dateninhaber im Falle einer unbefugten Übertragung, des unbefugten Zugriffs oder der unbefugten Nutzung der von ihnen geteilten nicht-personenbezogenen Daten unverzüglich.

(5) Ermöglichen anerkannte datenaltruistische Organisationen die Datenverarbeitung durch Dritte, einschließlich durch die Bereitstellung von Werkzeugen zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten, so geben sie gegebenenfalls das Drittland an, in dem die Datennutzung stattfinden soll.

Artikel 32g

Überwachung der Einhaltung

(1) Die in Artikel 32b genannten zuständigen Behörden überwachen und beaufsichtigen entweder von sich aus oder auf Ersuchen einer natürlichen oder juristischen Person, ob anerkannte Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen die in diesem Kapitel festgelegten Anforderungen erfüllen, auch darüber, ob sie die darin festgelegten Eintragungsanforderungen weiterhin erfüllen.

(2) Die zuständigen Behörden sind befugt, von anerkannten Anbietern von Datenvermittlungsdiensten oder anerkannten datenaltruistischen Organisationen oder deren gesetzlichen Vertretern alle Informationen anzufordern, die erforderlich sind, um die Einhaltung der in diesem Kapitel festgelegten Anforderungen zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(3) Stellt eine zuständige Behörde fest, dass ein anerkannter Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies der Einrichtung oder ihrem gesetzlichen Vertreter mit und gibt ihr Gelegenheit, innerhalb von 30 Tagen nach Erhalt der Mitteilung dazu Stellung zu nehmen.

(4) Die zuständige Behörde ist befugt, die Beendigung des in Absatz 3 genannten Nichteinhaltung entweder unverzüglich oder innerhalb einer angemessenen Frist zu verlangen, und ergreift angemessene und verhältnismäßige Maßnahmen mit dem Ziel, die Einhaltung sicherzustellen.

(5) Erfüllt ein anerkannter Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation auch nach einer Mitteilung gemäß Absatz 3 eine oder mehrere der in diesem Kapitel festgelegten Anforderungen nicht, so

a) verliert er/sie sein/ihr Recht, die in Artikel 32a genannte Bezeichnung in schriftlicher und mündlicher Kommunikation zu verwenden;

b) wird er/sie aus dem öffentlichen Unionsregister gemäß Artikel 32a gestrichen.

Jede Entscheidung über den Entzug des Rechts zur Verwendung der Bezeichnung gemäß Unterabsatz 1 Buchstabe a wird von der zuständigen Behörde veröffentlicht.

KAPITEL VIIb

Freier Verkehr nicht-personenbezogener Daten in der Union

Artikel 32h

Verbot von Lokalisierungsauflagen für nicht-personenbezogene Daten in der Union

(1) Datenlokalisierungsauflagen für nicht-personenbezogene Daten sind verboten, es sei denn, sie sind aus Gründen der öffentlichen Sicherheit im Einklang mit dem Grundsatz der Verhältnismäßigkeit gerechtfertigt oder auf der Grundlage des Unionsrechts festgelegt.

(2) Die Mitgliedstaaten teilen der Kommission umgehend alle Entwürfe von Vorschriften mit, die neue Datenlokalisierungsauflagen enthalten oder bestehende Datenlokalisierungsauflagen ändern, gemäß den Verfahren, die in den Artikeln 5, 6 und 7 der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates festgelegt sind.

Kapitel VIIc

Weiterverwendung von Daten und Dokumenten öffentlicher Stellen

ABSCHNITT 1

ALLGEMEINE BESTIMMUNGEN

Artikel 32i

Gegenstand und Anwendungsbereich

(1) Dieses Kapitel enthält Vorschriften für die Weiterverwendung und die praktischen Vorkehrungen zur Erleichterung der Weiterverwendung von

a) bestehenden Daten und Dokumenten, die sich im Besitz öffentlicher Stellen der Mitgliedstaaten befinden, einschließlich bestimmter Kategorien geschützter Daten;

b) vorhandenen Daten und Dokumenten im Besitz öffentlicher Unternehmen, die

i) in den gemäß Kapitel II der Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates genannten Bereichen tätig sind,

ii) als Betreiber eines öffentlichen Dienstes gemäß Artikel 2 der Verordnung (EG) Nr. 1370/2007 des Europäischen Parlaments und des Rates tätig sind,

iii) als Luftfahrtunternehmen gemeinwirtschaftliche Verpflichtungen gemäß Artikel 16 der Verordnung (EG) Nr. 1008/2008 des Europäischen Parlament und des Rates erfüllen, oder

iv) als Gemeinschaftsreeder Verpflichtungen des öffentlichen Dienstes gemäß Artikel 4 der Verordnung (EWG) des Rates Nr. 3577/92 erfüllen;

c) Forschungsdaten gemäß den in Artikel 32t festgelegten Bedingungen.

(2) Dieses Kapitel gilt nicht für

a) Daten und Dokumente, deren Bereitstellung nicht unter den gesetzlich oder durch andere verbindliche Rechtsvorschriften des Mitgliedstaats festgelegten öffentlichen Auftrag der betreffenden öffentlichen Stellen fällt oder, in Ermangelung solcher Rechtsvorschriften, nicht unter den durch allgemeine Verwaltungspraxis in dem betreffenden Mitgliedstaat festgelegten öffentlichen Auftrag fällt, vorausgesetzt, dass der Umfang der öffentlichen Aufträge transparent ist und regelmäßig überprüft wird;

b) Daten und Dokumente, die sich im Besitz öffentlicher Unternehmen befinden, und

i) die nicht im Rahmen der Erbringung von Dienstleistungen von allgemeinem Interesse im Sinne der gesetzlichen oder sonstigen verbindlichen Vorschriften der Mitgliedstaaten erstellt wurden;

ii) die mit unmittelbar dem Wettbewerb ausgesetzten Tätigkeiten zusammenhängen und daher gemäß Artikel 34 der Richtlinie 2014/25/EU nicht den Vorschriften für die Auftragsvergabe unterliegen;

c) Daten und Dokumente, wie z. B. sensible Daten, die aufgrund der Zugangsregelungen des Mitgliedstaats aus Gründen des Schutzes der nationalen Sicherheit (d. h. der Sicherheit des Staates), der Verteidigung oder der öffentlichen Sicherheit vom Zugang ausgeschlossen sind;

d) Daten und Dokumente, die im Besitz öffentlich-rechtlicher Rundfunkanstalten und ihrer Zweigstellen oder anderer Stellen und deren Zweigstellen sind und der Wahrnehmung eines öffentlichen Sendeauftrags dienen.

(3) Abschnitt 2 dieses Kapitels gilt nicht für

a) Daten oder Dokumente, wie zum Beispiel sensible Daten oder Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten nicht zugänglich sind, einschließlich aus folgenden Gründen:

i) statistische Geheimhaltung,

ii) geschäftliche Geheimhaltung (einschließlich Betriebsgeheimnissen, Berufsgeheimnissen, Unternehmensgeheimnissen);

b) Daten oder Dokumente, zu denen der Zugang aufgrund der Zugangsregelungen der Mitgliedstaaten beschränkt ist,

i) einschließlich der Fälle, in denen Bürger oder juristische Personen ein besonderes Interesse nachweisen müssen, um Zugang zu Dokumenten zu erhalten,

ii) aus Gründen des Schutzes personenbezogener Daten nicht oder nur eingeschränkt zugänglich sind, und Teile von Dokumenten oder Daten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, deren Weiterverwendung gesetzlich nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist oder gesetzlich als

Beeinträchtigung des Schutzes der Privatsphäre und der Integrität der betroffenen Personen definiert ist, insbesondere im Einklang mit dem Unionsrecht oder dem nationalen Recht im Hinblick auf den Schutz personenbezogener Daten; Logos, Wappen und Insignien;

c) Daten oder Dokumente, die geistiges Eigentum Dritter sind;

d) Daten oder Dokumente im Besitz anderer kultureller Einrichtungen als Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archiven;

e) Daten oder Dokumente im Besitz von Bildungseinrichtungen der Sekundarstufe und darunter und – bei allen sonstigen Bildungseinrichtungen – andere als die in Absatz 1 Buchstabe c genannten Dokumente oder Daten;

f) andere als die in Absatz 1 Buchstabe c genannten Daten oder Dokumente im Besitz von Forschungseinrichtungen und Forschungsfördereinrichtungen, einschließlich Einrichtungen, die zum Zweck des Transfers von Forschungsergebnissen gegründet wurden;

g) Daten oder Dokumente, die aufgrund ihrer Eigenschaft als vertrauliche Informationen über den Schutz kritischer Einrichtungen oder kritischer Infrastrukturen im Sinne des Artikels 2 Nummern 1 und 4 der Richtlinie 2022/2557/EU nicht oder nur eingeschränkt zugänglich sind;

(4) Abschnitt 3 dieses Kapitels gilt nicht für

a) Daten und Dokumente, bei denen es sich nicht um bestimmte Kategorien geschützter Daten handelt;

b) Daten oder Dokumente, die im Besitz öffentlicher Unternehmen sind;

c) Daten oder Dokumente, die im Besitz von Kultureinrichtungen und Bildungseinrichtungen sind;

d) unter Abschnitt 2 dieses Kapitels fallende Daten und Dokumente.

(5) Dieses Kapitel stützt sich auf die Zugangsregelungen der Union und der Mitgliedstaaten und lässt diese unberührt, insbesondere in Bezug auf die Gewährung des Zugangs zu amtlichen Dokumenten und deren Offenlegung.

(6) Die sich aus diesem Kapitel ergebenden Verpflichtungen sollten nur insoweit gelten, wie sie mit Bestimmungen völkerrechtlicher Übereinkommen zum Schutz der Rechte des geistigen Eigentums, insbesondere der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (Berner Übereinkunft), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS-Übereinkommen) und dem Urheberrechtsvertrag der Weltorganisation für geistiges Eigentum (WCT) vereinbar sind.

(7) Das Recht der Hersteller von Datenbanken gemäß Artikel 7 Absatz 1 der Richtlinie 96/9/EG darf von öffentlichen Stellen nicht in Anspruch genommen werden, um dadurch die Weiterverwendung von Daten und Dokumenten zu verhindern oder diese Weiterverwendung über die in dieser Richtlinie festgelegten Beschränkungen hinaus einzuschränken.

(8) Dieses Kapitel regelt die Weiterverwendung vorhandener Daten und Dokumente, die im Besitz öffentlicher Stellen und öffentlicher Unternehmen der Mitgliedstaaten sind, einschließlich der Daten und Dokumente, auf die die Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates anwendbar ist.

(9) Dieses Kapitel berührt nicht das Unionsrecht und das nationale Recht oder völkerrechtliche Übereinkünfte, denen die Union oder die Mitgliedstaaten beigetreten sind, in Bezug auf den Schutz der in Artikel 2 Nummer 54 genannten Daten- oder Dokumentkategorien.

Artikel 32j

Nichtdiskriminierung

(1) Alle anwendbaren Bedingungen für die Weiterverwendung von Daten oder Dokumenten müssen in Bezug auf die Daten- oder Dokumentkategorien, die Zwecke der Weiterverwendung und die Art der Daten oder Dokumente, deren Weiterverwendung erlaubt wird, nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen. Dieser Grundsatz gilt gleichermaßen für vergleichbare Kategorien der Weiterverwendung, auch für die grenzübergreifende Weiterverwendung.

(2) Werden Daten oder Dokumente von öffentlichen Stellen als Ausgangsmaterial für eigene gewerbliche Tätigkeiten weiterverwendet, die nicht unter ihren öffentlichen Auftrag fallen, so gelten für die Bereitstellung der Daten oder Dokumente für diese Tätigkeiten dieselben Entgelte oder Gebühren und sonstigen Bedingungen wie für andere Weiterverwender.

Artikel 32k

Ausschließlichkeitsvereinbarungen

(1) Die Weiterverwendung von Daten oder Dokumenten steht allen potenziellen Marktteilnehmern offen, selbst wenn auf diesen Daten oder Dokumenten beruhende Mehrwertprodukte bereits von einem oder mehreren Marktteilnehmern genutzt werden. Verträge oder sonstige Vereinbarungen oder Praktiken im Zusammenhang mit der Weiterverwendung von Daten oder Dokumenten, die die Gewährung ausschließlicher Rechte oder die Beschränkung der Verfügbarkeit von Daten oder Dokumenten zur Weiterverwendung durch andere Stellen als die Vertragsparteien dieser Verträge, Vereinbarungen oder Praktiken bezwecken oder bewirken, sind verboten.

(2) Ist für die Bereitstellung eines Dienstes von allgemeinem Interesse ein ausschließliches Recht erforderlich, so kann dieses Recht abweichend von Absatz 1 unter folgenden Bedingungen gewährt werden, soweit dies für die Erbringung des Dienstes oder der Bereitstellung des Produkts erforderlich ist:

a) Das ausschließliche Recht wird durch einen Verwaltungsakt oder eine vertragliche Vereinbarung gemäß dem geltenden Unionsrecht und dem nationalen Recht sowie im Einklang mit den Grundsätzen der Transparenz, der Gleichbehandlung und der Nichtdiskriminierung gewährt.

b) Die das ausschließliche Recht gewährenden Vereinbarungen, einschließlich der Begründung, warum die Gewährung eines solchen Rechts erforderlich ist, ist transparent und wird in einer Form, die dem einschlägigen Unionsrecht für die Vergabe öffentlicher Aufträge und nationalem Recht entspricht, im Internet öffentlich zugänglich gemacht.

c) Mit Ausnahme der ausschließlichen Rechte im Zusammenhang mit der Digitalisierung kultureller Ressourcen wird der Grund für die Gewährung

ausschließlicher Rechte an Daten und Dokumenten im Anwendungsbereich des Abschnitts 2 regelmäßig und in jedem Fall alle drei Jahre überprüft.

d) Am oder nach dem 16. Juli 2019 getroffene Ausschließlichkeitsvereinbarungen werden spätestens zwei Monate vor ihrem Inkrafttreten online öffentlich zugänglich gemacht. Die endgültigen Bedingungen solcher Vereinbarungen müssen transparent sein und online öffentlich zugänglich gemacht werden.

(3) Bezieht sich ein ausschließliches Recht auf die Digitalisierung von Kulturbeständen, darf es ungeachtet des Absatzes 1 im Allgemeinen für höchstens zehn Jahre gewährt werden. Wird es für mehr als zehn Jahre gewährt, wird die Gewährungsdauer im Einklang mit geltendem Unionsrecht und nationalem Recht im elften Jahr und danach gegebenenfalls alle sieben Jahre überprüft.

(4) Im Falle eines in Absatz 3 genannten ausschließlichen Rechts ist der betreffenden öffentlichen Stelle im Rahmen der Vereinbarung eine Kopie der digitalisierten Kulturbestände unentgeltlich zur Verfügung zu stellen. Diese Kopie wird am Ende des Ausschließlichkeitszeitraums zur Weiterverwendung zur Verfügung gestellt.

(5) Für bestimmte Kategorien geschützter Daten darf die Dauer des ausschließlichen Rechts auf Weiterverwendung von Daten 12 Monate nicht überschreiten. Wird ein Vertrag abgeschlossen, so ist dessen Dauer die gleiche wie die des ausschließlichen Rechts.

(6) Verträge und andere Vereinbarungen oder Praktiken, die nicht ausdrücklich ausschließliche Rechte gewähren, die aber darauf abzielen oder bei denen davon ausgegangen werden kann, dass sie die Weiterverwendung von Daten und Dokumenten durch andere Einrichtungen als die in Abschnitt 2 beteiligten beschränken, werden spätestens zwei Monate vor ihrem Inkrafttreten online öffentlich zugänglich gemacht. Die Auswirkungen solcher rechtlichen oder praktischen Vorkehrungen auf die Verfügbarkeit von Daten zur Weiterverwendung sind Gegenstand regelmäßiger Überprüfungen und werden mindestens alle drei Jahre überprüft. Die endgültigen Bedingungen solcher Vereinbarungen müssen transparent sein und online öffentlich zugänglich gemacht werden.

(7) Für bestehende Ausschließlichkeitsvereinbarungen gilt Folgendes:

a) Am 17. Juli 2013 bestehende Ausschließlichkeitsvereinbarungen über Daten und Dokumente, die in den Anwendungsbereich von Abschnitt 2 und nicht unter die Ausnahmen gemäß den Absätzen 2 und 3 fallen und die von öffentlichen Stellen getroffen wurden, werden bei Vertragsablauf, spätestens jedoch am 18. Juli 2043 beendet.

b) Am 16. Juli 2019 bestehende Ausschließlichkeitsvereinbarungen über Daten und Dokumente im Anwendungsbereich von Abschnitt 2, die nicht unter die Ausnahmen der Absätze 2 und 3 fallen und die von öffentlichen Unternehmen getroffen wurden, werden bei Vertragsablauf, spätestens jedoch am 17. Juli 2049 beendet.

Artikel 32l

Allgemeine Grundsätze für die Entgelterhebung

(1) Gemäß Absatz 2 oder Absatz 3 festgelegte Entgelte müssen transparent, nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen den Wettbewerb nicht einschränken.

(2) Im Falle von Standardgebühren oder Standardentgelten für die Weiterverwendung von Daten oder Dokumenten werden die entsprechenden Bedingungen und die tatsächliche Höhe dieser Gebühren oder Entgelte einschließlich der Berechnungsgrundlage dieser Gebühren oder Entgelte, im Voraus festgelegt und, soweit möglich und sinnvoll, in elektronischer Form veröffentlicht.

(3) Im Falle von Gebühren oder Entgelten für die Weiterverwendung, die in Absatz 1 nicht genannt sind, müssen im Voraus die Faktoren angegeben werden, die bei der Berechnung dieser Gebühren oder Entgelte berücksichtigt werden. Auf Anfrage gibt der Inhaber der Daten oder Dokumente auch die Berechnungsweise dieser Gebühren oder Entgelte in Bezug auf einen spezifischen Antrag auf Weiterverwendung an.

(4) Öffentliche Stellen müssen gewährleisten, dass alle Gebühren oder Entgelte auch online über weithin verfügbare grenzüberschreitende Zahlungsdienste ohne Diskriminierung aufgrund des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union bezahlt werden können.

Artikel 32m

Rechtsmittelbelehrung

Die öffentlichen Stellen gewährleisten, dass Antragsteller, die die Weiterverwendung von Daten oder Dokumenten beantragt haben, über die verfügbaren Rechtsbehelfe hinsichtlich der sie betreffenden Entscheidungen oder Verfahren unterrichtet werden.

ABSCHNITT 2

WEITERVERWENDUNG OFFENER STAATLICHER DATEN

Unterabschnitt 1 Anwendungsbereich und allgemeine Grundsätze

Artikel 32n

Allgemeiner Grundsatz für die Weiterverwendung offener staatlicher Daten

(1) Daten oder Dokumente, die in den Anwendungsbereich dieses Abschnitts fallen, können gemäß Abschnitt 1 und Abschnitt 2 Unterabschnitt 3 für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden.

(2) Für Daten oder Dokumente, an denen Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archiven Rechte des geistigen Eigentums innehaben, und für Daten und Dokumente im Besitz öffentlicher Unternehmen, falls deren Weiterverwendung erlaubt wird, dürfen diese Daten oder Dokumente gemäß Abschnitt 1 und Abschnitt 2 Unterabschnitt 3 für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden.

Unterabschnitt 2

Anträge auf Weiterverwendung

Artikel 32o

Bearbeitung von Anträgen auf Weiterverwendung

(1) Für die Bearbeitung von Anträgen auf Weiterverwendung und die Bereitstellung der Dokumente zur Weiterverwendung an den Antragsteller oder – falls eine Lizenz erforderlich ist – für die Unterbreitung eines endgültigen Lizenzangebots an den

Antragsteller halten die öffentlichen Stellen eine angemessene Frist ein, die der Frist für die Bearbeitung von Anträgen auf Zugang zu Daten oder Dokumenten entspricht, und bedienen sich dabei, soweit möglich und sinnvoll, elektronischer Mittel.

(2) Wurden keine Fristen oder sonstigen Regelungen für die rechtzeitige Bereitstellung der Daten oder Dokumente festgelegt, so müssen die öffentlichen Stellen so bald wie möglich, in jedem Fall innerhalb von 20 Arbeitstagen nach Eingang des Antrags den Antrag bearbeiten und dem Antragsteller die Dokumente zur Weiterverwendung bereitstellen oder – falls eine Lizenz erforderlich ist – ihm ein endgültiges Lizenzangebot unterbreiten. Diese Frist kann bei umfangreichen oder komplexen Anträgen um weitere 20 Arbeitstage verlängert werden. In diesen Fällen wird der Antragsteller so bald wie möglich, in jedem Fall jedoch innerhalb von drei Wochen nach dem ursprünglichen Antrag unter Angabe der Gründe davon unterrichtet, dass für die Bearbeitung des Antrags mehr Zeit benötigt wird.

(3) Im Fall eines ablehnenden Bescheids teilt die öffentliche Stelle dem Antragsteller die Gründe für die Ablehnung mit und stützt sich dabei auf die einschlägigen Bestimmungen der Zugangsregelung des betreffenden Mitgliedstaats oder auf die Bestimmungen dieser Verordnung, insbesondere auf Artikel 32i Absatz 2 Buchstaben a bis c und Artikel 32i oder Artikel 32n Absatz 3 Buchstaben a bis d. Wird ein ablehnender Bescheid auf Artikel 32i Absatz 3 Buchstabe d gestützt, so verweist die öffentliche Stelle auf die natürliche oder juristische Person, die Inhaber der Rechte ist, soweit diese bekannt ist, oder ersatzweise auf den Lizenzgeber, von dem die öffentliche Stelle das betreffende Material erhalten hat. Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archive sind nicht zu diesem Verweis verpflichtet.

(4) Zu den Rechtsbehelfen gehört die Möglichkeit der Überprüfung durch eine unabhängige Überprüfungsinstanz mit den entsprechender Sachkenntnis, wie die nationale Wettbewerbsbehörde, die für den Zugang zu Daten und Dokumenten zuständige Behörde, die gemäß der Verordnung (EU) 2016/679 errichtete Aufsichtsbehörde oder ein nationales Gericht, deren Entscheidungen für die betreffende öffentliche Stelle bindend sind.

(5) Für die Zwecke dieses Artikels legen die Mitgliedstaaten praktische Vorkehrungen zur Vereinfachung der effektiven Weiterverwendung von Daten oder Dokumenten fest. Diese Vorkehrungen können insbesondere die Mittel für die Bereitstellung angemessener Informationen über die in der vorliegenden Verordnung vorgesehenen Rechte sowie für die Bereitstellung einschlägiger Unterstützung und Orientierung umfassen.

(6) Dieser Artikel gilt nicht für

a) öffentliche Unternehmen;

b) Bildungseinrichtungen, Forschungseinrichtungen und Forschungsförderungseinrichtungen.

Unterabschnitt 3

Bedingungen für die Weiterverwendung

Artikel 32p

Verfügbare Formate

(1) Unbeschadet des Unterabschnitts 5 stellen öffentliche Stellen und öffentliche Unternehmen ihre Daten und Dokumente in allen vorhandenen Formaten oder Sprachen und, soweit möglich und sinnvoll, auf elektronischem Wege in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zusammen mit den zugehörigen Metadaten zur Verfügung. Sowohl die Formate als auch die Metadaten müssen soweit möglich förmlichen offenen Standards entsprechen.

(2) Die Mitgliedstaaten bestärken öffentliche Stellen und öffentliche Unternehmen darin, in den Anwendungsbereich dieser Verordnung fallende Daten und Dokumente nach dem Grundsatz „konzeptionell und standardmäßig offen“ (*open by design and by default*) zu erstellen und zur Verfügung zu stellen.

(3) Absatz 1 verpflichtet die öffentlichen Stellen nicht, Daten oder Dokumente neu zu erstellen oder anzupassen oder Auszüge aus Dokumenten zur Verfügung zu stellen, um diesem Absatz nachzukommen, wenn dies mit einem unverhältnismäßigen Aufwand verbunden ist, der über eine einfache Bearbeitung hinausgeht.

(4) Öffentliche Stellen sind nicht verpflichtet, die Erstellung und Speicherung bestimmter Arten von Daten oder Dokumenten im Hinblick auf deren Weiterverwendung durch eine Organisation des privaten oder öffentlichen Sektors fortzusetzen.

(5) Öffentliche Stellen machen dynamische Daten unmittelbar nach der Erfassung mithilfe geeigneter API und gegebenenfalls als Massen-Download zur Weiterverwendung zugänglich.

(6) Würde die Bereitstellung von dynamischen Daten zur Weiterverwendung unmittelbar nach der Erfassung gemäß Absatz 5 die finanzielle und technische Leistungsfähigkeit der öffentlichen Stelle übersteigen und somit zu einem unverhältnismäßigen Aufwand führen, werden jene dynamischen Daten innerhalb einer Frist oder mit vorübergehenden technischen Beschränkungen zur Weiterverwendung zugänglich gemacht, die die Nutzung ihres wirtschaftlichen und sozialen Potenzials nicht übermäßig beeinträchtigen.

(7) Die Absätze 1 bis 6 gelten für vorhandene Daten oder Dokumente im Besitz öffentlicher Unternehmen, die zur Weiterverwendung verfügbar sind.

(8) Die hochwertigen Datensätze, die gemäß Artikel 32v Absatz 1 in einer Liste aufgeführt werden, werden in maschinenlesbarem Format über geeignete APIs und gegebenenfalls als Massen-Download zur Weiterverwendung zugänglich gemacht.

Artikel 32q

Grundsätze für die Erhebung von Entgelten für offene staatliche Daten

(1) Die Weiterverwendung von Daten oder Dokumenten, die in den Anwendungsbereich dieses Abschnitts fallen, ist unentgeltlich. Allerdings können die durch die Reproduktion, Bereitstellung und Verbreitung von Daten und Dokumenten sowie durch die Anonymisierung personenbezogener Daten und Maßnahmen zum Schutz vertraulicher Geschäftsinformationen verursachten Grenzkosten der öffentlichen Stelle, die im Besitz der Daten ist, erstattet werden.

(2) Absatz 1 gilt nicht für die folgenden Einrichtungen:

a) öffentliche Stellen, deren Auftrag das Erzielen von Einnahmen erfordert, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihrer öffentlichen Aufträge zu decken;

b) Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archive;

c) öffentliche Unternehmen.

(3) Die Mitgliedstaaten veröffentlichen online eine Liste der in Absatz 2 Buchstabe a genannten öffentlichen Stellen.

(4) In den in Absatz 2 Buchstaben a und c genannten Fällen werden die Gesamtkosten nach objektiven, transparenten und nachprüfbaren Kriterien berechnet. Diese Kriterien werden durch die Mitgliedstaaten festgelegt. Die Gesamteinnahmen aus der Bereitstellung von Daten und Dokumenten und der Gestattung ihrer Weiterverwendung in dem entsprechenden Abrechnungszeitraum dürfen die Kosten ihrer Erfassung, Erstellung, Reproduktion, Verbreitung und Datenspeicherung, zuzüglich einer angemessenen Gewinnspanne, sowie – gegebenenfalls – der Anonymisierung personenbezogener Daten und Maßnahmen zum Schutz vertraulicher Geschäftsinformationen nicht übersteigen. Gebühren und Entgelte werden nach Maßgabe der geltenden Buchführungsgrundsätze berechnet.

(5) Soweit die in Absatz 2 Buchstabe b genannten öffentlichen Stellen Gebühren erheben, dürfen die Gesamteinnahmen aus der Bereitstellung von Daten oder Dokumenten und der Gestattung ihrer Weiterverwendung in dem entsprechenden Abrechnungszeitraum die Kosten ihrer Erfassung, Erstellung, Reproduktion, Verbreitung, Datenspeicherung, Bewahrung und der Rechteklärung sowie, gegebenenfalls, der Anonymisierung personenbezogener Daten und Maßnahmen zum Schutz vertraulicher Geschäftsinformationen zuzüglich einer angemessenen Gewinnspanne nicht übersteigen. Gebühren und Entgelte werden nach Maßgabe der für die betreffenden öffentlichen Stellen geltenden Buchführungsgrundsätze berechnet.

(6) Öffentliche Stellen können für die Weiterverwendung von Daten und Dokumenten durch sehr große Unternehmen höhere Entgelte als die in den Absätzen 1, 4 und 5 vorgesehenen Entgelte festlegen. Solche Entgelte müssen verhältnismäßig sein und auf objektiven Kriterien beruhen, wobei die Wirtschaftskraft oder die Fähigkeit des Unternehmens, Daten zu erwerben, zu berücksichtigen ist, einschließlich insbesondere der Benennung als Torwächter gemäß der Verordnung (EU) 2022/1925. Zusätzlich zu den in Absatz 1 dieses Artikels aufgeführten Elementen können diese Entgelte die Kosten der Erfassung, Erstellung, Reproduktion, Verbreitung und Speicherung von Daten und gegebenenfalls die Kosten der Anonymisierung oder Maßnahmen zum Schutz der Vertraulichkeit der Daten oder Dokumente zuzüglich einer angemessenen Gewinnspanne decken.

(7) Die Weiterverwendung folgender Daten ist für den Nutzer unentgeltlich:

a) vorbehaltlich Artikel 32y Absätze 3, 4 und 5 die Weiterverwendung hochwertiger Datensätze, die gemäß Absatz 1 jenes Artikels in einer Liste festgelegt werden,

b) Weiterverwendung von Forschungsdaten gemäß Artikel 32i Absatz 1 Buchstabe c.

Artikel 32r

Standardlizenzen

(1) Die Weiterverwendung von Daten oder Dokumenten unterliegt keinen Bedingungen, es sei denn, diese Bedingungen sind objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt.

(2) Wenn die Weiterverwendung an Bedingungen gebunden ist, dürfen diese Bedingungen die Möglichkeiten der Weiterverwendung nicht unnötig einschränken und nicht der Behinderung des Wettbewerbs dienen.

(3) In Mitgliedstaaten, in denen Lizenzen verwendet werden, stellen öffentliche Stellen sicher, dass für die Weiterverwendung von Daten oder Dokumenten des öffentlichen Sektors Standardlizenzen, die an besondere Lizenzanträge angepasst werden können, in digitaler Form zur Verfügung stehen und elektronisch bearbeitet werden können.

(4) Öffentliche Stellen können besondere Bedingungen für die Weiterverwendung von Daten und Dokumenten durch sehr große Unternehmen festlegen. Diese Bedingungen müssen verhältnismäßig sein und sollten auf objektiven Kriterien beruhen. Sie werden unter Berücksichtigung der Wirtschaftskraft oder der Fähigkeit des Unternehmens festgelegt, Daten zu erwerben, wobei insbesondere eine Benennung als Torwächter gemäß der Verordnung (EU) 2022/1925 berücksichtigt wird.

Artikel 32s

Praktische Vorkehrungen

(1) Die Mitgliedstaaten treffen praktische Vorkehrungen, die eine Suche nach den zur Weiterverwendung verfügbaren Daten oder Dokumenten erleichtern, wie z. B. Bestandslisten der wichtigsten Daten oder Dokumente mit zugehörigen Metadaten, die, soweit möglich und sinnvoll, online verfügbar sind und in einem maschinenlesbaren Format vorliegen, sowie Internet-Portale, die mit den Bestandslisten verknüpft sind. Soweit möglich, sorgen die Mitgliedstaaten – insbesondere, indem sie die Metadatenaggregation auf Unionsebene ermöglichen – dafür, dass eine sprachübergreifende Suche nach Daten oder Dokumenten vorgenommen werden kann.

Die Mitgliedstaaten bestärken öffentliche Stellen auch darin, praktische Vorkehrungen zu treffen, um die Bewahrung von zur Weiterverwendung verfügbaren Daten oder Dokumenten zu erleichtern.

(2) Die Mitgliedstaaten setzen in Zusammenarbeit mit der Kommission ihre Bemühungen fort, um den Zugang zu Datensätzen auf elektronischem Wege über zugängliche, einfach auffindbare und weiterverwendbare Formate zu vereinfachen, insbesondere indem sie eine zentrale Anlaufstelle einrichten und geeignete Datensätze im Besitz öffentlicher Stellen, mit Blick auf die Daten oder Dokumente, auf die dieser Abschnitt Anwendung findet, zu Daten im Besitz der Organe der Union verfügbar machen.

Unterabschnitt 4

Forschungsdaten

Artikel 32t

Forschungsdaten

(1) Die Mitgliedstaaten unterstützen die Verfügbarkeit von Forschungsdaten durch die Annahme nationaler Strategien und einschlägiger Maßnahmen mit dem Ziel, öffentlich finanzierte Forschungsdaten nach dem Grundsatz der „standardmäßig

offenen Daten“ und im Einklang mit den FAIR-Grundsätzen offen zugänglich zu machen (im Folgenden „Politik des offenen Zugangs“). In diesem Zusammenhang sind Anliegen in Bezug auf Rechte des geistigen Eigentums, den Schutz personenbezogener Daten sowie Vertraulichkeit, Sicherheit und legitime Geschäftsinteressen nach dem Grundsatz „so offen wie möglich, so geschlossen wie nötig“ (*as open as possible, as closed as necessary*) zu berücksichtigen. Diese Politik des offenen Zugangs richtet sich an Forschungseinrichtungen und Forschungsförderungseinrichtungen.

(2) Unbeschadet des Artikels 32n Absatz 3 Buchstabe d können die Forschungsdaten gemäß Abschnitt 1 und Abschnitt 2 Unterabschnitt 3 für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden, soweit sie öffentlich finanziert wurden und wenn sie von Forschern, Forschungseinrichtungen oder Forschungsförderungseinrichtungen bereits über ein institutionelles oder thematisches Archiv öffentlich zugänglich gemacht wurden. In diesem Zusammenhang sind berechtigte Geschäftsinteressen, Wissenstransfertätigkeiten und bestehende Rechte Dritter an geistigem Eigentum zu berücksichtigen.

Unterabschnitt 5

Hochwertige Datensätze

Artikel 32u

Thematische Kategorien von hochwertigen Datensätzen

(1) Die thematischen Kategorien hochwertiger Datensätze sind in Anhang I festgelegt.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 45 Absatz 2a delegierte Rechtsakte zur Änderung des Anhangs I durch Aufnahme neuer thematischer Kategorien hochwertiger Datensätze zu erlassen, die der Technologie- und Marktentwicklung Rechnung tragen.

Artikel 32v

Bestimmte hochwertige Datensätze und Modalitäten der Veröffentlichung und Weiterverwendung

(1) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung einer Liste bestimmter im Besitz öffentlicher Stellen oder öffentlicher Unternehmen befindlicher hochwertiger Datensätze der im Anhang I angegebenen Kategorien unter den Daten oder Dokumenten, auf die dieser Abschnitt Anwendung findet.

Solche bestimmten hochwertigen Datensätze müssen

a) vorbehaltlich der Absätze 3, 4 und 5 unentgeltlich verfügbar sein,

b) maschinenlesbar sein,

c) über API verfügbar sein und

d) gegebenenfalls als Massen-Download verfügbar sein.

In jenen Durchführungsrechtakten können die Modalitäten der Veröffentlichung und Weiterverwendung hochwertiger Datensätze festgelegt werden. Diese Modalitäten müssen mit den offenen Standardlizenzen vereinbar sein.

Diese Modalitäten können Bedingungen umfassen, die für die Weiterverwendung, Daten- und Metadatenformate sowie die technischen Modalitäten der Verbreitung gelten. Investitionen der Mitgliedstaaten in Konzepte für offene Daten, wie etwa

Investitionen in die Entwicklung und Einführung bestimmter Standards, werden berücksichtigt und gegen den potenziellen Nutzen einer Aufnahme in die Liste abgewogen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 46 Absatz 2 genannten Prüfverfahren erlassen.

(2) Die Ermittlung bestimmter hochwertiger Datensätze gemäß Absatz 1 beruht auf der Bewertung ihres Potenzials

a) für die Erzielung bedeutender sozioökonomischer oder ökologischer Vorteile und innovativer Dienstleistungen,

b) für eine große Zahl von Nutzern, insbesondere KMU und kleine Midcap-Unternehmen, von Nutzen zu sein,

c) der Erzielung von Einnahmen zu dienen und

d) mit anderen Datensätzen kombiniert zu werden.

Zum Zweck der Ermittlung solcher bestimmter hochwertiger Datensätze führt die Kommission angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durch, nimmt eine Folgenabschätzung vor und stellt die Komplementarität mit bestehenden Rechtsakten, wie der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates, in Bezug auf die Weiterverwendung von Dokumenten sicher. Diese Folgenabschätzung umfasst eine Kosten-Nutzen-Analyse und eine Analyse, ob sich die unentgeltliche Bereitstellung hochwertiger Datensätze durch öffentliche Stellen, die Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten bei der Wahrnehmung ihres öffentlichen Auftrags zu decken, wesentlich auf den Haushalt solcher Stellen auswirken würde. Bei hochwertigen Datensätzen im Besitz öffentlicher Unternehmen wird die Rolle dieser Unternehmen in einem wettbewerbsbestimmten wirtschaftlichen Umfeld in der Folgenabschätzung besonders berücksichtigt.

(3) Abweichend von Absatz 1 Unterabsatz 2 Buchstabe a wird in den Durchführungsrechtsakten gemäß diesem Absatz festgelegt, dass die unentgeltliche Verfügbarkeit hochwertiger Datensätze nicht für bestimmte hochwertige Datensätze im Besitz öffentlicher Unternehmen gilt, wenn dies zu einer Verfälschung des Wettbewerbs auf den betreffenden Märkten führen würde.

(4) Die Anforderung, hochwertige Datensätze gemäß Absatz 1 Unterabsatz 2 Buchstabe a unentgeltlich verfügbar zu machen, gilt nicht für Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archive.

(5) In Fällen, in denen sich die unentgeltliche Bereitstellung hochwertiger Datensätze durch öffentliche Stellen, die Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten bei der Wahrnehmung ihres öffentlichen Auftrags zu decken, wesentlich auf den Haushalt der betreffenden Stellen auswirken würde, können die Mitgliedstaaten diese Stellen für einen Zeitraum von höchstens zwei Jahren nach Inkrafttreten des entsprechenden Durchführungsrechtsakts, der gemäß Absatz 1 erlassen wurde, von der Anforderung der unentgeltlichen Bereitstellung dieser hochwertigen Datensätze befreien.

Abschnitt 3

Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen

Artikel 32w

Bedingungen für die Weiterverwendung

(1) Öffentliche Stellen, die nach nationalem Recht dafür zuständig sind, den Zugang zwecks Weiterverwendung von zu bestimmten Datenkategorien gehörenden Daten oder Dokumenten zu gewähren oder zu verweigern, machen die Bedingungen für das Erlauben einer solchen Weiterverwendung und das Verfahren für die Beantragung einer solchen Weiterverwendung über die zentrale Informationsstelle nach Artikel 32aa öffentlich zugänglich. Bei der Gewährung oder Verweigerung des Zugangs zur Weiterverwendung können sie von den in Artikel 32z Absatz 1 genannten zuständigen Stellen unterstützt werden.

Die Mitgliedstaaten stellen sicher, dass die öffentlichen Stellen über die notwendigen Ressourcen verfügen und den vorliegenden Artikel und Artikel 32x einhalten.

(2) Die Weiterverwendung von Daten oder Dokumenten darf den Schutz dieser Daten oder Dokumente nicht beeinträchtigen und ist nur zulässig,

a) wenn dies im Einklang mit den Rechten des geistigen Eigentums steht,

b) wenn Daten, die nach dem Unionsrecht oder dem nationalen Recht über die geschäftliche oder statistische Geheimhaltung als vertraulich gelten, infolge der Gestattung der Weiterverwendung nicht offengelegt werden, es sei denn, eine solche Weiterverwendung ist auf der Grundlage der Einwilligung der betroffenen Person oder der Erlaubnis des Dateninhabers gemäß Absatz 5 zulässig,

c) gemäß der Verordnung (EU) Nr. 2016/679.

(3) Um den Schutz dieser Daten und Dokumente gemäß Absatz 2 zu gewährleisten, können öffentliche Stellen die folgenden Anforderungen festlegen:

a) der Zugang zwecks Weiterverwendung von Daten oder Dokumenten wird nur gewährt, wenn die öffentliche Stelle oder die zuständige Stelle nach Eingang des Antrags auf Weiterverwendung sichergestellt hat, dass die Daten oder Dokumente

i) im Falle personenbezogener Daten anonymisiert wurden,

ii) sonstigen Formen der Aufbereitung personenbezogener Daten unterzogen wurden,

iii) im Falle von vertraulichen Geschäftsinformationen, einschließlich Geschäftsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte, nach einer anderen Methode der Offenlegungskontrolle verändert, aggregiert oder aufbereitet wurden,

b) der Zugang zu den Daten oder Dokumenten und deren Weiterverwendung erfolgt durch Fernzugriff in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten sicheren Verarbeitungsumgebung,

c) der Zugang zu den Daten oder Dokumenten und deren Weiterverwendung erfolgt unter Einhaltung hoher Sicherheitsstandards innerhalb der physischen Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, sofern ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden.

Im Falle einer gemäß Unterabsatz 1 Buchstabe a Ziffer i erlaubten Weiterverwendung unterliegt die Weiterverwendung von Daten oder Dokumenten den Vorschriften über offene staatliche Daten gemäß Abschnitt 2. Dies gilt unbeschadet des Artikels 32y, der im Konfliktfall Vorrang hat.

Die öffentlichen Stellen erlegen im Falle einer erlaubten Weiterverwendung gemäß Unterabsatz 1 Buchstaben b und c Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird.

(4) Die öffentliche Stelle behält sich das Recht vor, den Prozess, die Mittel und die Ergebnisse der vom Weiterverwender vorgenommenen Verarbeitung von Daten oder Dokumenten zu überprüfen, um die Integrität des Schutzes der Daten oder Dokumente zu wahren. Sie behält sich ferner das Recht vor, die Verwendung von Ergebnissen zu verbieten, die Informationen enthalten, die die Rechte und Interessen Dritter gefährden. Die Entscheidung, die Verwendung der Ergebnisse zu verbieten, muss für den Weiterverwender verständlich und transparent sein.

Sofern im nationalen Recht für die Weiterverwendung von Daten keine besonderen Schutzvorkehrungen bezüglich geltender Geheimhaltungspflichten für die Weiterverwendung bestimmter Kategorien geschützter Daten vorgesehen sind, macht die öffentliche Stelle die Weiterverwendung der gemäß Absatz 3 des vorliegenden Artikels bereitgestellten Daten oder Dokumente davon abhängig, ob der Weiterverwender einer Geheimhaltungspflicht nachkommt, wonach ihm die Offenlegung von Informationen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, untersagt ist, wenn dadurch die Rechte und Interessen Dritter verletzt würden. Im Falle der unbefugten Weiterverwendung nicht-personenbezogener Daten muss der Weiterverwender unverzüglich, gegebenenfalls mit Unterstützung der öffentlichen Stelle, verpflichtet werden, die natürlichen oder juristischen Personen zu unterrichten, deren Rechte und Interessen beeinträchtigt werden könnten.

(5) Wenn die Weiterverwendung von Daten oder Dokumenten gemäß den Absätzen 3 und 4 nicht gestattet werden kann, ist die Weiterverwendung nur möglich,

a) wenn es keine andere Rechtsgrundlage als die Einwilligung zur Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, mit Einwilligung der betroffenen Personen,

b) wenn die Dateninhaber, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, dies erlauben.

Die öffentliche Stelle bemüht sich im Einklang mit dem Unionsrecht und dem nationalen Recht nach besten Kräften, potenzielle Weiterverwender bei der Einholung der Einwilligung der betroffenen Personen oder der Erlaubnis der Dateninhaber, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, zu unterstützen, sofern dies ohne unverhältnismäßige Belastung der öffentlichen Stelle möglich ist.

In den Fällen, in denen die öffentliche Stelle eine solche Unterstützung leistet, kann sie von den in Artikel 32z genannten zuständigen Stellen unterstützt werden.

Artikel 32x

Anforderungen an die Übermittlung nicht-personenbezogener Daten in Drittländer durch Weiterverwender

(1) Beabsichtigt ein Weiterverwender, bestimmte Kategorien geschützter nicht-personenbezogener Daten in ein Drittland zu übertragen, so hat er die öffentliche Stelle zum Zeitpunkt der Beantragung der Weiterverwendung solcher Daten von seiner Absicht, solche Daten zu übertragen, und dem Zweck dieser Übertragung zu unterrichten. Im Falle einer Weiterverwendung auf der Grundlage einer Genehmigung des Dateninhabers unterrichtet der Weiterverwender, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die natürliche oder juristische Person, deren Rechte und Interessen beeinträchtigt werden können, über diese Absicht, den Zweck und die angemessenen Schutzvorkehrungen. Die öffentliche Stelle gestattet die Weiterverwendung nur, wenn die natürliche oder juristische Person die Erlaubnis für die Übertragung erteilt.

(2) Öffentliche Stellen übermitteln nicht-personenbezogene vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten nur dann an einen Weiterverwender, der beabsichtigt, diese Daten in ein nicht gemäß Absatz 7 benanntes Drittland zu übertragen, wenn der Weiterverwender sich vertraglich dazu verpflichtet,

a) die Verpflichtungen, die im Einklang mit den Rechten des geistigen Eigentums und den Rechtsvorschriften der Union oder der Mitgliedstaaten über die geschäftliche oder statistische Geheimhaltung auferlegt wurden, auch nach der Übermittlung der Daten an das Drittland einzuhalten,

b) die Zuständigkeit der Gerichte des Mitgliedstaats der übermittelnden öffentlichen Stelle für alle Streitigkeiten im Zusammenhang mit der Wahrung der Rechte des geistigen Eigentums und der Rechtsvorschriften der Union oder der Mitgliedstaaten über die geschäftliche oder statistische Geheimhaltung anzuerkennen.

(3) Die Kommission kann Durchführungsrechtsakte mit Mustervertragsklauseln für die Erfüllung der in Absatz 2 des vorliegenden Artikels genannten Verpflichtungen erlassen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 46 Absatz 2 genannten Prüfverfahren erlassen.

(4) Öffentliche Stellen bieten den Weiterverwendern gegebenenfalls und im Rahmen ihrer Möglichkeiten Beratung und Unterstützung, indem sie den in Absatz 2 genannten Verpflichtungen nachkommen.

(5) Wenn dies aufgrund der Vielzahl unionsweit gestellter Anträge auf Weiterverwendung nicht-personenbezogener Daten in bestimmten Drittländern gerechtfertigt ist, kann die Kommission Durchführungsrechtsakte erlassen, in denen sie erklärt, dass die Rechts-, Aufsichts- und Durchsetzungsmechanismen eines Drittlands

a) den Schutz geistigen Eigentums und von Geschäftsgeheimnissen in einer Weise gewährleisten, die im Wesentlichen dem durch das Unionsrecht gewährleisteten Schutz gleichwertig ist,

b) wirksam angewendet und durchgesetzt werden und

c) wirksame gerichtliche Rechtsbehelfe vorsehen.

(6) Diese Durchführungsrechtsakte werden gemäß dem in Artikel 46 Absatz 2 genannten Prüfverfahren erlassen.

(7) Nach besonderen Gesetzgebungsakten der Union können bestimmte Kategorien nicht-personenbezogener Daten, die im Besitz öffentlicher Stellen sind, für die

Zwecke dieses Artikels als hochsensibel gelten, wenn die Übertragung dieser Daten in Drittländer Ziele des Gemeinwohls der Union, beispielsweise in den Bereichen Sicherheit und öffentliche Gesundheit, gefährden könnte oder die Gefahr einer erneuten Identifizierung anhand nicht-personenbezogener, anonymisierter Daten birgt. Wird ein solcher Rechtsakt erlassen, so erlässt die Kommission gemäß Artikel 45 delegierte Rechtsakte zur Ergänzung dieser Verordnung durch Festlegung besonderer Bedingungen für die Übertragung dieser Daten in Drittländer.

Wenn dies nach einem besonderen Gesetzgebungsakt der Union gemäß Unterabsatz 1 erforderlich ist, können diese besonderen Bedingungen Vorgaben für die Übertragung oder diesbezügliche technische Vorkehrungen, Beschränkungen bezüglich der Weiterverwendung von Daten in Drittländern oder Kategorien von Personen, die berechtigt sind, solche Daten in Drittländer zu übertragen, oder – in Ausnahmefällen – Beschränkungen für Übertragungen in Drittländer umfassen.

Der Weiterverwender, dem das Recht auf Weiterverwendung nicht-personenbezogener Daten gewährt wurde, darf die Daten nur in solche Drittländer übertragen, die die Anforderungen der Absätze 2, 4 und 5 erfüllen.

Artikel 32y
Gebühren

(1) Öffentliche Stellen, die eine Weiterverwendung bestimmter Kategorien von geschützten Daten erlauben, können Gebühren für die Erlaubnis der Weiterverwendung dieser Daten erheben.

(2) Erheben die öffentlichen Stellen Gebühren, so ergreifen sie Maßnahmen, um – gemäß den Vorschriften über staatliche Beihilfen – Anreize für die Weiterverwendung bestimmter Kategorien geschützter Daten zu nichtgewerblichen Zwecken wie der wissenschaftlichen Forschung und durch KMU und Start-up-Unternehmen zu schaffen. In diesem Zusammenhang können öffentliche Stellen die Daten insbesondere KMU, Start-up-Unternehmen, kleinen Midcap-Unternehmen, der Zivilgesellschaft und Forschungs- und Bildungseinrichtungen auch gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung stellen. Öffentliche Stellen können zu diesem Zweck eine Liste der Kategorien von Weiterverwendern aufstellen, denen Daten oder Dokumente für die Weiterverwendung gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung gestellt werden. Diese Liste wird zusammen mit den Kriterien, die bei ihrer Aufstellung verwendet wurden, veröffentlicht.

(3) Gebühren werden aus den Kosten abgeleitet, die mit der Durchführung des Antragsverfahrens auf Weiterverwendung von bestimmten Kategorien geschützter Daten verbunden sind, und auf die für das Folgende erforderlichen Kosten beschränkt:

a) Vervielfältigung, Bereitstellung und Verbreitung der Daten,

b) Freigabe der Urheberrechte,

c) Anonymisierung oder sonstige Aufbereitung personenbezogener oder vertraulicher Geschäftsinformationen gemäß Artikel 32w Absatz 3 [Bedingungen für die Weiterverwendung],

d) Instandhaltung einer sicheren Verarbeitungsumgebung,

e) Erwerb des Rechts auf Erlaubnis der Weiterverwendung gemäß diesem Abschnitt von Dritten außerhalb des öffentlichen Sektors, Unterstützung von

Weiterverwendern bei der Einholung der Einwilligung der betroffenen Personen und der Erlaubnis der Dateninhaber, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten.

(4) Die Kriterien und die Methode für die Gebührenberechnung werden von den Mitgliedstaaten festgelegt und veröffentlicht. Die öffentliche Stelle veröffentlicht eine Beschreibung der wichtigsten Kostenarten und die Regeln der Kostenzuweisung.

(5) Öffentliche Stellen können in Bezug auf sehr große Unternehmen auf der Grundlage objektiver Kriterien und unter Berücksichtigung der Wirtschaftskraft oder der Fähigkeit des Unternehmens, Daten zu erwerben, einschließlich insbesondere der Benennung als Torwächter gemäß der Verordnung (EU) 2022/1925, höhere Gebühren erheben als nach den Absätzen 2 und 3 des vorliegenden Artikels zulässig. Solche berechneten Gebühren müssen verhältnismäßig sein. Zusätzlich zu den in Absatz 3 dieses Artikels aufgeführten Elementen können sie die Kosten für die Erfassung und Erstellung der Daten zuzüglich einer angemessenen Gewinnspanne abdecken.

Artikel 32z

Zuständige Stellen

(1) Für die Durchführung der in diesem Artikel genannten Aufgaben benennt jeder Mitgliedstaat gemäß Artikel 37 Absatz 1 eine oder mehrere zuständige Stellen, die für bestimmte Sektoren zuständig sein können, die zusammen aber alle Sektoren abdecken müssen, welche die öffentlichen Stellen, die Zugang zwecks Weiterverwendung von bestimmten Kategorien von geschützten Daten gewähren oder verweigern, unterstützen. Die Mitgliedstaaten können entweder eine oder mehrere neue zuständige Stellen einrichten oder sich auf bestehende öffentliche Stellen oder interne Dienste öffentlicher Stellen stützen, die die in diesem Abschnitt festgelegten Bedingungen erfüllen.

(2) Die zuständigen Stellen können nach dem Unionsrecht oder dem nationalen Recht, wenn darin eine solche Zugangsgewährung vorgesehen ist, befugt werden, den Zugang zwecks Weiterverwendung von bestimmten Kategorien geschützter Daten zu gewähren. Wenn sie den Zugang zwecks Weiterverwendung gewähren oder verweigern, unterliegen diese zuständigen Stellen den Artikeln 32k, 32w, 32x, 32y und 32ab.

(3) Die zuständigen Stellen müssen zur Erfüllung der ihnen übertragenen Aufgaben über angemessene rechtliche, finanzielle, technische und personelle Mittel, einschließlich der erforderlichen technischen Sachkenntnis, verfügen, damit sie in der Lage sind, das einschlägige Unionsrecht bzw. nationale Recht in Bezug auf die Regelungen für den Zugang zu Daten der in Artikel 2 Nummer 54 genannten geschützten Datenkategorien einzuhalten.

(4) Soweit erforderlich, beinhaltet die Unterstützung nach Absatz 1 Folgendes:

a) Leistung technischer Unterstützung durch Bereitstellung einer sicheren Verarbeitungsumgebung für die Gewährung des Zugangs zwecks Weiterverwendung von Daten oder Dokumenten,

b) Beratung und technische Unterstützung bei der bestmöglichen Strukturierung und Speicherung von Daten, um diese Daten oder Dokumente leicht zugänglich zu machen,

c) Bereitstellung technischer Unterstützung für Anonymisierung, Pseudonymisierung und modernste Methoden zum Schutz der Privatsphäre, nicht nur für personenbezogene Daten, sondern auch für vertrauliche Geschäftsinformationen, einschließlich Geschäftsgeheimnissen oder Inhalten, die durch Rechte des geistigen Eigentums geschützt sind,

d) gegebenenfalls Unterstützung der öffentlichen Stellen, damit sie Weiterverwendern bei der Einholung der Einwilligung der betroffenen Personen zur Weiterverwendung oder der Erlaubnis der Dateninhaber entsprechend ihrer besonderen Festlegungen Hilfestellung leisten, auch im Hinblick auf die Rechtsordnung, in der die Datenverarbeitung stattfinden soll, und Unterstützung der öffentlichen Stellen bei der Einrichtung technischer Mechanismen, mit denen Einwilligungsanfragen oder die Erlaubnis der Weiterverwender übermittelt werden können, soweit dies praktikabel ist,

e) Unterstützung öffentlicher Stellen bei der Beurteilung, ob die von einem Weiterverwender nach Artikel 32x Absatz 2 eingegangenen vertragliche Zusagen angemessen sind.

Artikel 32aa

Zentrale Informationsstelle

(1) Jeder Mitgliedstaat benennt eine einzige Informationsstelle. Diese Stelle stellt leicht zugängliche Informationen über die Anwendung der Artikel 32w, 32x und 32y zur Verfügung.

(2) Die zentrale Informationsstelle ist befugt, Anfragen oder Anträge in Bezug auf die Weiterverwendung von bestimmten Kategorien geschützter Daten entgegenzunehmen, und übermittelt diese – sofern möglich und angebracht durch automatisierte Verfahren – an die zuständigen öffentlichen Stellen oder gegebenenfalls an die in Artikel 32z Absatz 1 genannten zuständigen Stellen.

(3) Die zentrale Informationsstelle kann einen gesonderten, vereinfachten und gut dokumentierten Informationskanal für KMU, kleine Midcap-Unternehmen, Start-up-Unternehmen und Forschungseinrichtungen einrichten, der auf deren Bedarf und Kapazitäten mit Blick auf die Beantragung der Weiterverwendung von Daten der in Artikel 2 Nummer 54 genannten Datenkategorien abstellt.

(4) Die zentrale Informationsstelle stellt auf elektronischem Wege eine durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Dokumentressourcen, gegebenenfalls einschließlich der bei sektoralen, regionalen oder lokalen Informationsstellen verfügbaren Dokumentressourcen, und einschlägige Informationen mit einer Beschreibung der verfügbaren Daten und Dokumente bereit, die mindestens das Datenformat und den Datenumfang und die Bedingungen für ihre Weiterverwendung umfasst.

(5) Die Kommission richtet ein europaweites zentrales Zugangsportal ein, über das ein durchsuchbares elektronisches Verzeichnis der bei den zentralen nationalen Informationsstellen verfügbaren Daten oder Dokumente sowie weitere Informationen darüber bereitgestellt werden, wie über die zentralen nationalen Informationsstellen Daten oder Dokumente angefordert werden können.

Artikel 32ab

Verfahren für Anträge auf Weiterverwendung

(1) Sofern nicht gemäß dem nationalen Recht kürzere Fristen festgelegt sind, treffen die zuständigen öffentlichen Stellen oder die in Artikel 32z Absatz 1 genannten zuständigen Stellen eine Entscheidung über den Antrag auf Weiterverwendung von bestimmten Kategorien geschützter Daten innerhalb von zwei Monaten nach Eingang des Antrags.

(2) Bei außergewöhnlich umfangreichen und komplexen Anträgen auf Weiterverwendung kann diese Frist von zwei Monaten um bis zu 30 Tage verlängert werden. In solchen Fällen teilen die zuständigen öffentlichen Stellen oder die in Artikel 32z Absatz 1 genannten zuständigen Stellen dem Antragsteller möglichst bald mit, dass für die Durchführung des Verfahrens mehr Zeit benötigt wird, zusammen mit den Gründen für die Verzögerung.

(3) Jede natürliche oder juristische Person, die von einer Entscheidung gemäß Absatz 1 direkt betroffen ist, hat in dem Mitgliedstaat, in dem die betreffende Stelle ihren Sitz hat, einen wirksamen Rechtsbehelfsanspruch. Dieser Rechtsbehelfsanspruch ist durch das nationale Recht geregelt und umfasst die Möglichkeit der Überprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis, wie die nationale Wettbewerbsbehörde, die für den Zugang zu Dokumenten zuständige Behörde, die gemäß der Verordnung (EU) 2016/679 errichtete Aufsichtsbehörde oder ein nationales Gericht, deren Entscheidungen für die betreffende öffentliche Stelle oder die zuständige Stelle bindend sind.“

19. Artikel 38 erhält folgende Fassung:

„(1) Unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs haben natürliche und juristische Personen das Recht, einzeln oder gegebenenfalls gemeinsam eine Beschwerde einzureichen:

a) bei der jeweils zuständigen Behörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder ihrer Niederlassung, wenn sie der Auffassung sind, dass ihre Rechte nach dieser Verordnung verletzt wurden;

b) in Bezug auf alle Angelegenheiten, die in den Anwendungsbereich dieser Verordnung fallen und sich speziell gegen einen anerkannten Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation richten, bei der jeweils zuständigen Behörde für die Registrierung von Datenvermittlungsdiensten oder der jeweils zuständigen Behörde für die Registrierung von datenaltruistischen Organisationen.

(2) Der Datenkoordinator stellt natürlichen und juristischen Personen auf Anfrage alle erforderlichen Informationen bereit, damit sie bei der zuständigen Behörde Beschwerde einlegen können.

(3) Die zuständige Behörde, bei der die Beschwerde eingereicht wurde, teilt dem Beschwerdeführer im Einklang mit dem nationalen Recht Folgendes mit:

a) den Stand des Verfahrens, die getroffene Entscheidung und

b) die Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 39.“

20. In Artikel 40 wird folgender Absatz 6 eingefügt:

„(6) Dieser Artikel gilt nicht für Kapitel VIIc.“

21. Nach Artikel 41 wird folgende Überschrift eingefügt:

„KAPITEL IXa

Europäischer Dateninnovationsrat“

22. Folgender Artikel 41a wird eingefügt:

„Artikel 41a

Europäischer Dateninnovationsrat

(1) Der Europäische Dateninnovationsrat (EDIB) wird eingerichtet, um die Kommission bei der Koordinierung der Durchsetzung dieser Verordnung zu beraten und zu unterstützen und als Diskussionsforum für die Entwicklung einer europäischen Datenwirtschaft und Datenpolitik zu dienen.

(2) Er setzt sich mindestens aus Vertretern der Mitgliedstaaten, die für Fragen im Zusammenhang mit Daten zuständig sind, den für die Durchsetzung der Kapitel II, III, V, VIIa und VIIc dieser Verordnung zuständigen Behörden, dem Europäischen Datenschutzausschuss, dem Europäischen Datenschutzbeauftragten, der ENISA, dem KMU-Beauftragten der EU oder einem vom Netz der KMU-Beauftragten benannten Vertreter zusammen. Die Kommission kann beschließen, weitere Kategorien von Mitgliedern hinzuzufügen. Bei der Ernennung einzelner Sachverständiger strebt die Kommission im Hinblick auf die Zusammensetzung der Expertengruppe ein ausgewogenes Geschlechterverhältnis und geografische Ausgewogenheit unter den Mitgliedern der Gruppe an.

(3) Die Kommission entscheidet über die Zusammensetzung der verschiedenen Konfigurationen, in denen der Ausschuss seine Aufgaben erfüllen wird.

(4) Die Kommission führt den Vorsitz in den Sitzungen des Europäischen Dateninnovationsrats.“

23. Artikel 42 erhält folgende Fassung:

„Artikel 42

Rolle des Europäischen Dateninnovationsrats

(1) Der Europäische Dateninnovationsrat (EDIB) unterstützt die einheitliche Anwendung dieser Verordnung

a) indem er als Forum für strategische Diskussionen über Datenpolitik, Daten-Governance, internationalen Datenverkehr und sektorübergreifende Entwicklungen dient, die für die europäische Datenwirtschaft relevant sind,

b) durch Beratung und Unterstützung der Kommission in Bezug auf die Entwicklung einer kohärenten Praxis der zuständigen Behörden bei der Durchsetzung der Kapitel II, III, V, VII, VIIa und VIIc,

c) durch die Erleichterung der Zusammenarbeit zwischen den zuständigen Behörden mittels Kapazitätsaufbau und Informationsaustausch,

d) durch die Förderung des Austauschs von Erfahrungen und bewährten Verfahren zwischen den Mitgliedstaaten im Bereich der Weiterverwendung

von Informationen des öffentlichen Sektors in Zusammenarbeit mit anderen einschlägigen Verwaltungseinrichtungen.“

24. Artikel 45 wird wie folgt geändert:

a) Absatz 2 erhält folgende Fassung:

„(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 29 Absatz 7, Artikel 32u Absatz 2 und Artikel 33 Absatz 2 wird der Kommission auf unbestimmte Zeit übertragen.“

b) Absatz 3 erhält folgende Fassung:

„(3) Die Befugnisübertragung gemäß Artikel 29 Absatz 7, Artikel 32u Absatz 2 und Artikel 33 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.“

c) Absatz 6 erhält folgende Fassung:

„(6) Ein delegierter Rechtsakt, der gemäß Artikel 29 Absatz 7, Artikel 32u Absatz 2 und Artikel 33 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Veranlassung des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.“

25. Artikel 46 wird wie folgt geändert:

a) Absatz 1 Satz 1 erhält folgende Fassung:

„Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.“

b) Folgender Absatz 1a wird eingefügt:

„(1a) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 4 der Verordnung (EU) Nr. 182/2011.“

26. Artikel 49 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

i) Der einleitende Teil erhält folgende Fassung:

„(1) Bis zum 12. September 2028 führt die Kommission eine Bewertung der Kapitel II, III, IV, V, VI, VII und VIII durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über ihre wichtigsten Ergebnisse. Im Zuge dieser Bewertung wird insbesondere Folgendes geprüft:“

ii) Buchstabe m erhält folgende Fassung:

„m) die Auswirkung der vorliegenden Verordnung auf KMU und kleine Midcap-Unternehmen im Hinblick auf deren Innovationsfähigkeit und die Verfügbarkeit von Datenverarbeitungsdiensten für Nutzer in der Union sowie auf mit der Einhaltung der neuen Verpflichtungen verbundene Belastungen.“

b) Folgender Absatz 2a wird eingefügt:

„(2a) Bis zum [5 Jahre nach dem Datum des Inkrafttretens] führt die Kommission eine Bewertung der Kapitel VIIa, VIIb und VIIc dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über ihre wichtigsten Ergebnisse.

Dabei wird in dem Bericht insbesondere Folgendes bewertet:

a) Stand der Eintragungen der Datenvermittlungsdienste und Art der von ihnen angebotenen Dienste,

b) Art der eingetragenen datenaltruistischen Organisationen und ein Überblick über die mit der gemeinsamen Datennutzung verfolgten Zwecke von allgemeinem Interesse, um diesbezüglich klare Kriterien festzulegen,

c) Anwendungsbereich sowie soziale und wirtschaftliche Auswirkungen von Kapitel VIIc Abschnitt 2 einschließlich

d) des Steigerungsgrads der Weiterverwendung – vor allem durch KMU und kleine Midcap-Unternehmen – von Dokumenten des öffentlichen Sektors, auf die Absatz 2 von Kapitel VIIc anwendbar ist,

e) der Auswirkungen der hochwertigen Datensätze,

f) des Zusammenwirkens der Datenschutzvorschriften und der Möglichkeiten der Weiterverwendung;

g) Die Mitgliedstaaten übermitteln der Kommission alle erforderlichen Angaben zur Ausarbeitung des Berichts.“

c) Absatz 5 erhält folgende Fassung:

„(5) Die Kommission kann dem Europäischen Parlament und dem Rat auf der Grundlage der in den Absätzen 1, 2 und 2a genannten Berichte gegebenenfalls einen Gesetzgebungsvorschlag zur Änderung dieser Verordnung vorlegen.“

27. Anhang I wird gemäß dem Anhang II der vorliegenden Verordnung hinzugefügt.

Artikel 2

Änderungen der Verordnung (EU) 2018/1724

In der Tabelle in Anhang II der Verordnung (EU) 2018/1724 erhält der Eintrag „Gründung, Führung und Schließung eines Unternehmens“ folgende Fassung:

„Lebensereignisse Verfahren	Erwartete Ergebnisse, gegebenenfalls vorbehaltlich einer Bewertung des Antrags durch die zuständige Behörde

		gemäß nationalen Rechtsvorschriften
Gründung, Führung und Schließung eines Unternehmens	Meldung einer Geschäftstätigkeit, Zulassung zur Ausübung einer Geschäftstätigkeit, Änderung einer Geschäftstätigkeit und Einstellung einer Geschäftstätigkeit ausgenommen Insolvenz- oder Liquidationsverfahren, ausgenommen der erstmaligen Eintragung einer Geschäftstätigkeit in das Unternehmens-Register, und ausgenommen Eintragungen im Rahmen des Verfahren zur Gründung von – oder späteren Anmeldungen oder Einreichungen von Meldungen von – Gesellschaften oder Unternehmen im Sinne von Artikel 54 Absatz 2 AEUV	Bestätigung des Eingangs der Meldung oder Änderung einer Geschäftstätigkeit oder des Antrags auf Genehmigung der Geschäftstätigkeit
	Registrierung eines Arbeitgebers (einer natürlichen Person) bei obligatorischen Versorgungs- und Versicherungssystemen	Bestätigung der Registrierung oder Sozialversicherungs-Kennnummer
	Registrierung von Beschäftigten bei obligatorischen Versorgungs- und Versicherungssystemen	Bestätigung der Registrierung oder Sozialversicherungs-Kennnummer
	Einreichung einer Körperschaftsteuererklärung	Bestätigung des Eingangs der Erklärung
	Meldung an die Sozialversicherungssysteme bei Beendigung des Vertrags mit einem Beschäftigten, ausgenommen bei Verfahren zur kollektiven Beendigung von Arbeitnehmerverträgen	Bestätigung des Eingangs der Meldung
	Zahlung von Sozialbeiträgen für Beschäftigte	Empfangs- oder andere Art der Bestätigung der Zahlung der Sozialbeiträge für Beschäftigte
	Eintragung als Anbieter von Datenvermittlungsdiensten	Bestätigung der Eintragung
	Eintragung als in der Union anerkannte datenaltruistische	Bestätigung der Eintragung“

Artikel 3

Änderung der Verordnung (EU) 2016/679 (DSGVO)

Die Verordnung (EU) 2016/679 wird wie folgt geändert:

1. Artikel 4 wird wie folgt geändert:

   a) In Nummer 1 werden die folgenden Sätze angefügt:

   „Angaben zu einer natürlichen Person sind nicht notwendigerweise personenbezogene Daten für jede andere Person oder Einrichtung, nur weil eine andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung die natürliche Person, auf die sich die Angaben beziehen, in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel, nicht identifizieren kann; derartige Angaben werden für diese Einrichtung nicht allein deshalb personenbezogen, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können;“

   b) Folgende Nummern werden angefügt:

   „32. ‚Endeinrichtung‘ eine Endeinrichtung im Sinne des Artikels 1 Nummer 1 der Richtlinie 2008/63/EG;

   33. ‚elektronische Kommunikationsnetze‘ Kommunikationsnetze im Sinne der Begriffsbestimmung in Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972;

   34. ‚Webbrowser‘ einen Webbrowser im Sinne des Artikels 2 Nummer 11 der Verordnung (EU) 2022/1925;

   35. ‚Mediendienst‘ einen Mediendienst im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2024/1083;

   36. ‚Mediendiensteanbieter‘ einen Mediendiensteanbieter im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2024/1083;

   37. ‚Online-Schnittstelle‘ eine Online-Schnittstelle im Sinne des Artikels 3 Buchstabe m der Verordnung (EU) 2022/2065;

   38. ‚wissenschaftliche Forschung‘ jede Forschungstätigkeit, die auch Innovationen, wie etwa technologische Entwicklung und Demonstration, unterstützen kann. Mit diesen Tätigkeiten werden Beiträge zu den vorhandenen wissenschaftlichen Erkenntnissen geleistet oder vorhandene Erkenntnisse auf neuartige Weise angewendet; sie werden mit dem Ziel durchgeführt, zur Entwicklung des allgemeinen Wissens und des Wohlergehens der Gesellschaft beizutragen, wobei in dem betreffenden Forschungsbereich ethische Standards eingehalten werden. Dabei ist es nicht ausgeschlossen, dass die Forschung auch der Förderung eines gewerblichen Interesses dienen kann.“

2. Artikel 5 Absatz 1 Buchstabe b erhält folgende Fassung:

„für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 als vereinbar mit den ursprünglichen Zwecken, unabhängig von den Bedingungen des Artikels 6 Absatz 4 dieser Verordnung (‚Zweckbindung');"

3. Artikel 9 wird wie folgt geändert:

a) In Absatz 2 werden folgende Buchstaben angefügt:

„k) die Verarbeitung erfolgt im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells unter den in Absatz 5 genannten Bedingungen,

l) die Verarbeitung biometrischer Daten zum Zwecke der Bestätigung der Identität einer betroffenen Person (Überprüfung) ist erforderlich, sofern die biometrischen Daten oder die für die Überprüfung erforderlichen Mittel unter der alleinigen Kontrolle der betroffenen Person stehen."

b) Folgender Absatz wird angefügt:

„(5) Für die in Absatz 2 Buchstabe k genannte Verarbeitung werden geeignete organisatorische und technische Maßnahmen getroffen, um die Erhebung und sonstige Verarbeitung besonderer Kategorien personenbezogener Daten zu vermeiden. Stellt der Verantwortliche trotz der Umsetzung solcher Maßnahmen fest, dass in den für das Trainieren, Testen oder Validieren verwendeten Datensätzen oder im KI-System oder KI-Modell besondere Kategorien personenbezogener Daten enthalten sind, so entfernt er diese Daten. Erfordert das Entfernen dieser Daten einen unverhältnismäßigen Aufwand, so schützt der Verantwortliche diese Daten in jedem Fall unverzüglich wirksam davor, zur Erzeugung von Ergebnissen verwendet, offengelegt oder auf andere Weise Dritten zur Verfügung gestellt zu werden."

4. Artikel 12 Absatz 5 erhält folgende Fassung:

„(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person oder bei Anträgen nach Artikel 15 kann der Verantwortliche, wenn die betroffene Person die ihr durch diese Verordnung verliehenen Rechte zu anderen Zwecken als dem Schutz ihrer Daten missbraucht, entweder

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat nachzuweisen, dass der Antrag offenkundig unbegründet ist oder dass hinreichende Gründe für die Annahme bestehen, dass der Antrag exzessiv ist."

5. Artikel 13 Absatz 4 erhält folgende Fassung:

„(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn die personenbezogenen Daten im Rahmen einer klaren und begrenzten Beziehung zwischen betroffenen Personen und einem Verantwortlichen, der eine nicht datenintensive Tätigkeit ausübt, erhoben wurden und hinreichende Gründe für die Annahme bestehen, dass die betroffene Person bereits über die in Absatz 1 Buchstaben a und c genannten Informationen verfügt, es sei denn, der Verantwortliche übermittelt die Daten an andere Empfänger oder Kategorien von Empfängern, übermittelt die Daten in ein Drittland, führt eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absatz 1 durch oder die Verarbeitung hat voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen im Sinne des Artikels 35 zur Folge.“

6. In Artikel 13 wird folgender Absatz 5 angefügt:

„(5) Findet die Verarbeitung zu Zwecken der wissenschaftlichen Forschung statt und erweist sich die Bereitstellung von Informationen gemäß den Absätzen 1, 2 und 3 als unmöglich oder wäre sie vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien mit einem unverhältnismäßigen Aufwand verbunden, oder ist die Verpflichtung gemäß Absatz 1 des vorliegenden Artikels geeignet, die Verwirklichung der Ziele dieser Verarbeitung unmöglich zu machen oder ernsthaft zu beeinträchtigen, so muss der Verantwortliche die Informationen gemäß den Absätzen 1, 2 und 3 nicht bereitstellen. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.“

7. Artikel 22 Absätze 1 und 2 erhalten folgende Fassung:

„(1) Eine Entscheidung, die für eine betroffene Person Rechtswirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, darf nur dann ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhen, wenn diese Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen notwendig ist, unabhängig davon, ob die Entscheidung auf andere Weise als mit ausschließlich automatisierten Mitteln getroffen werden könnte,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.“

8. Artikel 33 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher

Personen zur Folge hat, meldet der Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich und nach Möglichkeit spätestens 96 Stunden, nachdem er davon Kenntnis erlangt hat, über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle der gemäß den Artikeln 55 und 56 zuständigen Aufsichtsbehörde. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 96 Stunden, so ist eine Begründung für die Verzögerung beizufügen.“

b) Folgender Absatz wird eingefügt:

„(1a) Bis zur Einrichtung der zentralen Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555 melden die Verantwortlichen Verletzungen des Schutzes personenbezogener Daten gemäß den Artikeln 55 und 56 weiterhin direkt der zuständigen Aufsichtsbehörde.“

c) Folgende Absätze werden angefügt:

„(6) Der Ausschuss erstellt einen Vorschlag für eine gemeinsame Vorlage für die Meldung einer Verletzung des Schutzes personenbezogener Daten an die in Absatz 1 genannte zuständige Aufsichtsbehörde und einen Vorschlag für eine Liste der Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person zur Folge hat, und übermittelt sie der Kommission. Die Vorschläge werden der Kommission innerhalb von [Amt für Veröffentlichungen: neun Monate nach dem Datum des Inkrafttretens dieser Verordnung] vorgelegt. Die Kommission überprüft sie nach sorgfältiger Abwägung wie erforderlich und ist befugt, sie im Wege eines Durchführungsrechtsakts gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 anzunehmen.

(7) Die Vorlage und die Liste nach Absatz 6 werden mindestens alle drei Jahre überprüft und soweit erforderlich aktualisiert. Der Ausschuss legt der Kommission seine Bewertung und etwaige Vorschläge für Aktualisierungen zu gegebener Zeit vor. Die Kommission überprüft die Vorschläge nach sorgfältiger Abwägung und ist befugt, nach dem Verfahren in Absatz 6 etwaige Aktualisierungen vorzunehmen.“

9. Artikel 35 wird wie folgt geändert:

a) Die Absätze 4, 5 und 6 erhalten folgende Fassung:

„(4) Der Ausschuss erstellt einen Vorschlag für eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und übermittelt ihn der Kommission.

(5) Der Ausschuss erstellt einen Vorschlag für eine Liste der Verarbeitungsvorgänge, für keine Datenschutz-Folgenabschätzung durchzuführen ist, und übermittelt ihn der Kommission.

(6) Der Ausschuss erstellt einen Vorschlag für eine gemeinsame Vorlage und eine gemeinsame Methodik für die Durchführung von Datenschutz-Folgenabschätzungen und übermittelt ihn der Kommission.“

b) Folgende Absätze werden eingefügt:

„(6a) Die Vorschläge für die in den Absätzen 4 und 5 genannten Listen sowie für die Vorlage und die Methode nach Absatz 6 werden der Kommission innerhalb von [Amt für Veröffentlichungen: neun Monate nach dem Datum des Inkrafttretens dieser Verordnung] vorgelegt. Die Kommission überprüft sie nach sorgfältiger Abwägung wie erforderlich und ist befugt, sie im Wege eines Durchführungsrechtsakts gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 anzunehmen.

(6b) Die Listen sowie die Vorlage und die Methodik nach Absatz 6a werden mindestens alle drei Jahre überprüft und soweit erforderlich aktualisiert. Der Ausschuss legt der Kommission seine Bewertung und etwaige Vorschläge für Aktualisierungen zu gegebener Zeit vor. Die Kommission überprüft die Vorschläge nach sorgfältiger Abwägung und ist befugt, nach dem Verfahren in Absatz 6a etwaige Aktualisierungen vorzunehmen.

(6c) Von den Aufsichtsbehörden erstellte und veröffentlichte Listen der Arten von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung erforderlich ist, und der Arten von Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist, bleiben so lange gültig, bis die Kommission den in Absatz 6a genannten Durchführungsrechtsakt erlässt.“

10. Folgender Artikel wird eingefügt:

„Artikel 41a

(1) Die Kommission kann Durchführungsrechtsakte erlassen, um Mittel und Kriterien festzulegen, mit denen bestimmt wird, ob Daten, die sich aus der Pseudonymisierung ergeben, für bestimmte Einrichtungen keine personenbezogenen Daten mehr darstellen.

(2) Für die Zwecke des Absatzes 1 wird die Kommission wie folgt tätig:

a) sie bewertet den Stand der verfügbaren Techniken,

b) sie entwickelt Kriterien und/oder Kategorien für Verantwortliche und Empfänger, um das Risiko einer Re-Identifizierung im Hinblick auf typische Empfänger von Daten zu bewerten.

(3) Die Umsetzung der in einem Durchführungsrechtsakt festgelegten Mittel und Kriterien kann als Kriterium verwendet werden, um nachzuweisen, dass Daten nicht zu einer Re-Identifizierung der betroffenen Personen führen können.

(4) Die Kommission bezieht den EDSA eng in die Ausarbeitung der Durchführungsrechtsakte ein. Der EDSA gibt innerhalb von acht Wochen nach Eingang des Entwurfs des Durchführungsrechtsakts der Kommission eine Stellungnahme dazu ab.

(5) Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 3 genannten Prüfverfahren erlassen.“

11. Artikel 57 Absatz 1 wird wie folgt geändert:

(a) Buchstabe k wird gestrichen.

12. Artikel 64 Absatz 1 Buchstabe a wird gestrichen.

13. Artikel 70 Absatz 1 Buchstabe h wird gestrichen.

14. In Artikel 70 Absatz 1 werden folgende Buchstaben eingefügt:

„ha) Ausarbeitung eines Vorschlags für eine Liste der Arten von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung erforderlich ist und für die keine Datenschutz-Folgenabschätzung gemäß Artikel 35 erforderlich ist, und Übermittlung dieses Vorschlags an die Kommission;

hb) Ausarbeitung eines Vorschlags für eine gemeinsame Vorlage und eine gemeinsame Methodik für die Durchführung von Datenschutz-Folgenabschätzungen gemäß Artikel 35 und Übermittlung dieses Vorschlags an die Kommission;

hc) Ausarbeitung eines Vorschlags für eine gemeinsame Vorlage für die Meldung einer Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde sowie für eine Liste der Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person nach Artikel 33 zur Folge hat, und Übermittlung dieses Vorschlags an die Kommission;“

15. Nach Artikel 88 wird folgender Artikel eingefügt:

„Artikel 88a

Verarbeitung personenbezogener Daten in Endeinrichtungen natürlicher Personen

(1) Die Speicherung personenbezogener Daten oder der Zugriff auf personenbezogene Daten, die bereits in der Endeinrichtung einer natürlichen Person gespeichert sind, ist nur zulässig, wenn diese Person im Einklang mit dieser Verordnung ihre Einwilligung erteilt hat.

(2) Absatz 1 steht der Speicherung personenbezogener Daten oder dem Zugriff auf bereits in der Endeinrichtung einer natürlichen Person gespeicherte personenbezogene Daten auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats im Sinne und unter den Bedingungen des Artikels 6 zur Wahrung der in Artikel 23 Absatz 1 genannten Ziele nicht entgegen.

(3) Die Speicherung personenbezogener Daten oder der Zugriff auf bereits gespeicherte personenbezogene Daten in der Endeinrichtung einer natürlichen Person ohne Einwilligung und die anschließende Verarbeitung sind rechtmäßig, soweit sie für einen der folgenden Zwecke erforderlich sind:

a) Durchführung der Übertragung einer elektronischen Kommunikation über ein elektronisches Kommunikationsnetz;

b) Erbringung einer von der betroffenen Person ausdrücklich verlangten Dienstleistung;

c) Erstellung aggregierter Informationen über die Nutzung eines Online-Dienstes zur Messung der Zielgruppe eines solchen Dienstes, wenn sie von dem für diesen Online-Dienst Verantwortlichen ausschließlich für seine eigene Nutzung durchgeführt wird;

d) Aufrechterhaltung oder Wiederherstellung der Sicherheit eines von dem Verantwortlichen bereitgestellten Dienstes, der von der betroffenen Person oder der für die Erbringung dieses Dienstes verwendeten Endeinrichtung verlangt wurde.

(4) Beruht die Speicherung personenbezogener Daten oder der Zugriff auf bereits in der Endeinrichtung gespeicherte personenbezogene Daten einer natürlichen Person auf einer Einwilligung, so gilt Folgendes:

a) die betroffene Person muss in der Lage sein, Einwilligungsanfragen auf einfache und verständliche Weise über eine Schaltfläche mit einem einzigen Klick oder mit gleichwertigen Mitteln abzulehnen;

b) erteilt die betroffene Person ihre Einwilligung, so stellt der Verantwortliche während des Zeitraums, in dem er sich rechtmäßig auf die Einwilligung der betroffenen Person stützen kann, keine neue Einwilligungsanfrage für denselben Zweck;

c) lehnt die betroffene Person eine Einwilligungsanfrage ab, so stellt der Verantwortliche für einen Zeitraum von mindestens sechs Monaten keine neue Einwilligungsanfrage für denselben Zweck.

Dieser Absatz gilt auch für die anschließende Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung.

(5) Dieser Artikel gilt ab dem [Amt für Veröffentlichungen: Bitte das Datum sechs Monate nach dem Datum des Inkrafttretens dieser Verordnung einfügen].

Artikel 88b

Automatisierte und maschinenlesbare Angaben zu den Wahlentscheidungen der betroffenen Person im Hinblick auf die Verarbeitung personenbezogener Daten in Endeinrichtungen natürlicher Personen

(1) Die Verantwortlichen stellen sicher, dass ihre Online-Schnittstellen es den betroffenen Personen ermöglichen,

a) die Einwilligung mit automatisierten und maschinenlesbaren Mitteln zu erteilen, sofern die in dieser Verordnung festgelegten Bedingungen für die Einwilligung erfüllt sind;

b) eine Einwilligungsanfrage mit automatisierten und maschinenlesbaren Mitteln abzulehnen und das Widerspruchsrecht gemäß Artikel 21 Absatz 2 auszuüben.

(2) Die Verantwortlichen beachten die von den betroffenen Personen gemäß Absatz 1 getroffenen Wahlentscheidungen.

(3) Die Absätze 1 und 2 gelten nicht für Verantwortliche, die Mediendiensteanbieter sind, wenn sie einen Mediendienst bereitstellen.

(4) Die Kommission beauftragt gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen mit der Ausarbeitung von Normen für die Auswertung maschinenlesbarer Angaben über die Wahlentscheidungen betroffener Personen.

Bei den von den Verantwortlichen verwendeten Online-Schnittstellen, die mit harmonisierten Normen oder Teilen davon übereinstimmen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht worden sind, wird eine Konformität mit den Anforderungen nach Absatz 1 vermutet, die von den betreffenden Normen oder Teilen davon abgedeckt ist.

(5) Die Artikel 1 und 2 gelten ab dem [Amt für Veröffentlichungen: Bitte das Datum 24 Monate nach dem Datum des Inkrafttretens dieser Verordnung einfügen].

(6) Anbieter von Webbrowsern, bei denen es sich nicht um KMU handelt, stellen die technischen Mittel bereit, die es den betroffenen Personen ermöglichen, ihre Einwilligung zu erteilen, eine Einwilligungsanfrage abzulehnen und das Widerspruchsrecht gemäß Artikel 21 Absatz 2 mithilfe der in Absatz 1 des

vorliegenden Artikels genannten automatisierten und maschinenlesbaren Mittel, wie sie gemäß den Absätzen 2 bis 5 des vorliegenden Artikels angewandt werden, auszuüben.

(7) Absatz 6 gilt ab dem [Amt für Veröffentlichungen: Bitte das Datum 48 Monate nach dem Datum des Inkrafttretens dieser Verordnung einfügen].

Artikel 88c

Verarbeitung im Zusammenhang mit der Entwicklung und dem Betrieb von KI

Ist die Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells im Interesse des Verantwortlichen erforderlich, so kann diese Verarbeitung gegebenenfalls aus berechtigtem Interesse im Sinne des Artikels 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 erfolgen, es sei denn, andere Rechtsvorschriften der Union oder der Mitgliedstaaten sehen ausdrücklich eine Einwilligung vor und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt.

Eine solche Verarbeitung unterliegt geeigneten organisatorischen, technischen Maßnahmen und Garantien für die Rechte und Freiheiten der betroffenen Person, zum Beispiel um in der Phase der Auswahl der Quellen und des Trainings und Testens von KI-Systemen oder KI-Modellen die Einhaltung der Datenminimierung sicherzustellen, im KI-System oder KI-Modell auf Vorrat gespeicherte Daten vor der Offenlegung zu schützen, für mehr Transparenz für die betroffenen Personen zu sorgen und den betroffenen Personen ein bedingungsloses Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzuräumen.“

Artikel 4

Änderung der Verordnung (EU) 2018/1725 [EU-DSVO]

Die Verordnung (EU) 2018/1725 wird wie folgt geändert:

1. Artikel 3 wird wie folgt geändert:

a) In Nummer 1 werden die folgenden Sätze angefügt:

„Angaben zu einer natürlichen Person sind nicht notwendigerweise personenbezogene Daten für jede andere Person oder Einrichtung, nur weil eine andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung die natürliche Person, auf die sich die Angaben beziehen, in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel, nicht identifizieren kann; derartige Angaben werden für diese Einrichtung nicht allein deshalb personenbezogen, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können;“

b) Nummer 25 erhält folgende Fassung:

„25. ‚elektronische Kommunikationsnetze‘ Kommunikationsnetze im Sinne der Begriffsbestimmung in Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972;’

c) Folgende Nummern werden angefügt:

„27. ‚mobile Anwendung‘ eine mobile Anwendung im Sinne des Artikels 3 Nummer 2 der Richtlinie (EU) 2016/2102;

28. ‚Online-Schnittstelle‘ eine Online-Schnittstelle im Sinne des Artikels 3 Buchstabe m der Verordnung (EU) 2022/2065;

29. ‚wissenschaftliche Forschung‘ jede Forschungstätigkeit, die auch Innovationen, wie etwa technologische Entwicklung und Demonstration, unterstützen kann. Mit diesen Tätigkeiten werden Beiträge zu den vorhandenen wissenschaftlichen Erkenntnissen geleistet oder vorhandene Erkenntnisse auf neuartige Weise angewendet; sie werden mit dem Ziel durchgeführt, zur Entwicklung des allgemeinen Wissens und des Wohlergehens der Gesellschaft beizutragen, wobei in dem betreffenden Forschungsbereich ethische Standards eingehalten werden. Dabei ist es nicht ausgeschlossen, dass die Forschung auch der Förderung eines gewerblichen Interesses dienen kann.“

2. Artikel 4 Absatz 1 Buchstabe b erhält folgende Fassung:

„b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 13 als vereinbar mit den ursprünglichen Zwecken, unabhängig von den Bedingungen des Artikels 6 dieser Verordnung (‚Zweckbindung‘),“

3. Artikel 10 wird wie folgt geändert:

a) In Absatz 2 werden folgende Buchstaben angefügt:

„k) die Verarbeitung erfolgt im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells unter den in Absatz 4 genannten Bedingungen,

l) die Verarbeitung biometrischer Daten zum Zwecke der Bestätigung der Identität einer betroffenen Person (Überprüfung) ist erforderlich, sofern die biometrischen Daten oder die für die Überprüfung erforderlichen Mittel unter der alleinigen Kontrolle der betroffenen Person stehen.“

b) Folgender Absatz 4 wird angefügt:

„(4) Für die in Absatz 2 Buchstabe k genannte Verarbeitung werden geeignete organisatorische und technische Maßnahmen getroffen, um die Erhebung und sonstige Verarbeitung besonderer Kategorien personenbezogener Daten zu vermeiden. Stellt der Verantwortliche trotz der Umsetzung solcher Maßnahmen fest, dass in den für das Trainieren, Testen oder Validieren verwendeten Datensätzen oder im KI-System oder KI-Modell besondere Kategorien personenbezogener Daten enthalten sind, so entfernt er diese Daten. Erfordert das Entfernen dieser Daten einen unverhältnismäßigen Aufwand, so

schützt der Verantwortliche diese Daten in jedem Fall unverzüglich wirksam davor, zur Erzeugung von Ergebnissen verwendet, offengelegt oder auf andere Weise Dritten zur Verfügung gestellt zu werden.“

4. Artikel 14 Absatz 5 erhält folgende Fassung:

„(5) Informationen gemäß den Artikeln 15 und 16 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 17 bis 24 und Artikel 35 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person oder bei Anträgen nach Artikel 17 kann der Verantwortliche, wenn die betroffene Person die ihr durch diese Verordnung verliehenen Rechte zu anderen Zwecken als dem Schutz ihrer Daten missbraucht, sich weigern, dem Antrag nachzukommen. Der Verantwortliche hat nachzuweisen, dass der Antrag offenkundig unbegründet ist oder dass hinreichende Gründe für die Annahme bestehen, dass der Antrag exzessiv ist.“

5. In Artikel 15 wird folgender neuer Absatz 5 angefügt:

„(5) Findet die Verarbeitung zu Zwecken der wissenschaftlichen Forschung statt und erweist sich die Bereitstellung von Informationen gemäß den Absätzen 1, 2 und 3 als unmöglich oder wäre sie vorbehaltlich der in Artikel 13 genannten Bedingungen und Garantien mit einem unverhältnismäßigen Aufwand verbunden, oder ist die Verpflichtung gemäß Absatz 1 des vorliegenden Artikels geeignet, die Verwirklichung der Ziele dieser Verarbeitung unmöglich zu machen oder ernsthaft zu beeinträchtigen, so muss der Verantwortliche die Informationen gemäß den Absätzen 1, 2 und 3 nicht bereitstellen. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.“

6. Artikel 24 Absätze 1 und 2 erhalten folgende Fassung:

„(1) Eine Entscheidung, die für eine betroffene Person Rechtswirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, darf nur dann ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhen, wenn diese Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen notwendig ist, unabhängig davon, ob die Entscheidung auf andere Weise als mit ausschließlich automatisierten Mitteln getroffen werden könnte;

b) aufgrund von Rechtsvorschriften der Union, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.“

7. Artikel 34 Absatz 1 erhält folgende Fassung:

„(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, meldet der Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich und nach Möglichkeit

spätestens 96 Stunden, nachdem er davon Kenntnis erlangt hat, dem Europäischen Datenschutzbeauftragten. Erfolgt die Meldung an den Europäischen Datenbeauftragten nicht binnen 96 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.“

8. In Artikel 37 werden die folgenden Absätze angefügt:

„(2) Die Speicherung personenbezogener Daten oder der Zugriff auf personenbezogene Daten, die bereits in der Endeinrichtung einer natürlichen Person gespeichert sind, ist nur zulässig, wenn diese Person im Einklang mit dieser Verordnung ihre Einwilligung erteilt hat.

(3) Absatz 1 steht der Speicherung personenbezogener Daten oder dem Zugriff auf bereits in der Endeinrichtung einer natürlichen Person gespeicherte personenbezogene Daten auf der Grundlage des Unionsrechts im Sinne und unter den Bedingungen des Artikels 5 zur Wahrung der in Artikel 25 Absatz 1 genannten Ziele nicht entgegen.

(4) Die Speicherung personenbezogener Daten oder der Zugriff auf bereits gespeicherte personenbezogene Daten in der Endeinrichtung einer natürlichen Person ohne Einwilligung und die anschließende Verarbeitung sind rechtmäßig, soweit sie für einen der folgenden Zwecke erforderlich sind:

a) Durchführung der Übertragung einer elektronischen Kommunikation über ein elektronisches Kommunikationsnetz,

b) Erbringung einer von der betroffenen Person ausdrücklich verlangten Dienstleistung,

c) Erstellung aggregierter Informationen über die Nutzung eines Online-Dienstes zur Messung der Zielgruppe eines solchen Dienstes, wenn sie von dem für diesen Online-Dienst Verantwortlichen ausschließlich für seine eigene Nutzung durchgeführt wird,

d) Aufrechterhaltung oder Wiederherstellung der Sicherheit eines von dem Verantwortlichen bereitgestellten Dienstes, der von der betroffenen Person oder der für die Erbringung dieses Dienstes verwendeten Endeinrichtung verlangt wurde.

(5) Beruht die Speicherung personenbezogener Daten oder der Zugriff auf bereits in der Endeinrichtung gespeicherte personenbezogene Daten einer natürlichen Person auf einer Einwilligung, so gilt Folgendes:

a) die betroffene Person muss in der Lage sein, Einwilligungsanfragen auf einfache und verständliche Weise über eine Schaltfläche mit einem einzigen Klick oder mit gleichwertigen Mitteln abzulehnen,

b) gibt die betroffene Person ihre Einwilligung, so stellt der Verantwortliche während des Zeitraums, in dem er sich rechtmäßig auf die Einwilligung der betroffenen Person stützen kann, keine neue Einwilligungsanfrage für denselben Zweck,

c) lehnt die betroffene Person eine Einwilligungsanfrage ab, so stellt der Verantwortliche für einen Zeitraum von mindestens sechs Monaten keine neue Einwilligungsanfrage für denselben Zweck.

Dieser Absatz gilt auch für die anschließende Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung.

(6) Dieser Artikel gilt ab dem [Amt für Veröffentlichungen: Bitte das Datum sechs Monate nach dem Datum des Inkrafttretens dieser Verordnung einfügen].

(7) Die Verantwortlichen stellen sicher, dass ihre Online-Schnittstellen es den betroffenen Personen ermöglichen,

a) die Einwilligung mit automatisierten und maschinenlesbaren Mitteln zu erteilen, sofern die in dieser Verordnung festgelegten Bedingungen für die Einwilligung erfüllt sind,

b) eine Einwilligungsanfrage mit automatisierten und maschinenlesbaren Mitteln abzulehnen.

(8) Die Verantwortlichen beachten die von den betroffenen Personen gemäß Absatz 7 getroffenen Wahlentscheidungen.

(9) Bei den von den Verantwortlichen verwendeten Online-Schnittstellen, die mit harmonisierten Normen oder Teilen davon übereinstimmen, auf die in Artikel 88b Absatz 4 der Verordnung (EU) 2016/679 Bezug genommen wird, wird eine Konformität mit den Anforderungen nach Absatz 7 vermutet, die von den betreffenden Normen oder Teilen davon abgedeckt ist.

(10) Die Artikel 7 und 9 gelten ab dem [Amt für Veröffentlichungen: Bitte das Datum 24 Monate nach dem Datum des Inkrafttretens dieser Verordnung einfügen].“

8. Artikel 39 wird wie folgt geändert:

a) Absatz 4 erhält folgende Fassung:

„(4) Die Listen, die Vorlage und die Methode, die von der Kommission angenommen wurden und auf die in Artikel 35 Absatz 6a der Verordnung (EU) 2016/679 Bezug genommen wird, sollten für die Verarbeitung personenbezogener Daten nach der vorliegenden Verordnung gelten.“

b) Die Absätze 5 und 6 werden gestrichen.

9. Folgender Artikel wird angefügt:

„Artikel 45a

Die von der Kommission angenommenen und in Artikel 41a der Verordnung (EU) 2016/679 genannten gemeinsamen Kriterien sollten für die Verarbeitung personenbezogener Daten nach der vorliegenden Verordnung gelten.“

Artikel 5

Änderung der Richtlinie 2002/58/EG (e-Datenschutzrichtlinie)

Die Richtlinie 2002/58/EG wird wie folgt geändert:

1. Artikel 4 wird gestrichen.

2. In Artikel 5 Absatz 3 wird folgender Unterabsatz angefügt:

„Dieser Absatz findet keine Anwendung, wenn es sich bei dem Teilnehmer oder Nutzer um eine natürliche Person handelt und die gespeicherten oder abgerufenen Informationen eine Verarbeitung personenbezogener Daten darstellen oder zu einer solchen Verarbeitung führen.“

Artikel 6

Änderung der Richtlinie (EU) 2022/2555

Die Richtlinie (EU) 2022/2555 wird wie folgt geändert:

1. Folgender Artikel 23a wird eingefügt:

„Artikel 23a

Zentrale Anlaufstelle zur Meldung von Vorfällen

(1) Die ENISA entwickelt und unterhält eine zentrale Anlaufstelle, um die Erfüllung der Pflicht zur Meldung von Sicherheitsvorfällen und damit zusammenhängenden Ereignissen gemäß den Rechtsakten der Union zu unterstützen, soweit diese Rechtsakte der Union dies vorsehen (im Folgenden „zentrale Anlaufstelle “). Unbeschadet des Artikels 16 der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates kann die ENISA sicherstellen, dass die zentrale Anlaufstelle auf der gemäß der genannten Verordnung eingerichteten einheitlichen Meldeplattform aufbaut.

(2) Die ENISA ergreift geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen, um die Risiken für die Sicherheit der zentralen Anlaufstelle und der über die zentrale Anlaufstelle übermittelten oder verbreiteten Informationen zu steuern. Die ENISA berücksichtigt gemäß den in Absatz 1 genannten Rechtsakten der Union die Sensibilität der Informationen, die übermittelt oder verbreitet werden, und stellt sicher, dass die nach diesen Rechtsakten der Union zuständigen Behörden Zugang zu den Informationen haben und sie gemäß diesen Rechtsakten der Union verarbeiten.

(3) Die ENISA legt die Spezifikationen für die technischen, operativen und organisatorischen Maßnahmen im Hinblick auf die Errichtung, die Wartung und den sicheren Betrieb der zentralen Anlaufstelle fest und setzt sie um. Die ENISA erarbeitet die Spezifikationen gemäß den in Absatz 1 genannten Rechtsakten der Union in Zusammenarbeit mit der Kommission, dem CSIRTs-Netzwerk und den zuständigen Behörden. Mit den Spezifikationen wird sichergestellt, dass

a) für die erforderliche Fähigkeit zur Interoperabilität in Bezug auf andere einschlägige Meldepflichten gemäß Absatz 1 gesorgt ist;

b) technische Vorkehrungen getroffen wurden, damit die einschlägigen Einrichtungen und Behörden nach den in Absatz 1 genannten Rechtsakten der Union auf Informationen der zentralen Anlaufstelle zugreifen, diese übermitteln, abrufen, übertragen oder anderweitig verarbeiten können, und technische Protokolle und Werkzeuge bereitgestellt werden, die es den Einrichtungen und Behörden ermöglichen, die erhaltenen Informationen in ihren Systemen weiter zu verarbeiten;

c) den Besonderheiten der Anforderungen für die Meldung von Vorfällen, die in den in Absatz 1 genannten Rechtsakten der Union festgelegt sind, gebührend Rechnung getragen wird;

d) die zentrale Anlaufstelle soweit erforderlich mit den in dem [*Vorschlag für eine Verordnung: Titel des Vorschlags einfügen*] genannten europäischen Unternehmensbrieftaschen interoperabel und kompatibel ist und dass die europäischen Unternehmensbrieftaschen zumindest zur Identifizierung und

Authentifizierung von Einrichtungen über die zentrale Anlaufstelle verwendet werden können;

e) Einrichtungen, die die zentrale Anlaufstelle nutzen, Informationen, die sie zuvor über die zentrale Anlaufstelle übermittelt haben, abrufen und ergänzen können;

f) eine einzige Meldung der Informationen, die von einer Einrichtung über die zentrale Anlaufstelle übermittelt werden, zur Erfüllung der Meldepflichten gemäß einem anderen Rechtsakt der Union, der die Meldung von Vorfällen an die zentrale Anlaufstelle vorsieht, verwendet werden kann.

(4) Sofern in den in Absatz 1 genannten Rechtsakten der Union nichts anderes vorgesehen ist, hat die ENISA keinen Zugang zu den über die zentrale Anlaufstelle übermittelten Meldungen.

(5) Innerhalb von [18] Monaten nach Inkrafttreten dieser Verordnung erprobt die ENISA die Funktionsweise der zentralen Anlaufstelle für jeden hinzugefügten Rechtsakt der Union, unter anderem durch Tests, bei denen die Besonderheiten und Anforderungen für die Meldungen gemäß dem jeweiligen Rechtsakt der Union berücksichtigt werden, und nach Konsultation der Kommission und der gemäß den jeweiligen Rechtsakten der Union zuständigen Behörden. Die ENISA ermöglicht die Meldung von Vorfällen im Rahmen jedes in Absatz 1 genannten Rechtsakts der Union erst, nachdem sie die Funktionsweise erprobt hat und nachdem die Kommission gemäß Absatz 6 eine Bekanntmachung veröffentlicht hat.

(6) Die Kommission bewertet in Zusammenarbeit mit der ENISA die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität und die Vertraulichkeit der zentralen Anlaufstelle. Stellt die Kommission nach Konsultation des CSIRTs-Netzwerks und der nach den in Absatz 1 genannten Rechtsakten der Union zuständigen Behörden fest, dass die zentrale Anlaufstelle die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität und die Vertraulichkeit sicherstellt, so veröffentlicht sie im *Amtsblatt der Europäischen Union* eine entsprechende Bekanntmachung.

(7) Gelangt die Kommission bei ihrer Bewertung zu dem Schluss, dass die zentrale Anlaufstelle die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität oder die Vertraulichkeit nicht sicherstellt, ergreift die ENISA in Zusammenarbeit mit der Kommission unverzüglich alle erforderlichen Korrekturmaßnahmen, um die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität oder die Vertraulichkeit unverzüglich sicherzustellen, und unterrichtet die Kommission über die Ergebnisse. Danach überprüft die Kommission die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität oder die Vertraulichkeit der zentralen Anlaufstelle und veröffentlicht gemäß Absatz 6 eine Bekanntmachung.“

2. Artikel 23 wird wie folgt geändert:

a) Absatz 1 Satz 1 erhält folgende Fassung:

„Jeder Mitgliedstaat stellt sicher, dass wesentliche und wichtige Einrichtungen über die gemäß Artikel 23a eingerichtete zentrale Anlaufstelle ihr CSIRT oder soweit erforderlich ihre zuständigen Behörde gemäß Absatz 4 dieses Artikels unverzüglich über jeden Vorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat.“

b) Folgender Absatz 12 wird angefügt:

„Meldet ein Hersteller einen schwerwiegenden Sicherheitsvorfall gemäß Artikel 14 Absatz 3 der Verordnung (EU) 2024/2847 und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel einschlägige Informationen gemäß Absatz 4 des vorliegenden Artikels, so gilt die Meldung des Herstellers nach Artikel 14 Absatz 3 der Verordnung (EU) 2024/2847 auch als Meldung von Informationen gemäß Absatz 4 des vorliegenden Artikels."

3. Artikel 30 Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten stellen sicher, dass zusätzlich zu der Meldepflicht nach Artikel 23 Meldungen den CSIRTs oder soweit erforderlich den zuständigen Behörden auf freiwilliger Basis über die gemäß Artikel 23a eingerichtete zentrale Anlaufstelle übermittelt werden können, und zwar durch

a) wesentliche und wichtige Einrichtungen in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle;

b) andere als die in Buchstabe a genannten Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, in Bezug auf erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle."

Artikel 7

Änderung der Verordnung (EU) Nr. 910/2014

Die Verordnung (EU) Nr. 910/2014 wird wie folgt geändert:

1. In Artikel 19a wird folgender Absatz 1a eingefügt:

„(1a) „Meldungen gemäß Absatz 1 Buchstabe b des vorliegenden Artikels an die Aufsichtsstelle und gegebenenfalls an andere jeweils zuständige Behörden erfolgen über die zentrale Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555."

2. In Artikel 24 wird folgender Absatz 2a eingefügt:

„(2a) Meldungen nach Absatz 2 Buchstabe fb des vorliegenden Artikels an die Aufsichtsstelle und soweit erforderlich an andere einschlägige zuständige Stellen erfolgen über die zentrale Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555."

3. In Artikel 45a wird folgender Absatz 3a eingefügt:

„(3a) Meldungen nach Absatz 3 an die Kommission und die zuständige Aufsichtsstelle erfolgen über die zentrale Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555."

Artikel 8

Änderungen der Verordnung (EU) 2022/2554

Artikel 19 der Verordnung (EU) 2022/2554 wird wie folgt geändert:

1. Absatz 1 Unterabsatz 1 erhält folgende Fassung:

„Finanzunternehmen melden der nach Artikel 46 jeweils zuständigen Behörde gemäß Absatz 4 des vorliegenden Artikels schwerwiegende IKT-bezogene Vorfälle über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle.“

2. Absatz 2 Unterabsatz 1 erhält folgende Fassung:

„Finanzunternehmen können der jeweils zuständigen Behörde auf freiwilliger Basis über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist. Die jeweils zuständige Behörde kann derartige Informationen anderen in Absatz 6 genannten einschlägigen Behörden zur Verfügung stellen.“

Artikel 9

Änderung der Richtlinie (EU) 2022/2557

Artikel 15 der Richtlinie (EU) 2022/2557 wird wie folgt geändert:

1. Absatz 1 Satz 1 erhält folgende Fassung:

„Die Mitgliedstaaten stellen sicher, dass die kritischen Einrichtungen der zuständigen Behörde über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle alle Vorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder erheblich stören könnten, unverzüglich melden.“

2. In Absatz 2 wird folgender Unterabsatz angefügt:

„Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art und das Format der gemäß Artikel 15 Absatz 1 gemeldeten Informationen genauer festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 24 Absatz 2 genannten Prüfverfahren erlassen.“

Artikel 10

Aufhebungen und Übergangsklauseln

(1) Die Verordnung (EU) 2019/1150/EU wird mit Wirkung vom [Datum des Inkrafttretens der vorliegenden Verordnung] aufgehoben.

(2) Abweichend von Absatz 1 gelten die folgenden Bestimmungen weiterhin bis zum 31. Dezember 2032:

(a) Artikel 2 Nummer 1,

(b) Artikel 2 Nummer 2,

(c) Artikel 2 Nummer 5,

(d) Artikel 4,

(e) Artikel 11,

(f) Artikel 15.

(3) Die folgenden Rechtsakte werden mit Wirkung vom [Datum des Inkrafttretens der Änderungen] aufgehoben:

a) die Verordnung (EU) 2022/868,

b) die Verordnung (EU) 2018/1807,

c) die Richtlinie (EU) 2019/1024.

(4) Bezugnahmen auf die Verordnung (EU) 2022/868, die Verordnung (EU) 2018/1807 und die Richtlinie (EU) 2019/1024 sind nach Maßgabe der Entsprechungstabelle in Anhang I der vorliegenden Verordnung zu lesen.

Artikel 11

Schlussbestimmungen

Diese Verordnung tritt am dritten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Abweichend von Absatz 3 tritt Artikel 5 Absatz 2 sechs Monate nach der Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 3 Absatz 8 Buchstaben a bis c, Artikel 6 Absätze 2 und 3 und Artikel 7 bis 9 treten 18 Monate nach Inkrafttreten dieser Verordnung in Kraft. Abweichend von Satz 1 treten die Pflichten zur Meldung über die zentrale Anlaufstelle gemäß Artikel 23 Absatz 4 der Richtlinie (EU) 2022/2555, Artikel 19a Absatz 1a, Artikel 24 Absatz 2a und Artikel 45a Absatz 3a der Verordnung (EU) Nr. 910/2014, Artikel 33 Absatz 1 der Verordnung (EU) 2016/679, Artikel 19 Absätze 1 und 2 der Verordnung (EU) 2022/2554 und Artikel 15 Absatz 1 der Richtlinie (EU) 2022/2557 24 Monate nach dem Inkrafttreten der vorliegenden Verordnung in Kraft, wenn die Kommission in ihrer Bewertung gemäß Artikel 23a Absatz 7 der Richtlinie (EU) 2022/2555 feststellt, dass die zentrale Anlaufstelle die ordnungsgemäße Funktionsweise, die Zuverlässigkeit, die Integrität oder die Vertraulichkeit nicht sicherstellt.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Die Präsidentin*

FINANZ- UND DIGITALBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Vereinfachung des digitalen Besitzstands, zur Änderung der Verordnungen (EU) 2023/2854, (EU) 2016/679, (EU) 2024/1689 und der Richtlinien 2002/58/EG und (EU) 2022/2555 sowie zur Aufhebung der Verordnungen (EU) 2022/868, (EU) 2018/1807, (EU) 2019/1150 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung für den digitalen Besitzstand)

1.2. Politikbereich(e)

Kommunikationsnetze, Inhalte und Technologien;

Binnenmarkt, Industrie, Unternehmertum und KMU

1.3. Ziel(e)

1.3.1. Allgemeine(s) Ziel(e)

Vereinfachung der Anwendung des digitalen Besitzstands und Kosteneinsparungen für Unternehmen

1.3.2. Einzelziel(e)

Einzelziel Nr. 1

Verbesserung der Governance und der wirksamen Durchsetzung des digitalen Besitzstands durch die Verringerung der Komplexität der Vorschriften, der Verwaltungskosten für Unternehmen und der Verwaltungskosten sowie durch die Aufhebung von Rechtsakten

Einzelziel Nr. 2

Bereitstellung einer zentralen Anlaufstelle zur Meldung von Vorfällen im Anwendungsbereich mehrerer Rechtsrahmen

1.3.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken sollte.

Geringere Kosten für Unternehmen infolge der Verringerung der Komplexität der Rechtsvorschriften und der Straffung der Berichterstattung

1.3.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren die Fortschritte und Ergebnisse verfolgt werden sollen.

Indikator 1

Berechnete Kostensenkungen für Unternehmen

Indikator 2

Kosteneinsparungen bei der Meldung von Sicherheitsvorfällen durch Unternehmen

Indikator 3

1.4. Der Vorschlag/Die Initiative betrifft

☐ eine neue Maßnahme

☐ eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme[39]

☒ die Verlängerung einer bestehenden Maßnahme

☐ die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Das Inkrafttreten wird innerhalb von drei Tagen nach der Veröffentlichung im Amtsblatt erwartet. Das Inkrafttreten sollte unmittelbar erfolgen, mit nennenswerten Ausnahmen für Vorschriften, die einen Übergangszeitraum erfordern. Für Kapitel III über die Meldung von Sicherheitsvorfällen und plattformbezogene Vorschriften ist ein ausreichender Zeitraum für die Umsetzung erforderlich, der an die Bedürfnisse der Unternehmen, der Mitgliedstaaten und der Unionsorgane angepasst ist.

1.5.2Mehrwert aufgrund des Tätigwerdens der EU (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größere Wirksamkeit oder Komplementarität). Für die Zwecke dieses Abschnitts bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der EU" den Wert, der sich aus dem Tätigwerden der EU ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Die Gründe für Maßnahmen auf EU-Ebene ergeben sich daraus, dass die Änderungen bestehende EU-Rechtsvorschriften betreffen und die Komplexität des Unionsrechts dadurch verringert wird (ex ante).

Der erwartete EU-Mehrwert (ex post) besteht in der Straffung des Unionsrechts, der Verringerung des Verwaltungsaufwands und der Senkung der Kosten für Unternehmen.

Bei der Einrichtung der zentralen Anlaufstelle zur Meldung von Vorfällen ergibt sich der besondere Mehrwert aus der Bereitstellung einer Lösung auf Unionsebene, mit der den nationalen Anforderungen Rechnung getragen wird. Die Kosten für Unternehmen werden optimiert, indem eine zentrale Anlaufstelle bereitgestellt wird, unabhängig davon, wo in der Union die meldende Einrichtung ansässig ist und welche Behörden mit der Entgegennahme der Meldungen beauftragt sind.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die Änderungen der jeweiligen Verordnungen stützen sich auf die praktischen Erfahrungen bei der Umsetzung der Vorschriften, wie in der beigefügten Arbeitsunterlage der Kommissionsdienststellen dargelegt. Sie beruhen auf einer umfassenden Konsultation der Interessenträger, bei der der Schwerpunkt in erster Linie auf der täglichen Anwendung der Vorschriften lag.

[39] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Die Änderungen sind mit dem mehrjährigen Finanzrahmen vereinbar, da keine zusätzlichen Ausgaben vorgesehen sind.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

–

1.6. Laufzeit der vorgeschlagenen Maßnahme/Initiative und der finanziellen Auswirkungen

5. ☐ Befristete Laufzeit

   ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

   ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ

6. ☒ Unbefristete Laufzeit

   Anlaufphase von JJJJ bis JJJJ

   Anschließend reguläre Umsetzung

1.7. Vorgeschlagene Haushaltsvollzugsart(en)[40]

7. ☒ **Direkte Mittelverwaltung** durch die Kommission

   ☒ über ihre Dienststellen, einschließlich ihres Personals in den EU-Delegationen

   ☐ über Exekutivagenturen

8. ☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

9. ☐ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

   ☐ Drittländer oder die von ihnen benannten Einrichtungen

   ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

   ☐ die Europäische Investitionsbank und den Europäischen Investitionsfonds

   ☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

   ☐ öffentlich-rechtliche Körperschaften

   ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern ihnen ausreichende finanzielle Garantien bereitgestellt werden

[40] Erläuterungen zu den Haushaltsvollzugsarten und Verweise auf die Haushaltsordnung finden sich auf der Website BUDGpedia (in englischer Sprache): https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und denen ausreichende finanzielle Garantien bereitgestellt werden

☐ Einrichtungen oder Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der Gemeinsamen Außen- und Sicherheitspolitik im Rahmen des Titels V des Vertrags über die Europäische Union betraut und die in dem maßgeblichen Basisrechtsakt benannt sind

☐ in einem Mitgliedstaat ansässige Einrichtungen, die dem Privatrecht eines Mitgliedstaats oder dem Unionsrecht unterliegen und im Einklang mit sektorspezifischen Vorschriften für die Betrauung mit der Ausführung von Unionsmitteln oder mit der Erteilung von Haushaltsgarantien in Betracht kommen, insofern diese Einrichtungen von privatrechtlichen, im öffentlichen Auftrag tätig werdenden Einrichtungen kontrolliert und von den Kontrollstellen mit angemessenen finanziellen Garantien mit gesamtschuldnerischer Haftung oder gleichwertigen finanziellen Garantien ausgestattet werden, die bei jeder Maßnahme auf den Höchstbetrag der Unionsunterstützung begrenzt sein können.

I

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

10. Die Änderungen werden als Teil der geänderten Rechtsvorschriften überwacht.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Haushaltsvollzugsart(en), des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

11. Die Verwaltungs- und Kontrollsysteme, die bei den bestehenden Rechtsvorschriften Anwendung finden, stellen auch für die Änderungen eine wirksame Kontrolle sicher.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

12. Keine zusätzlichen Risiken identifiziert

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

13. Die Kontrollkosten unterscheiden sich nicht von den früheren Kosten.

2.3. Prävention von Betrug und Unregelmäßigkeiten

14. Für die Änderungen finden weiterhin dieselben Präventivmaßnahmen Anwendung.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

Bestehende Haushaltslinien

15. In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beiträge			
	Nummer	GM/NGM [41].	von EFTA-Ländern [42]	von Kandidatenländern und potenziellen Kandidaten [43]	von anderen Drittländern	andere zweckgebundene Einnahmen
	20 02 06 Verwaltungsausgaben	NGM	NEIN	NEIN	NEIN	NEIN

Neu zu schaffende Haushaltslinien

16. In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beiträge			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern und potenziellen Kandidaten	von anderen Drittländern	andere zweckgebundene Einnahmen

[41] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[42] EFTA: Europäische Freihandelsassoziation.
[43] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

☒ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

☐ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

3.2.1.1. Mittel aus dem verabschiedeten Haushaltsplan

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	

GD <…….>			Jahr	Jahr	Jahr	Jahr	**2021-2027 INSGESAMT**
			2024	**2025**	**2026**	**2027**	
Operative Mittel							
Haushaltslinie	Verpflichtungen	(1a)					**0,000**
	Zahlungen	(2a)					**0,000**
Haushaltslinie	Verpflichtungen	(1b)					**0,000**
	Zahlungen	(2b)					**0,000**
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsmittel[44]							
Haushaltslinie		(3)					**0,000**
Mittel INSGESAMT für die GD <….>	Verpflichtungen	=1a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
	Zahlungen	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[44] Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

==========

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanz- und Digitalbogens zu Rechtsakten (Anhang 5[45] des Beschlusses der Kommission über die internen Vorschriften für die Ausführung des Einzelplans Kommission des Gesamthaushaltsplans der Europäischen Union), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

GD <…….>		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**
• Personalausgaben		0,000	0,000	0,000	0,000	**0,000**
• Sonstige Verwaltungsausgaben		0,000	0,000	0,000	0,000	**0,000**
GD <…….> INSGESAMT	Mittel	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

GD <…….>		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**
• Personalausgaben		0,000	0,000	0,000	0,000	**0,000**
• Sonstige Verwaltungsausgaben		0,000	0,000	0,000	0,000	**0,000**
GD <…….> INSGESAMT	Mittel	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

in Mio. EUR (3 Dezimalstellen)

	Jahr	Jahr	Jahr	Jahr	**2021-2027**

[45] Wenn Sie die Verwendung der Mittel unter Rubrik 7 melden, ist das Ausfüllen von Anhang 5 obligatorisch.

		2024	2025	2026	2027	INSGESAMT
Mittel INSGESAMT unter den RUBRIKEN 1 bis 7	Verpflichtungen	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
des Mehrjährigen Finanzrahmens	Zahlungen	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.1.2. Mittel aus externen zweckgebundenen Einnahmen

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	

GD <…….>			Jahr	Jahr	Jahr	Jahr	**2021-2027 INSGESAMT**
			2024	**2025**	**2026**	**2027**	
Operative Mittel							
Haushaltslinie	Verpflichtungen	(1a)					**0,000**
	Zahlungen	(2a)					**0,000**
Haushaltslinie	Verpflichtungen	(1b)					**0,000**
	Zahlungen	(2b)					**0,000**
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsmittel[46]							
Haushaltslinie		(3)					**0,000**
Mittel INSGESAMT für die GD <….>	Verpflichtungen	=1a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
	Zahlungen	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[46] Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Rubrik des Mehrjährigen Finanzrahmens	**7**	„Verwaltungsausgaben“[47]

in Mio. EUR (3 Dezimalstellen)

GD <…….>		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**
• Personalausgaben		0,000	0,000	0,000	0,000	**0,000**
• Sonstige Verwaltungsausgaben		0,000	0,000	0,000	0,000	**0,000**
GD <…….> INSGESAMT	Mittel	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

GD <…….>		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**
• Personalausgaben		0,000	0,000	0,000	0,000	**0,000**
• Sonstige Verwaltungsausgaben		0,000	0,000	0,000	0,000	**0,000**
GD <…….> INSGESAMT	Mittel	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

in Mio. EUR (3 Dezimalstellen)

	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**

[47] Der Mittelbedarf sollte auf der Grundlage der Angaben zu den Durchschnittskosten veranschlagt werden, die auf der einschlägigen BUDGpedia-Seite verfügbar sind.

Mittel INSGESAMT unter den RUBRIKEN 1 bis 7	Verpflichtungen	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
des Mehrjährigen Finanzrahmens	Zahlungen	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.2. Geschätzter Ergebnisse, die mit operativen Mitteln finanziert werden (nicht auszufüllen im Fall dezentraler Agenturen)

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Outputs angeben ⇩			Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		Bei länger andauernden Auswirkungen bitte weitere Spalten einfügen (siehe 1.6)						**INSGESAMT**	
	OUTPUTS																	
	Art[48]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[49]…																		
- Output																		
- Output																		
- Output																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 ...																		
- Output																		

[48] Outputs sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer).
[49] Wie in Kapitel 1.3.2 („Einzelziele…“) beschrieben.

Zwischensumme für Einzelziel Nr. 2																
INSGESAMT																

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

☒ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

☐ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

3.2.3.1. Mittel aus dem verabschiedeten Haushaltsplan

BEWILLIGTE MITTEL	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**2021-2027 INSGESAMT**
RUBRIK 7					
Personalausgaben	0,000	0,000	0,000	0,000	**0,000**
Sonstige Verwaltungsausgaben	0,000	0,000	0,000	0,000	**0,000**
Zwischensumme RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Außerhalb der RUBRIK 7					
Personalausgaben	0,000	0,000	0,000	0,000	**0,000**
Sonstige Verwaltungsausgaben	0,000	0,000	0,000	0,000	**0,000**
Zwischensumme außerhalb der RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
INSGESAMT	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD und/oder durch eine Umschichtung innerhalb der GD gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

3.2.4. Geschätzter Personalbedarf

☒ Für den Vorschlag/die Initiative wird kein Personal benötigt.

☐ Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

3.2.4.1. Finanziert aus dem verabschiedeten Haushalt

Schätzung in Vollzeitäquivalenten (VZÄ)[50]

17.

BEWILLIGTE MITTEL	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**
• Planstellen (Beamte und Bedienstete auf Zeit)				
20 01 02 01 (Zentrale Dienststellen und Vertretungen der Kommission)	0	0	0	0
20 01 02 03 (EU-Delegationen)	0	0	0	0
01 01 01 01 (Indirekte Forschung)	0	0	0	0
01 01 01 11 (Direkte Forschung)	0	0	0	0

[50] Bitte unter der Tabelle angeben, wie viele der aufgeführten VZÄ bereits der Verwaltung der Maßnahme zugeordnet sind und/oder durch Personalumschichtung innerhalb der GD dieser Aufgabe zugeteilt werden können. Den Nettobedarf beziffern.

Sonstige Haushaltslinien (bitte angeben)		0	0	0	0
• Externes Personal (in VZÄ)					
20 02 01 (VB und ANS der Globaldotation)		0	0	0	0
20 02 03 (VB, ÖB, ANS und JPD in den EU-Delegationen)		0	0	0	0
Haushaltslinie administr. Unterstützung [XX.01.YY.YY]	- in den zentralen Dienststellen	0	0	0	0
	- in den EU-Delegationen	0	0	0	0
01 01 01 02 (VB und ANS – indirekte Forschung)		0	0	0	0
01 01 01 12 (VB und ANS – direkte Forschung)		0	0	0	0
Sonstige Haushaltslinien (bitte angeben) – Rubrik 7		0	0	0	0
Sonstige Haushaltslinien (bitte angeben) – außerhalb der Rubrik 7		0	0	0	0
INSGESAMT		**0**	**0**	**0**	**0**

3.2.5. Einschätzung der Auswirkungen auf die Investitionen im Zusammenhang mit digitalen Technologien

18. Obligatorisch: In die Tabelle unten ist die bestmögliche Einschätzung der für den Vorschlag/die Initiative erforderlichen Investitionen in digitale Technologien einzutragen.

19. Wenn dies für die Durchführung des Vorschlags/der Initiative erforderlich ist, sollten die Mittel unter Rubrik 7 ausnahmsweise in der dafür vorgesehenen Haushaltslinie ausgewiesen werden.

20. Die unter die Rubriken 1 bis 6 fallenden Mittel sollten als „IT-Ausgaben zur Politikunterstützung für operationelle Programme“ aufgeführt werden. Diese Ausgaben beziehen sich auf die operativen Mittel, die für die Weiterverwendung/den Erwerb/die Entwicklung von IT-Plattformen/Instrumenten verwendet werden, welche in direktem Zusammenhang mit der Durchführung der Initiative und den damit verbundenen Investitionen stehen (z. B. Lizenzen, Studien, Datenspeicherung usw.). Die Angaben in dieser Tabelle sollten mit den Einzelheiten in Abschnitt 4 „Digitale Aspekte“ vereinbar sein.

Mittel INSGESAMT für Digitales und IT	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**MFF 2021 - 2027 INSGESAMT**
RUBRIK 7					
IT-Ausgaben (intern)	0,000	0,000	0,000	0,000	**0,000**
Zwischensumme RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Außerhalb der RUBRIK 7					
IT-Ausgaben zur Politikunterstützung für operationelle Programme	0,000	0,000	0,000	0,000	**0,000**
Zwischensumme außerhalb der RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
INSGESAMT	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.6. Vereinbarkeit mit dem derzeitigen Mehrjährigen Finanzrahmen

21. Der Vorschlag/Die Initiative

☒ kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

☐ erfordert eine Änderung des MFR.

3.2.7. Finanzierungsbeteiligung Dritter

22. Der Vorschlag/Die Initiative

☒ sieht keine Kofinanzierung durch Dritte vor.

☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (drei Dezimalstellen)

	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	Insgesamt
Kofinanzierende Einrichtung					
Kofinanzierung INSGESAMT					

3.3. Geschätzte Auswirkungen auf die Einnahmen

☒ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar

  – ☐ auf die Eigenmittel

  – ☐ auf die übrigen Einnahmen

  – ☐ Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind.

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[51]			
		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**
Artikel ….					

23. Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

24. […]

25. Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[51] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

26. […]

27. 4. DIGITALE ASPEKTE

4.1. Anforderungen von digitaler Relevanz

Allgemeine Beschreibung der Anforderungen von digitaler Relevanz und der damit verbundenen Kategorien (Daten, Digitalisierung und Automatisierung von Prozessen, digitale Lösungen und/oder digitale öffentliche Dienste)

Anforderung	**Beschreibung der Anforderung**	**Von der Anforderung betroffene oder sie betreffende Akteure**	**Verfahren auf übergeordneter Ebene**	**Kategorien**
Artikel 1	Änderung von Artikel 1 Absatz 1 der Datenverordnung, mit der ihr Anwendungsbereich auf die Errichtung folgender Rahmen ausgeweitet wird: • Rahmen für die Registrierung von Datenvermittlungsdiensten; • Rahmen für die freiwillige Eintragung von Einrichtungen, die zur Verfügung gestellte Daten für altruistische Zwecke sammeln und verarbeiten; • ein Rahmen für die Einsetzung eines Europäischen Dateninnovationsrats.	Europäische Kommission Datenvermittlungsdienste Datenerhebungs- und -verarbeitungseinrichtungen	Ausweitung des Anwendungsbereichs der Datenverordnung	Digitale öffentliche Dienste
Artikel 1	Änderung von Artikel 4 Absatz 8 und Artikel 5 Absatz 11 der Datenverordnung. Dateninhaber, die	Dateninhaber (Inhaber von Geschäftsgeheimnissen)	Notifizierung	Daten

	die Weitergabe von Daten gemäß der Ausnahme für Geschäftsgeheimnisse verweigern, müssen eine angemessene Mitteilung zu dieser Entscheidung bereitstellen.	Urheber von Zugriffsanfragen		
Artikel 1	Einfügung von Artikel 15a in die Datenverordnung. Pflicht zur Bereitstellung von Daten wegen eines öffentlichen Notstands.	Öffentliche Stelle Europäische Kommission Europäische Zentralbank Einrichtung der Union Dateninhaber	Bereitstellung von Daten	Daten
Artikel 1	Änderung von Artikel 21 Absatz 5 der Datenverordnung. Anforderungen im Hinblick auf die Weitergabe von im Zusammenhang mit einem öffentlichen Notstand erhaltenen Daten an Forschungseinrichtungen oder statistische Ämter. Einfügung von Artikel 22a in die Datenverordnung, mit der Beschwerden im Zusammenhang mit Kapitel V („*Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit*“) ermöglicht werden.	Öffentliche Stelle Europäische Kommission Europäische Zentralbank Einrichtung der Union Dateninhaber Zuständige nationale Behörde	Gemeinsame Nutzung von Daten Beschwerden	Daten

Artikel 1	Änderungen des Artikels 32 Absätze 1 bis 5 der Datenverordnung über den Zugang von Drittländern zu nicht-personenbezogenen Daten.	Anbieter von Datenverarbeitungsdiensten Anbieter von Datenvermittlungsdiensten Datenaltruistische Organisationen Nationale Einrichtungen oder Behörden	Staatlicher Zugang und staatliche Übermittlung im internationalen Umfeld	Daten Digitale öffentliche Dienste
Artikel 1	Änderung von Artikel 35 Absatz 5 der Datenverordnung, mit der es der Kommission ermöglicht wird, gemeinsame Spezifikationen im Hinblick auf die Interoperabilität von Datenverarbeitungsdiensten anzunehmen.	Anbieter von Datenverarbeitungsdiensten Europäische Kommission	Annahme gemeinsamer Spezifikationen	Digitale öffentliche Dienste
Artikel 1	Änderungen an Artikel 32a bis 32e der Datenverordnung zur Aufnahme von Kapitel VIIa über den Regelungsrahmen für ein europäisches Gütesiegel für Datenvermittlungsdienste, einschließlich Notifizierung, Einrichtung eines öffentlichen Registers, Bedingungen für die Erbringung von Diensten, Benennung der zuständigen Behörden und Überwachung der Einhaltung.	Anbieter von Datenvermittlungsdiensten Betroffene Personen, Dateninhaber, Datennutzer Mitgliedstaat Zuständige Behörden Europäische Kommission	Einführung des europäischen Gütesiegels für Datenvermittlungsdienste Einführung des freien Datenverkehrs in der Europäischen Union	Daten Digitale Lösung Digitalisierung der Prozesse Digitale öffentliche Dienste

	Änderungen des Artikels 32h der Datenverordnung zur Aufnahme von Kapitel VIIb über den freien Datenverkehr innerhalb der Union, einschließlich des Verbots von Datenlokalisierungsauflagen, Meldepflichten gegenüber der Kommission und der Veröffentlichung einer konsolidierten Liste.			
Artikel 1	Änderungen des Artikels 32h der Datenverordnung zur Aufnahme von Kapitel VIIb über den freien Datenverkehr innerhalb der Union, einschließlich des Verbots von Datenlokalisierungsauflagen, Meldepflichten gegenüber der Kommission und der Veröffentlichung einer konsolidierten Liste.	Mitgliedstaat Europäische Kommission	Einführung des freien Datenverkehrs in der Europäischen Union	Daten Digitalisierung der Prozesse Digitale öffentliche Dienste
Artikel 1	Einfügung von Artikel 32i in die Datenverordnung, in dem der Anwendungsbereich von Kapitel VIIc festgelegt wird. Es werden darin eine	Mitgliedstaat Dateninhaber	Festlegung des Gegenstands und des Anwendungsbereichs	Digitale öffentliche Dienste

	Reihe von Mindestvorschriften für die Weiterverwendung und die praktischen Vorkehrungen zur Erleichterung der Weiterverwendung von Daten festgelegt. Einfügung von Artikel 32j in die Datenverordnung; Bestimmung über die Nichtdiskriminierung in Verbindung mit der Weiterverwendung von Daten und Dokumenten.	Datenbenutzer	Nichtdiskriminierung	
Artikel 1	Einfügung von Artikel 32k in die Datenverordnung. Vorschriften über Ausschließlichkeitsvereinbarungen für die Weiterverwendung von Daten. Umfasst die Verpflichtung, die endgültigen Bedingungen der Vereinbarungen öffentlich zugänglich zu machen.	Potenzielle Akteure auf dem Markt Öffentliche Stellen Vertragsparteien solcher Vereinbarungen		Digitale öffentliche Dienste Daten
Artikel 1	Änderungen der Datenverordnung: • (41): Einfügung von Artikel 32n über den allgemeinen Grundsatz der Weiterverwendung offener staatlicher Daten. • (42): Einfügung von Artikel 32o über die Bearbeitung von Anträgen auf Weiterverwendung von Daten.	Dateninhaber Datenbenutzer Mitgliedstaaten (öffentliche Stellen) Europäische Kommission	Vorschriften für die Weiterverwendung von Daten	Digitale öffentliche Dienste Daten Digitalisierung der Prozesse

	• (43): Einfügung von Artikel 32p über Formate für die Weiterverwendung von Daten. • (46): Einfügung von Artikel 32s über praktische Vorkehrungen zur Erleichterung der Suche nach Daten oder Dokumenten, die zur Weiterverwendung zur Verfügung stehen.			
Artikel 1	Einfügung von Artikel 32t in die Datenverordnung; Anforderung zur Unterstützung der Verfügbarkeit von Forschungsdaten.	Mitgliedstaat Forschungseinrichtungen Datenbenutzer	Vorschriften für die Weiterverwendung von Daten	Digitale öffentliche Dienste Daten
Artikel 1	Einfügung von Artikel 32u in die Datenverordnung. Festlegung der Modalitäten für die Veröffentlichung und die Weiterverwendung bestimmter hochwertiger Datensätze.	Europäische Kommission Öffentliche Stellen, öffentliche Unternehmen	Vorschriften für die Weiterverwendung von Daten	Digitale öffentliche Dienste Daten
Artikel 1	Einfügung von Artikel 32w in die Datenverordnung. Festlegung der Bedingungen für die Weiterverwendung bestimmter Datenkategorien. Die Verfahren für die Beantragung und die Bedingungen für die Genehmigung einer solchen Weiterverwendung werden über die zentrale Informationsstelle öffentlich	Öffentliche Stellen Datenbenutzer	Vorschriften für die Weiterverwendung von Daten	Digitale öffentliche Dienste Daten

	zugänglich gemacht.			
Artikel 1	Einfügung von Artikel 32x in die Datenverordnung; Anforderungen an die Übermittlung nicht-personenbezogener Daten in Drittländer durch Weiterverwender.	Weiterverwender von Daten Öffentliche Stellen Natürliche/juristische Personen, deren Rechte beeinträchtigt werden können	Übermittlungen von Daten an Drittstaaten	Digitale öffentliche Dienste Daten
Artikel 1	Änderungen der Datenverordnung: • (55): Einfügung von Artikel 32z; organisatorische Maßnahmen im Hinblick auf die zuständigen Stellen. • (57): Einfügung von Artikel 32ab über Verfahren für Anträge auf Weiterverwendung von Daten. • (58): Ersetzung von Artikel 38 Absätze 1 und 2 über das Recht auf Beschwerde.	Zuständige Stellen Mitgliedstaat Öffentliche Stellen	Errichtung der zuständigen Stellen Antragsverfahren Beschwerden	Digitale öffentliche Dienste Daten
Artikel 1	Einfügung von Artikel 32aa in die Datenverordnung. Verpflichtung zur Nutzung einer zentralen Informationsstelle zur Erleichterung der Weiterverwendung von Daten.	Mitgliedstaat Dateninhaber Datenbenutzer Europäische Kommission.	Errichtung einer zentralen Zugangsstelle	Digitale Lösungen Digitale öffentliche Dienste Digitalisierung der Prozesse

				Daten
Artikel 1	Änderungen der Artikel 41a, 42, 45, 46, 48a, 49 und 49a der Datenverordnung zur Aufnahme von Kapitel IXa zur Errichtung des Europäischen Dateninnovationsrats (EDIB) als Expertengruppe zur Koordinierung der Durchsetzung und zur Erleichterung der Entwicklung einer europäischen Datenwirtschaft, einschließlich Anforderungen für die Zusammensetzung, Rolle, Erleichterung der Zusammenarbeit zwischen den zuständigen Behörden und Unterstützung einer einheitlichen Anwendung der rechtlichen Anforderungen.	Europäische Kommission, Europäischer Dateninnovationsrat (EDIB) Für die Datenwirtschaftspolitik zuständige Vertreter der Mitgliedstaaten Für die Durchsetzung der Kapitel II, III und V zuständige Behörden Für die Weiterverwendung von Informationen des öffentlichen Sektors zuständige Behörden (Richtlinie über offene Daten) Zuständige Behörden für Datenvermittlungsdienste Für die Registrierung von datenaltruistischen Organisationen zuständige Behörden Europäischer Datenschutzausschuss (EDSA), Europäischer	Errichtung des Europäischen Dateninnovationsrats (EDIB)	Digitale öffentliche Dienste Daten

		Datenschutzbeauftragter (EDSB) ENISA (Agentur der Europäischen Union für Cybersicherheit) KMU-Beauftragter der EU oder Vertreter des Netzes der KMU-Beauftragten Andere Vertreter maßgeblicher Einrichtungen bestimmter Sektoren Einrichtungen mit spezifischem Fachwissen Normungsorganisationen Europäisches Parlament, Rat der Europäischen Union, Europäischer Wirtschafts- und Sozialausschuss Anbieter von Datenvermittlungsdiensten Anerkannte datenaltruistische Organisationen		

Artikel 3	Änderung von Artikel 33 der Verordnung (EU) 2016/679 (DSGVO) im Hinblick auf die Meldung von Verletzungen des Schutzes personenbezogener Daten. Unter anderem wird darin die Nutzung der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle vorgeschrieben und die Verwendung von Meldevorlagen vorgesehen.	Betroffene Personen Für die Verarbeitung Verantwortliche Aufsichtsbehörden Europäischer Datenschutzausschuss Europäische Kommission	Notifizierung	Daten
Artikel 3	Änderung von Artikel 35 und Artikel 70 Absatz 1 der Verordnung (EU) 2016/679 (DSGVO). Verpflichtung des Europäischen Datenschutzausschusses zur Übermittlung von Vorschlägen zur weiteren Operationalisierung bestimmter Aspekte der Datenschutz-Folgenabschätzung an die Kommission. Dazu gehört unter anderem eine gemeinsame Vorlage für solche Abschätzungen.	Europäischer Datenschutzausschuss Europäische Kommission	Übermittlung von Vorschlägen des Ausschusses an die Kommission	Daten
Artikel 3	Einfügung von Artikel 88b in die Verordnung (EU) 2016/679 (DSGVO); die betroffenen Personen müssen in der Lage sein, mit automatisierten und maschinenlesbaren Mitteln ihre	Betroffene Personen Für die Verarbeitung Verantwortliche Europäische Normungsorganisationen	Automatisierte und maschinenlesbare Angaben zu den Wahlentscheidungen der betroffenen Person	Digitale Lösungen Prozessautomatisierung

	Einwilligung zu erteilen bzw. ihr Widerspruchsrecht auszuüben. Es ist vorgesehen, dass von einer oder mehreren europäischen Normungsorganisationen Normen ausgearbeitet werden.	Europäische Kommission		
Artikel 6	Änderung der Richtlinie (EU) 2022/2555 (NIS-2): • (1): Einfügung von Artikel 23a über den Aufbau und die Unterhaltung einer zentralen Anlaufstelle zur Meldung von Vorfällen; • (3): Änderung von Artikel 23 Absatz 4 zur Verpflichtung der Nutzung der zentralen Anlaufstelle zur Meldung schwerwiegender Vorfälle; • (4): Einfügung von Artikel 23 Absatz 12 zur Sicherstellung, dass schwerwiegende Sicherheitsvorfälle nur einmal gemeldet werden (entweder im Rahmen der NIS-2-Richtlinie oder im Rahmen der Cyberresilienzverordnung); • (5): Änderung von Artikel 30 Absatz 1 zur Sicherstellung, dass die zentrale Anlaufstelle auf freiwilliger Basis für	Notifizierende (wesentliche und wichtige Einrichtungen) CSIRTs/zuständige Behörden (falls zutreffend) Europäische Kommission ENISA,	Notifizierung	Daten Digitale Lösungen Digitale öffentliche Dienste

	Meldungen verschiedener Stellen genutzt werden kann.			
Artikel 7	Änderung der Verordnung (EU) Nr. 910/2014 (EUDI-Brieftaschen) zur Verpflichtung zur Nutzung der zentralen Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555 für folgende Meldungen: • Artikel 19a Absatz 1a: Die in Absatz 1 Buchstabe b genannten Meldungen. • Artikel 24 Absatz 2a: Die in Absatz 2 Buchstabe b genannten Meldungen. Artikel 45a Absatz 3a: Die in Absatz 3 genannten Meldungen.	Notifizierende (nichtqualifizierte Vertrauensdiensteanbieter; qualifizierter Vertrauensdiensteanbieter; Anbieter eines Webbrowsers) Aufsichtsorgane Sonstige maßgebliche zuständige Stellen/Behörden Europäische Kommission	Notifizierung	Daten

Artikel 8	Änderung der Verordnung (EU) 2022/2554 (DORA) zur Verpflichtung zur Nutzung der zentralen Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555 für folgende Meldungen: • Artikel 19 Absatz 1: Schwerwiegende IKT-bezogene Vorfälle • Artikel 19 Absatz 2: Freiwillige Meldungen erheblicher Cyberbedrohungen.	Notifizierende (Finanzunternehmen) Aufsichtsorgane Sonstige maßgebliche zuständige Stellen/Behörden Europäische Kommission ENISA,	Notifizierung	Daten
Artikel 9	Änderung der Richtlinie (EU) 2022/2557 (CER) zur Verpflichtung zur Nutzung der zentralen Anlaufstelle gemäß Artikel 23a der Richtlinie (EU) 2022/2555 für folgende Meldungen: • Artikel 15 Absatz 1: Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder erheblich stören könnten.	Notifizierende (kritische Einrichtungen) Aufsichtsorgane Sonstige maßgebliche zuständige Stellen/Behörden Europäische Kommission ENISA,	Notifizierung	Daten

4.2. Daten

Allgemeine Beschreibung der erfassten Daten

Art der Daten	**Anforderung(en)**	**Standard und/oder Spezifikation (falls zutreffend)**
Ablehnung eines Antrags auf Datenzugang auf der Grundlage der Ausnahme für Geschäftsgeheimnisse (*und entsprechende Mitteilung an die zuständige Behörde*)	Artikel 1	Auf der Grundlage objektiver Kriterien hinreichend zu begründen.
Im Zusammenhang mit einem öffentlichen Notstand bereitzustellende Daten	Artikel 1	Einschließlich der Metadaten, die für die Auslegung und Nutzung der Daten erforderlich sind. Im Fall von personenbezogenen Daten nach Möglichkeit pseudonymisiert.
Meldung der Absicht, Daten im Zusammenhang mit einem öffentlichen Notstand zur Verfügung zu stellen	Artikel 1	Angabe der Identität und der Kontaktdaten der Organisation oder Person, die die Daten erhält, des Zwecks der Übermittlung oder der Bereitstellung der Daten, des Zeitraums, in dem die Daten verwendet werden sollen, sowie der getroffenen technischen Schutzmaßnahmen und organisatorischen Maßnahmen.
Beschwerden nach Kapitel V („*Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit*“)	Artikel 1	//
In der Europäischen Union gespeicherte nicht-	Artikel 1	//

personenbezogene Daten		
Daten, die als Antwort auf einen Antrag auf Weiterverwendung von Daten bereitzustellen sind	Artikel 1	Bereitstellung der zulässigen Mindestdatenmenge
Meldung über die bevorstehende Bewilligung eines Antrags auf Weiterverwendung von Daten	Artikel 1	//
Daten, für die Vermittlungsdienste erbracht werden (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	Von der betroffenen Person/dem Inhaber erhaltenes Format, Umwandlungen ausschließlich zur Verbesserung der Interoperabilität oder zur Einhaltung internationaler/europäischer Datenstandards
Informationen über Datennutzungen und Bedingungen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	In präziser, transparenter, verständlicher und leicht zugänglicher Weise bereitzustellen.
Anträge auf Eintragung in das öffentliche Unionsregister und Änderungen gemeldeter Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	Die zuständigen Behörden erstellen die erforderlichen Antragsformulare.
Angenommene Anträge auf Eintragung in das öffentliche Unionsregister (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Meldung späterer Änderungen der während des Antragsverfahrens bereitgestellten Informationen (Europäisches Gütesiegel für	Artikel 1	//

Datenvermittlungsdienste und datenaltruistische Organisationen)		
Eingang der Meldung späterer Änderungen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Den betroffenen Personen/Inhabern vor der Verarbeitung zur Verfügung gestellte Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Einwilligung (bzw. Widerruf der Einwilligung) in die Datenverarbeitung durch eine anerkannte datenaltruistische Organisation (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	Auf elektronischem Wege zu erhalten
Informationen über das Drittland, in dem die Datennutzung stattfinden soll	Artikel 1	//
Meldung von nicht autorisierten Übermittlungen, Zugriffen oder Verwendungen nicht-personenbezogener Daten (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Informationen für die Überwachung der Einhaltung der Vorschriften (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische	Artikel 1	Anträge müssen verhältnismäßig und begründet sein.

Organisationen)		
Meldung von Nichtkonformität (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Beschluss über den Widerruf des Rechts auf Verwendung des Gütesiegels (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1	//
Entwürfe von Vorschriften über Datenlokalisierungsauflagen	Artikel 1	//
Die endgültigen Bedingungen der Ausschließlichkeitsvereinbarungen	Artikel 1	//
Daten (und/oder Meldungen) im Zusammenhang mit einem Antrag auf Weiterverwendung	Artikel 1	In allen bereits bestehenden Formaten oder Sprachen und, soweit möglich und sinnvoll, auf elektronischem Wege in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zusammen mit den zugehörigen Metadaten.
Öffentlich finanzierte Forschungsdaten	Artikel 1	Offen verfügbar, nach dem Grundsatz „standardmäßig offen“ und im Einklang mit den FAIR-Grundsätzen.
Bestimmte hochwertige Datensätze	Artikel 1	Unentgeltlich verfügbar, maschinenlesbar sein, über APIs und als Massen-Download (soweit erforderlich) bereitgestellt. Durchführungsrechtsakte

		folgen; darin können etwa Daten- und Metadatenformate behandelt werden.
Bedingungen für die Genehmigung der Weiterverwendung von Daten oder Dokumenten gemäß Artikel 2 Nummer 54	Artikel 1	Öffentlich einsehbar.
Meldung der nicht autorisierten Weiterverwendung nicht-personenbezogener Daten	Artikel 1	//
Meldung der Absicht, nicht-personenbezogene Daten in ein Drittland zu übermitteln, und des Zwecks dieser Übermittlung (*an die öffentliche Stelle*)	Artikel 1	//
Meldung der Absicht, nicht-personenbezogene Daten in ein Drittland zu übermitteln, des Zwecks dieser Übermittlung und der geeigneten Schutzvorkehrungen (*an die natürliche oder juristische Person, deren Rechte und Interessen beeinträchtigt werden könnten*)	Artikel 1	//
Alle einschlägigen Informationen über die Anwendung der Artikel 32z [Bedingungen für die Weiterverwendung], 32aa [Drittländer] und 32ab [Gebühren] der Datenverordnung.	Artikel 1	Über eine zentrale Informationsstelle verfügbar und leicht zugänglich.
Von natürlichen/juristischen Personen eingereichte Beschwerde gegen die Verletzung ihrer Rechte nach der Datenverordnung oder im Zusammenhang mit anderen relevanten Angelegenheiten	Artikel 1	//

Informationen über den Stand von Verfahren/Rechtsbehelfen im Zusammenhang mit einer nach der Datenverordnung eingereichten Beschwerde	Artikel 1	//
Daten über Erfahrungen und bewährte Verfahren (EDIB)	Artikel 1	//
Bewertung der Kapitel II, III, IV, V, VI, VII und VIII der Datenverordnung Bewertung der Kapitel VIIa, VIIb und VIIc der Datenverordnung	Artikel 1 Artikel 1	Es werden Mindestanforderungen im Hinblick auf den Inhalt der Berichte festgelegt.
Meldungen von Verletzungen des Schutzes personenbezogener Daten	Artikel 3	Über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle (und somit unter Einhaltung ihrer Spezifikationen). Der Europäische Datenschutzausschuss arbeitet einen Vorschlag für eine gemeinsame Vorlage aus (*siehe folgenden Eintrag*).
Vorschlag des EDSA für eine gemeinsame Vorlage für die Meldung von Verletzungen des Schutzes personenbezogener Daten	Artikel 3	//
Vorschläge des EDSA zur Datenschutz-Folgenabschätzung	Artikel 3	//
Berichte über erhebliche Sicherheitsvorfälle gemäß der NIS-2-Richtlinie	Artikel 6	Über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle (und somit unter Einhaltung ihrer Spezifikationen).

Meldungen von Verletzungen des Schutzes personenbezogener Daten	Artikel 3	Über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle (und somit unter Einhaltung ihrer Spezifikationen).
Meldungen schwerwiegender IKT-bezogener Vorfälle gemäß DORA; freiwillige Meldungen erheblicher Cyberbedrohungen gemäß DORA	Artikel 8	Über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle (und somit unter Einhaltung ihrer Spezifikationen).
Meldungen von Sicherheitsvorfällen, die die Erbringung wesentlicher Dienste gemäß der Richtlinie über die Resilienz kritischer Einrichtungen erheblich stören oder erheblich stören könnten	Artikel 9	Über die gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichtete zentrale Anlaufstelle (und somit unter Einhaltung ihrer Spezifikationen).

Vereinbarkeit mit der europäischen Datenstrategie

Erläuterung, inwiefern die Anforderung(en) mit der Europäischen Datenstrategie vereinbar ist/sind.

Mit diesen Änderungen der Datenverordnung wird der EDIB (Kapitel IXa) eingeführt, der die Anwendung der Vorschriften koordiniert und Leitlinien für sektorspezifische gemeinsame europäische Datenräume ausarbeitet; ebenso wird das europäischen Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen (Kapitel VIIa) eingeführt, mit dem ein vertrauenswürdiges Ökosystem für den Datenaustausch und den Schutz von Rechten geschaffen wird; mit Kapitel VIIb wird der freie Verkehr nicht-personenbezogener Daten umgesetzt, indem ungerechtfertigte Datenlokalisierungsauflagen verboten werden; mit Kapitel VIIc werden die Vorschriften über die Weiterverwendung von Daten des öffentlichen Sektors gestrafft, indem die Bestimmungen der Richtlinie über offene Daten und des Daten-Governance-Rechtsakts zusammengeführt werden; mit den Vorschriften über internationale Datenübermittlungen wird die digitale Souveränität Europas gestärkt, indem Daten vor nicht autorisiertem Zugriff durch Drittländer geschützt werden; schließlich wird mit den Ausnahmen für KMU und der Präsenz des KMU-Beauftragten der EU im EDIB sichergestellt, dass die Datenwirtschaft auch für kleine Unternehmen besser zugänglich ist.

Vereinbarkeit mit dem Grundsatz der einmaligen Erfassung

Erläuterung, inwiefern der Grundsatz der einmaligen Erfassung berücksichtigt und inwiefern die Möglichkeit der Weiterverwendung vorhandener Daten geprüft wurde

Mit diesen Änderungen wird der Einmaligkeitsgrundsatz unterstützt, indem eine Infrastruktur für eine effiziente Weiterverwendung von Daten geschaffen wird: Der EDIB entwickelt Interoperabilitätsstandards für die gemeinsamen europäischen Datenräume, um doppelte Datenbereitstellung zu verringern; Datenvermittlungsdienste fungieren als vertrauenswürdige Vermittler, die einen sicheren Austausch vorhandener Daten ermöglichen, sodass redundante Datenerhebungen vermieden werden; datenaltruistische Organisationen erleichtern zum Nutzen der Allgemeinheit den freiwilligen Datenaustausch, indem sie Daten für Forschungszwecke und öffentliche Dienste weiterverwendbar machen; mit Bestimmungen über den freien Fluss werden Barrieren verhindert, die eine doppelte Speicherung an verschiedenen Orten erfordern; und Schutzvorkehrungen für die internationale Übermittlung sorgen für die grenzüberschreitende Zugänglichkeit von Daten bei gleichzeitiger Aufrechterhaltung des Schutzes und ermöglichen es, dass sowohl Einzelpersonen als auch Unternehmen ihre Daten einmal zur Verfügung stellen können und im Anschluss der Bedarf durch sichere, die Rechte wahrende Austauschmechanismen erfüllt wird. In der Zwischenzeit ermöglichen die Bestimmungen über die zentrale Anlaufstelle den Einmaligkeitsgrundsatz in Bezug auf die Meldung von Vorfällen.

Erläuterung, inwiefern neu geschaffene Daten auffindbar, zugänglich, interoperabel und wiederverwendbar sind und hohen Standards entsprechen

Mit diesen Änderungen wird durch koordinierte Mechanismen sichergestellt, dass neu geschaffene Daten den FAIR-Grundsätzen und Qualitätsstandards entsprechen: Der EDIB entwickelt für alle sektorspezifischen Datenräume gemeinsame technische Spezifikationen und zugängliche Interoperabilitätsprotokolle; durch Bestimmungen über den freien Fluss wird eine Fragmentierung, durch die die Datenqualität beeinträchtigt wird, verhindert; durch die Koordinierungsfunktion des EDIB kann in allen Mitgliedstaaten eine harmonisierte Umsetzung von Metadatenstandards, technischen Anforderungen und Qualitätsbenchmarks ermöglicht werden.

Datenströme

Allgemeine Beschreibung der Datenströme

Hinweis: Bei den meisten der nachstehend aufgeführten Datenströme handelt es sich um bereits vorhandene Datenströme, deren Rechtsgrundlage von einer Verordnung in eine andere übertragen wird. Insbesondere werden Bestimmungen aus dem Daten-Governance-Rechtsakt in die Datenverordnung übertragen.

Art der Daten	**Anforderung(en)**	**Akteure, die die Daten bereitstellen**	**Akteure, die die Daten empfangen**	**Auslöser für den Datenaustausch**	**Häufigkeit (falls zutreffend)**

Ablehnung eines Antrags auf Datenzugang auf der Grundlage der Ausnahme für Geschäftsgeheimnisse (*und entsprechende Mitteilung an die zuständige Behörde*)	Artikel 1 *Änderung von Artikel 4 Absatz 8 und Artikel 5 Absatz 11 der Datenverordnung*	Dateninhaber	Datennutzer (der die Anfrage stellt); die gemäß Artikel 37 bestimmte zuständige Behörde	Ablehnung eines Antrags auf Datenzugriff auf der Grundlage der Ausnahme für Geschäftsgeheimnisse	Ad-hoc-Maßnahme
Im Zusammenhang mit einem öffentlichen Notstand bereitzustellende Daten	Artikel 1 *Einfügung von Artikel 15a in die Datenverordnung*	Dateninhaber	Öffentliche Stelle; Europäische Kommission; Europäische Zentralbank; Einrichtung der Union	Öffentlicher Notstand + Antrag auf Datenzugriff, die die erforderlichen Voraussetzungen erfüllen	Ad-hoc-Maßnahme
Meldung der Absicht, Daten im Zusammenhang mit einem öffentlichen Notstand zur Verfügung zu stellen	Artikel 1 *Änderung von Artikel 21 Absatz 5 der Datenverordnung*	Öffentliche Stelle; Europäische Kommission; Europäische Zentralbank; Einrichtung der Union	Dateninhaber, von dem die Daten empfangen wurden	Öffentlicher Notstand + Absicht, Daten zu übermitteln oder zur Verfügung zu stellen	Ad-hoc-Maßnahme
Beschwerden nach Kapitel V („Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union	Artikel 1 *Einfügung von Artikel 22a in die Datenverordnung*	Dateninhaber; Öffentliche Stelle; Europäische Kommission; Europäische Zentralbank; Einrichtung der Union	Zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist	Bei Streitigkeiten über ein Datenverlangen nach Artikel 15a der Datenverordnung	Ad-hoc-Maßnahme

wegen außergewöhnlicher Notwendigkeit“)					
In der Europäischen Union gespeicherte nicht-personenbezogene Daten	Artikel 1 *Änderung der folgenden Artikel der Datenverordnung:* *Artikel 32 Absatz 1, Artikel 32 Absatz 3, Artikel 32 Absatz 4*	Anbieter von Datenverarbeitungsdiensten, Anbieter von Datenvermittlungsdiensten, datenaltruistische Organisationen	Gerichte/Gerichtshöfe in Drittländern, Verwaltungsbehörden, Kunden (Dateninhaber/betroffene Personen) in Drittändern	Antrag eines Drittlands auf der Grundlage einer internationalen Übereinkunft, Antrag eines Drittlands, das die Bedingungen des Artikels 32 Absatz 3 erfüllt, Antrag des Kunden auf Zugang zu seinen eigenen Daten	Ad-hoc-Maßnahme
Daten, die als Antwort auf einen Antrag auf Weiterverwendung von Daten bereitzustellen sind	Artikel 1 *Änderung von Artikel 32 Absätze 4 und 5 der Datenverordnung*	Anbieter von Datenvermittlungsdiensten oder anerkannte datenaltruistische Organisation	Urheber des Antrags auf Weiterverwendung von Daten (Behörde des Drittlands)	Datum der Bewilligung des Antrags auf Weiterverwendung	Ad-hoc-Maßnahme
Meldung über die bevorstehende Bewilligung eines Antrags auf Weiterverwendung von Daten	Artikel 1 *Änderung von Artikel 32 Absätze 4 und 5 der Datenverordn*	Anbieter von Datenvermittlungsdiensten oder anerkannte datenaltruistische Organisation	Ist der Kunde, der Lieferant oder keiner von beiden berechtigt, während des gesamten Verwendungszeitrau	Datum der Bewilligung des Antrags auf Weiterverwendung der Drittlandsbehörde stattgegeben wurde (*es sei denn, der Antrag dient*	Ad-hoc-Maßnahme

	ung		ms zu bestimmen, wie und für welchen Zweck der Vermögenswert eingesetzt wird?	*Strafverfolgungszwecken*)	
In öffentlichen Registern zu veröffentlichende Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32a in die Datenverordnung*	Europäische Kommission	Öffentlich	Informationen über anerkannte Datenvermittlungsdienste oder datenaltruistische Organisationen werden verfügbar oder müssen geändert werden	Laufend (regelmäßige Aktualisierung des Registers)
Daten, für die Vermittlungsdienste erbracht werden (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32c in die Datenverordnung*	Betroffene Personen Dateninhaber	Datennutzer (über Anbieter von Datenvermittlungsdiensten)	Einwilligung der betroffenen Person Erlaubnis des Dateninhabers Antrag des Datennutzers	Gemäß Vereinbarung/Vertrag zwischen den Parteien
Informationen über Datennutzungen und Bedingungen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32c in die Datenverordnung*	Anbieter von Datenvermittlungsdiensten	Betroffene Personen	Bevor die betroffene Person ihre Einwilligung zur Datennutzung erteilt	Jedes Mal, bevor um Einwilligung ersucht wird

Anträge auf Eintragung in das öffentliche Unionsregister und Änderungen gemeldeter Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32e in die Datenverordnung*	Anbieter von Datenvermittlungsdiensten Datenaltruistische Organisationen	Zuständige Behörde im Mitgliedstaat der Hauptniederlassung	Geltungsdauer	Ad-hoc-Maßnahme
Angenommene Anträge auf Eintragung in das öffentliche Unionsregister (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32e in die Datenverordnung*	Zuständige Behörde	Europäische Kommission	Antrag genehmigt	Ad hoc (innerhalb von 12 Wochen nach Eingang des Antrags, sofern die Entscheidung positiv ausfällt)
Meldung späterer Änderungen der während des Antragsverfahrens bereitgestellten Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32e in die Datenverordnung*	Registrierte Einrichtungen	Zuständige Behörde	Änderungen der bereitgestellten Informationen oder Einstellung der Tätigkeit von Einrichtungen in der Union	Ad-hoc-Maßnahme

Eingang der Meldung späterer Änderungen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32e in die Datenverordnung*	Zuständige Behörde	Europäische Kommission	Registrierte Organisationen melden Änderungen (siehe Eintrag oben)	Ad hoc, unverzüglich
Den betroffenen Personen/Inhabern vor der Verarbeitung zur Verfügung gestellte Informationen (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32f in die Datenverordnung*	Anerkannte datenaltruistischer Organisationen	Betroffene Personen Dateninhaber	Vor jeder Verarbeitung ihrer Daten	Vor jeder Verarbeitungstätigkeit (muss klar und leicht verständlich sein)
Einwilligung (bzw. Widerruf der Einwilligung) in die Datenverarbeitung durch eine anerkannte datenaltruistische Organisation (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32f in die Datenverordnung*	Betroffene Personen Dateninhaber (bei nicht-personenbezogenen Daten)	Datenaltruistische Organisation	Einwilligung der betroffenen Person/Erlaubnis des Dateninhabers für Verarbeitungstätigkeiten erforderlich	Gemäß erteilter Einwilligung/Erlaubnis, mit der Möglichkeit des jederzeitigen Widerrufs
Informationen über das Drittland, in dem die	Artikel 1	Datenaltruistische	Dateninhaber	Wenn datenaltruistische Organisationen die	Ad-hoc-

Datennutzung stattfinden soll	*Einfügung von Artikel 32f in die Datenverordnung*	Organisation		Datenverarbeitung durch Dritte erleichtern	Maßnahme
Meldung von nicht autorisierten Übermittlungen, Zugriffen oder Verwendungen nicht-personenbezogener Daten (europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32f in die Datenverordnung*	Datenaltruistische Organisation	Dateninhaber	Nicht autorisierter Vorgang	Ad hoc, unverzüglich
Informationen für die Überwachung der Einhaltung der Vorschriften (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32g in die Datenverordnung*	Anbieter von Datenvermittlungsdiensten Datenaltruistische Organisationen	Zuständige Behörden	Antrag der zuständigen Behörde Antrag einer natürlichen oder juristischen Person	Ad hoc (auf Antrag, der verhältnismäßig und begründet sein muss)
Meldung von Nichtkonformität (Europäisches Gütesiegel für	Artikel 1 *Einfügung von Artikel 32g in die*	Zuständige Behörde	Einrichtung, bei der die Nichtkonformität festgestellt wird	Die zuständige Behörde stellt fest, dass ein anerkannter Anbieter von Datenvermittlungsdiensten	Ad hoc (anschließend hat die Einrichtung Gelegenheit,

Datenvermittlungsdienste und datenaltruistische Organisationen)	*Datenverordnung*			oder eine anerkannte datenaltruistische Organisation nicht konform ist.	innerhalb von 30 Tagen Stellung zu nehmen)
Beschluss über den Widerruf des Rechts auf Verwendung des Gütesiegels (Europäisches Gütesiegel für Datenvermittlungsdienste und datenaltruistische Organisationen)	Artikel 1 *Einfügung von Artikel 32g in die Datenverordnung*	Zuständige Behörde	Öffentlich	Nach der Entscheidung über den Widerruf des Gütesiegels	Ad-hoc-Maßnahme
Entwürfe von Vorschriften über Datenlokalisierungsauflagen	Artikel 1	Mitgliedstaat	Europäische Kommission	Erstellung eines Entwurfs eines Rechtsakts, mit dem eine neue Datenlokalisierungsauflage eingeführt oder eine bestehende Datenlokalisierungsauflage geändert wird	Ad hoc, unverzüglich
Die endgültigen Bedingungen der Ausschließlichkeitsvereinbarungen	Artikel 1	Parteien der Regelung	Öffentlich	Am oder nach dem 16. Juli 2019 geschlossene Ausschließlichkeitsvereinbarungen	Ad hoc, mindestens zwei Monate vor Inkrafttreten einer Vereinbarung
Daten (und/oder Meldungen) im	Artikel 1	Öffentliche Stellen	Urheber von Anträgen	Im Fall von Dokumenten ist	Ad-hoc-

Zusammenhang mit einem Antrag auf Weiterverwendung	*Einfügung von Artikel 32p in die Datenverordnung*		auf Weiterverwendung von Daten	Folgendes bereitzustellen: angeforderte Daten/Dokumente; Lizenzangebot; Mitteilungen über Verzögerungen; Mitteilung über eine ablehnende Entscheidung.	Maßnahme
Die endgültigen Bedingungen der Ausschließlichkeitsvereinbarungen	Artikel 1 *Einfügung von Artikel 32k in die Datenverordnung*	Parteien einer Ausschließlichkeitsvereinbarung	breite Öffentlichkeit	Endgültige Bedingungen für das Zustandekommen einer Ausschließlichkeitsvereinbarung	Ad-hoc-Maßnahme
Bedingungen für die Genehmigung der Weiterverwendung von Daten oder Dokumenten gemäß Artikel 2 Nummer 54	Artikel 1 *Einfügung von Artikel 32z in die Datenverordnung*	Öffentliche Stellen (zuständig für die Bewilligung oder Ablehnung von Anträgen auf Zugang)	breite Öffentlichkeit	Wenn sie der Weiterverwendung von Daten oder Dokumenten stattgeben	Ad-hoc-Maßnahme
Meldung der nicht autorisierten Weiterverwendung nicht-personenbezogener Daten	Artikel 1 *Einfügung von Artikel 32z in die Datenverordnung*	Weiterverwender (möglicherweise mit Unterstützung der öffentlichen Stelle)	Natürliche/juristische Personen, deren Rechte und Interessen beeinträchtigt werden können	Nicht autorisierte Weiterverwendung erfolgt	Ad-hoc-Maßnahme

Meldung der Absicht, nicht-personenbezogene Daten in ein Drittland zu übermitteln, und des Zwecks dieser Übermittlung (an die öffentliche Stelle)	Artikel 1 *Einfügung von Artikel 32aa in die Datenverordnung*	Weiterverwender	Öffentliche Stelle	Absicht, Daten in ein Drittland zu übermitteln	Ad-hoc-Maßnahme
Meldung der Absicht, nicht-personenbezogene Daten in ein Drittland zu übermitteln, des Zwecks dieser Übermittlung und der geeigneten Schutzvorkehrungen (an die natürliche oder juristische Person, deren Rechte und Interessen beeinträchtigt werden könnten)	Artikel 1 *Einfügung von Artikel 32aa in die Datenverordnung*	Weiterverwender (möglicherweise mit Unterstützung der öffentlichen Stelle)	Natürliche oder juristische Person, deren Rechte und Interessen beeinträchtigt werden können	Absicht, Daten in ein Drittland zu übermitteln	Ad-hoc-Maßnahme
Alle einschlägigen Informationen über die Anwendung der Artikel 32z [Bedingungen für die Weiterverwendung], 32aa [Drittländer] und 32ab [Gebühren] der Datenverordnung.	Artikel 1 *Einfügung von Artikel 32ad in die Datenverordnung*	Mitgliedstaat	Steht den Nutzern der zentralen Informationsstelle zur Verfügung.	Es müssen einschlägige Informationen bereitgestellt werden.	Ad-hoc-Maßnahme
Von natürlichen/juristischen Personen eingereichte Beschwerde gegen die	Artikel 1 *Änderung von Artikel 38*	Natürliche oder juristische Personen	Jeweils zuständige Behörde im betreffenden	Zu erhebende Beschwerde	Ad-hoc-Maßnahme

Verletzung ihrer Rechte nach der Datenverordnung oder im Zusammenhang mit anderen relevanten Angelegenheiten	*Absätze 1 und 2 der Datenverordnung*		Mitgliedstaat		
Informationen über den Stand von Verfahren/Rechtsbehelfen im Zusammenhang mit einer nach der Datenverordnung eingereichten Beschwerde	Artikel 1 *Änderung von Artikel 38 Absätze 1 und 2 der Datenverordnung*	Jeweils zuständige Behörde	Natürliche oder juristische Personen, die die Beschwerde eingereicht haben	Eingereichte Beschwerde	Ad-hoc-Maßnahme
Daten über Erfahrungen und bewährte Verfahren (EDIB)	Artikel 1 *Einfügung von Kapitel IXa in die Datenverordnung*	Europäischer Dateninnovationsrat	Kommission; Zuständige Behörden	Beiträge erforderlich	Ad-hoc-Maßnahme
Bewertung der Kapitel II, III, IV, V, VI, VII und VIII der Datenverordnung Bewertung der Kapitel VIIa, VIIb und VIIc der Datenverordnung	Artikel 1 *Änderung von Artikel 49 Absatz 1 der Datenverordnung* Artikel 1 *Änderung von Artikel 49*	Europäische Kommission	Europäisches Parlament, Rat; Europäischer Wirtschafts- und Sozialausschuss	Bewertung der Datenverordnung durchgeführt	bis 12. September 2028 Bis zum [Inkrafttreten plus 5 Jahre]

	Absatz 2 der Datenverordnung				
Meldungen von Verletzungen des Schutzes personenbezogener Daten	Artikel 3 *Änderung von Artikel 33 Absatz 1 der DSGVO*	Für die Verarbeitung Verantwortlicher	Aufsichtsbehörde	Datenschutzverletzung erfolgt	Ad-hoc-Maßnahme
Vorschlag des EDSA für eine gemeinsame Vorlage für die Meldung von Verletzungen des Schutzes personenbezogener Daten	Artikel 3 *Änderung von Artikel 33 Absatz 1 der DSGVO*	Europäischer Datenschutzausschuss	Kommission	Vorschlag ist einzureichen	Innerhalb von [Monaten] nach dem Inkrafttreten dieser Verordnung dreijährlich
Vorschläge des EDSA zur Datenschutz-Folgenabschätzung	Artikel 3 *Änderung von Artikel 70 Absatz 1 der DSGVO*	Europäischer Datenschutzausschuss	Kommission	Vorschlag ist einzureichen	Ad-hoc-Maßnahme
Berichte über erhebliche Sicherheitsvorfälle gemäß der NIS-2-Richtlinie	Artikel 6 *Einfügung der Artikel 23a und 23b zur Änderung der Artikel 23 und Artikel 30 Absatz 1 der*	Wesentliche und wichtige Einrichtungen	CSIRTs/zuständige Behörden (falls zutreffend)	In Artikel 23 Absatz 3 der NIS-2-Richtlinie beschriebene Umstände	Ad-hoc-Maßnahme

	NIS-2-Richtlinie				
Meldungen von Verletzungen des Schutzes personenbezogener Daten	Artikel 3 *Änderung von Artikel 33 der DSGVO*	Für die Verarbeitung Verantwortlicher	Aufsichtsbehörde	Verletzung des Schutzes personenbezogener Daten	Ad-hoc-Maßnahme
Meldungen schwerwiegender IKT-bezogener Vorfälle gemäß DORA; freiwillige Meldungen erheblicher Cyberbedrohungen gemäß DORA	Artikel 8 *Änderung von Artikel 19 der DORA*	Finanzunternehmen	Jeweils zuständige Behörde	Schwerwiegende IKT-bezogene Vorfälle; Erhebliche Cyberbedrohungen	Ad-hoc-Maßnahme
Meldungen von Sicherheitsvorfällen, die die Erbringung wesentlicher Dienste gemäß der Richtlinie über die Resilienz kritischer Einrichtungen erheblich stören oder erheblich stören könnten	Artikel 9 *Änderung von Artikel 15 der Richtlinie über die Resilienz kritischer Einrichtungen*	Kritische Einrichtungen	Zuständige Behörde	Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder erheblich könnten	Ad-hoc-Maßnahme

4.3. Digitale Lösungen

Allgemeine Beschreibung der digitalen Lösungen

Hinweis: Bei allen nachstehend aufgeführten digitalen Lösungen handelt es sich um bereits vorhandene Lösungen, deren Rechtsgrundlage von einer Verordnung in eine andere übertragen wird. Insbesondere werden Bestimmungen aus dem Daten-Governance-Rechtsakt in die Datenverordnung überführt.

Digitale Lösung	**Anforderung(en)**	**Wichtigste vorgeschriebene Funktionen**	**Zuständige Stelle**	**Inwiefern wird Zugänglichkeit gewährleistet?**	**Wie wird die Wiederverwendbarkeit berücksichtigt?**	**Einsatz von KI-Technologien (falls zutreffend)**
Öffentliches Unionsregister der Datenvermittlungsdienste und datenaltruistischen Organisationen	*Einfügung von Artikel 32a in die Datenverordnung*	Speicherung und Veröffentlichung der vorgeschriebenen Informationen	Europäische Kommission	//	//	entfällt
Zentrale Informationsstelle (gemäß der Datenverordnung)	Artikel 1 *Einfügung von Artikel 32ad in die Datenverordnung*	Bereitzustellende und zugänglich zu machende Informationen Für die Entgegennahme von Anfragen oder Anträgen in Verbindung mit der Weiterverwendung von Kategorien geschützter Daten zuständig	Europäische Kommission	Zentrales Zugangsportal, über das ein durchsuchbares elektronisches Verzeichnis der bei den zentralen nationalen Informationsstellen verfügbaren Daten sowie weitere Informationen darüber bereitgestellt werden, wie über die zentralen	Elektronische Verfügbarkeit einer durchsuchbaren Liste der Vermögenswerte mit einem Überblick über alle verfügbaren Datenressourcen […] und die Bedingungen für ihre Weiterverwendung.	entfällt

		Übermittlung von Anträgen an die zuständigen öffentlichen Stellen, soweit möglich und angemessen auf automatisiertem Wege Elektronische Bereitstellung einer durchsuchbaren Liste der Vermögenswerte mit einem Überblick über alle verfügbaren Dokumentenressourcen		nationalen Informationsstellen Daten angefordert werden können.		
Zentrale Anlaufstelle zur Meldung von Vorfällen	Artikel 6 *Einfügung von Artikel 23a in die NIS-2-Richtlinie*	Ermöglichung der Meldung von Sicherheitsvorfällen gemäß den einschlägigen Rechtsakten auf Unionsebene Sicherstellung der Interoperabilität und Kompatibilität mit europäischen Unternehmensbrieftaschen	Europäische Kommission; ENISA,	Interoperabilität und Kompatibilität mit europäischen Unternehmensbrieftaschen und ihren eigenen Mitteln für die Barrierefreiheit	Möglichkeit zur Meldung von Vorfällen im Rahmen verschiedener Rechtsakte; Möglichkeit zur künftigen Aufnahme weiterer Rechtsgrundlagen in die Lösung für eine zentrale Anlaufstelle	entfällt

Für jede digitale Lösung Erläuterung, inwiefern diese mit geltenden digitalen Strategien und Rechtsvorschriften im Einklang steht.

Öffentliches Unionsregister der Datenvermittlungsdienste und datenaltruistischen Organisationen

Digitale und/oder sektorspezifische Strategie (falls anwendbar)	**Erläuterung der Vereinbarkeit**
KI-Verordnung	entfällt
EU-Rahmen für Cybersicherheit	entfällt
eIDAS-Verordnung	entfällt
Einheitliches digitales Zugangstor und IMI	Änderung der Verordnung (EU) 2018/1724 zur Einfügung von „Eintragung als Anbieter von Datenvermittlungsdiensten“ und „Eintragung als in der Union anerkannte datenaltruistische Organisation“ in Anhang II.
Sonstige	entfällt

Zentrale Informationsstelle (gemäß der Datenverordnung)

Digitale und/oder sektorspezifische Strategie (falls anwendbar)	**Erläuterung der Vereinbarkeit**
KI-Verordnung	entfällt
EU-Rahmen für Cybersicherheit	Öffentliche Stellen können vorschreiben, dass der Zugang zu den Daten oder Dokumenten und deren Weiterverwendung durch Fernzugriff in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten sicheren Verarbeitungsumgebung erfolgt. In diesen Fällen erlegen die öffentlichen Stellen Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der

	verwendeten sicheren Verarbeitungsumgebung gewahrt wird.
eIDAS-Verordnung	entfällt
Einheitliches digitales Zugangstor und IMI	entfällt
Sonstige	Die zentrale Informationsstelle muss der Verordnung (EU) 2016/679 (DSGVO) entsprechen. Öffentliche Stellen dürfen nur dann Anforderungen für die Gewährung des Zugangs zwecks Weiterverwendung von Daten oder Dokumenten vorsehen, wenn diese anonymisiert wurden und/oder einer anderen Form zweckdienlicher Vorbereitung unterzogen wurden. Darüber hinaus ist der Weiterverwender im Falle der nicht autorisierten Weiterverwendung nicht-personenbezogener Daten verpflichtet, die natürlichen Personen, deren Rechte und Interessen beeinträchtigt werden könnten, zu unterrichten.

Zentrale Anlaufstelle zur Meldung von Vorfällen

Digitale und/oder sektorspezifische Strategie (falls anwendbar)	**Erläuterung der Vereinbarkeit**
KI-Verordnung	entfällt
EU-Rahmen für Cybersicherheit	Eine Änderung der NIS-2-Richtlinie besteht darin, dass ein inhärenter Schwerpunkt auf der Cybersicherheit liegt. Im weiteren Sinne soll die zentrale Anlaufstelle als Zugangstor dienen, über das alle Meldungen von Cybersicherheitsvorfällen im Rahmen mehrerer Rechtsakte der Union an die jeweils zuständigen Behörden weitergeleitet werden.
eIDAS-Verordnung	Die zentrale Anlaufstelle ist ebenfalls mit der Meldung von Vorfällen gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) betraut. Die ENISA sorgt dafür, dass die zentrale Anlaufstelle mit den europäischen

	Unternehmensbrieftaschen interoperabel und kompatibel ist und dass die europäischen Unternehmensbrieftaschen zumindest verwendet werden können, um Einrichtungen über die zentrale Anlaufstelle zu identifizieren und zu authentifizieren. Die politische Initiative für die europäische Unternehmensbrieftaschen wird auf dem eIDAS-Rahmen aufbauen.
Einheitliches digitales Zugangstor und IMI	entfällt
Sonstige	Für den Vorschlag wurde der gesamte digitale Besitzstand berücksichtigt, einschließlich der Strategien in den Bereichen Daten, Cybersicherheit und Telekommunikation.

4.4. Interoperabilitätsbewertung

Allgemeine Beschreibung der von den Anforderungen betroffenen digitalen öffentlichen Dienste

Digitaler öffentlicher Dienst oder Kategorie digitaler öffentlicher Dienste	**Beschreibung**	**Anforderung(en)**	**Lösung(en) für ein interoperables Europa** **(NICHT ZUTREFFEND)**	**Andere Interoperabilitätslösung(en)**
Europäische Infrastruktur für Daten-Governance und Transparenz	Digitaler öffentlicher Dienst, der eine Infrastruktur für Daten-Governance und Transparenz ermöglicht und unter anderem ein öffentliches EU-Register von Datenvermittlungsdiensten und datenaltruistischen Organisationen sowie eine zentrale Informationsstelle nutzt, die Weiterverwendern dabei hilft, Informationen über die Weiterverwendung bestimmter Kategorien geschützter Daten zu finden. Kategorie digitaler öffentlicher Dienste gemäß COFOG 04.9.0 – Wirtschaft, a. n. g. (KS)	Artikel 1	//	//
Berichterstattung über Vorfälle	Digitaler öffentlicher Dienst, der die Meldung von Vorfällen über die zentrale Anlaufstelle	Artikel 6	//	Europäische Unternehmensbrieftaschen

	ermöglicht. Kategorie digitaler öffentlicher Dienste gemäß COFOG 03.6.0 Öffentliche Ordnung und Sicherheit, a. n. g. (CS).			

Auswirkungen der Anforderung(en) auf die grenzüberschreitende Interoperabilität nach digitalem öffentlichen Dienst

Hinweis: In der folgenden Analyse beziehen sich die im Abschnitt „Maßnahme(n)“ angegebenen Artikelnummern auf den/die zu ändernden Rechtsakt(e). Die Zuordnung zu den Anforderungen der Omnibus-Verordnung erfolgt einmal oben in jeder Zelle.

Digitaler öffentlicher Dienst Nr. 1 – Europäische Infrastruktur für Daten-Governance und Transparenz

Bewertung	**Maßnahme(n)**	**Mögliche verbleibende Hindernisse (falls zutreffend)**
Vereinbarkeit mit bestehenden digitalen und sektorspezifischen Strategien **Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.**	Artikel 1 Die Anpassung an bestehende digitale und sektorspezifische Strategien schlägt sich in den Erwägungsgründen des Daten-Governance-Rechtsakts nieder: Einheitliches digitales Zugangstor (Verordnung (EU) 2018/1724) (Erwägungsgrund 56): Die Notifizierungsverfahren für Datenvermittlungsdienste und die Eintragungsverfahren für datenaltruistische Organisationen müssen über das einheitliche digitale Zugangstor zugänglich gemacht werden, um einen grenzüberschreitenden Online-Zugang sicherzustellen. Europäischer Interoperabilitätsrahmen (Erwägungsgrund 54): Die digitale Infrastruktur muss den Grundsätzen des Europäischen Interoperabilitätsrahmens entsprechen, um eine grenzüberschreitende und sektorübergreifende Datennutzung sicherzustellen. CEF-Bausteine (Fazilität „Connecting Europe“ – Infrastrukturen für digitale Dienste) (Erwägungsgrund 54): Bezugnahmen auf „die Kernvokabulare und die CEF-Bausteine“.	

	Der digitale Dienst sollte für die technische Umsetzung die CEF-Bausteine (wie eDelivery, eID, eSignature) nutzen. Barrierefreiheitsanforderungen (Richtlinien (EU) 2016/2102 und (EU) 2019/882) (Erwägungsgrund 62). Richtlinie (EU) 2016/2102 (Richtlinie über den barrierefreien Zugang zu Websites): Öffentliche Register und digitale Dienste müssen für Menschen mit Behinderungen zugänglich sein; Richtlinie (EU) 2019/882 (europäischer Rechtsakt zur Barrierefreiheit): Digitale Dienste müssen den Barrierefreiheitsanforderungen entsprechen. DSGVO (Verordnung (EU) 2016/679) (Erwägungsgründe 4 und 35). Alle digitalen Dienste, mit denen personenbezogene Daten verarbeitet werden, müssen den Anforderungen der DSGVO im Hinblick auf Datenschutz, Privatsphäre und Sicherheit entsprechen. Verordnung (EU) 2018/1725 (Erwägungsgrund 4): Verarbeiten Unionsorgane Daten über diese Register, müssen sie diese Verordnung einhalten. Richtlinie über offene Daten (Richtlinie (EU) 2019/1024) (Erwägungsgründe 6 und 10): „Die Richtlinie (EU) 2019/1024 und sektorspezifisches Unionsrecht zielen darauf ab, dass öffentliche Stellen die Zugänglichkeit der von ihnen erzeugten Daten für die Verwendung und Weiterverwendung in größerem Umfang erleichtern“: Der digitale Dienst ergänzt die Richtlinie über offene Daten, indem er den Kategorien geschützter Daten Rechnung trägt, die nicht in ihren Anwendungsbereich fallen, und gleichzeitig sicherstellt, dass öffentliche Stellen gegebenenfalls den Grundsatz „konzeptionell und standardmäßig offen“ befolgen. Sektorspezifische Strategien für europäische Datenräume und sektorspezifische Daten, darunter der europäische Raum für Gesundheitsdaten, der europäische Mobilitätsdatenraum, Daten zum europäischen Grünen Deal/Klima- und Energiedaten, Fertigungs- und Industriedaten, Finanzdienstleistungsdaten, Agrardaten, der Datenraum für die öffentliche Verwaltung und der Kompetenzdatenraum.	

Organisatorische Maßnahmen für eine reibungslose grenzüberschreitende Erbringung digitaler öffentlicher Dienste **Bitte führen Sie die geplanten Governance-Maßnahmen auf.**	Artikel 1 **Benennung und Koordinierung der zuständigen Behörde** - Artikel 32b: Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für die Eintragung von Anbietern von Datenvermittlungsdiensten und datenaltruistischen Organisationen zuständig sind. Diese zuständigen Behörden wahren gegenüber anerkannten Anbietern von Datenvermittlungsdiensten oder anerkannten datenaltruistischen Organisationen ihre Unabhängigkeit. Artikel 32ac: Jeder Mitgliedstaat benennt eine oder mehrere zuständige Stellen, die öffentliche Stellen unterstützen, die den Zugang zwecks Weiterverwendung von Kategorien geschützter Daten gewähren oder verweigern. Artikel 32g: Die zuständigen Behörden überwachen und beaufsichtigen die Konformität anerkannter Anbieter von Datenvermittlungsdiensten und anerkannter datenaltruistischer Organisationen mit der Datenverordnung. **Mechanismus der grenzüberschreitenden gerichtlichen Zuständigkeit** Artikel 32e: Datenvermittlungsdienste fallen in den Bereich der zuständigen Behörde im Mitgliedstaat der Hauptniederlassung. Für datenaltruistische Organisationen gilt derselbe Grundsatz. **Gegenseitige Anerkennung und einmalige Eintragung** Artikel 32e: Die Eintragung als Datenvermittlungsdienst/datenaltruistische Organisation ist in allen Mitgliedstaaten gültig. Artikel 32a: Verwendung eines gemeinsamen Logos **Zentrale Register auf EU-Ebene für die Datenerhebung und Transparenz** Artikel 32 Buchstabe a: Öffentliche Unionsregister aller anerkannten Anbieter von Datenvermittlungsdiensten und datenaltruistischen Organisationen. Art 32 (e): Die zuständigen Behörden melden der Kommission unverzüglich auf	

	elektronischem Wege neue Eintragungen, Änderungen und Löschungen, und die Kommission aktualisiert die Unionsregister entsprechend. **Koordinierung der Überwachung und Durchsetzung** Zuständige nationale Behörden Europäischer Dateninnovationsrat **Governance für die Übermittlung von Daten in Drittländer** Artikel 32aa: Anforderungen an die Übermittlung nicht-personenbezogener Daten in Drittländer durch Weiterverwender. **Ausschließlichkeitsvereinbarungen** Artikel 32k: Definition der Zulässigkeit von Ausschließlichkeitsvereinbarungen über die Weiterverwendung von Daten oder Dokumenten, die sich im Besitz öffentlicher Stellen befinden. Schreibt Transparenz der endgültigen Bedingungen vor.	
Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**	Artikel 1 **Gemeinsame Normen und interoperable Rahmen** - Der EDIB berät die Europäische Kommission im Hinblick auf Normungstätigkeiten in Verbindung mit sektorübergreifenden Aspekten der gemeinsamen Datennutzung, unter anderem im Zusammenhang mit der Entstehung gemeinsamer europäischer Datenräume unter Berücksichtigung sektorspezifischer Normungstätigkeiten. o Artikel 42: Der EDIB unterstützt die „Annahme der Leitlinien zur Festlegung von interoperablen Rahmen und gemeinsamen Verfahren für das Funktionieren gemeinsamer europäischer Datenräume“. - Gemeinsames Logo zur Identifizierung von Datenvermittlungsdiensten und	

	datenaltruistischen Organisationen. - Artikel 32q: Öffentliche Stellen und öffentliche Unternehmen stellen ihre Daten oder Dokumente, soweit möglich und sinnvoll, auf elektronischem Wege in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zusammen mit den zugehörigen Metadaten zur Verfügung. Sowohl die Formate als auch die Metadaten müssen soweit möglich förmlichen offenen Standards entsprechen. **Sonstige einschlägige Maßnahmen:** - Artikel 32t: Die Mitgliedstaaten setzen sich in Zusammenarbeit mit der Kommission weiterhin dafür ein, den Zugang zu Datensätzen zu vereinfachen, indem sie auf elektronischem Wege geeignete Datensätze in Formaten zur Verfügung stellen, die zugänglich, leicht auffindbar und weiterverwendbar sind. - Artikel 32u: Die Mitgliedstaaten unterstützen die Verfügbarkeit von Forschungsdaten in einer Weise, die mit den FAIR-Grundsätzen vereinbar ist.	
Verwendung gemeinsam vereinbarter offener technischer Spezifikationen und Standards **Bitte führen Sie solche Maßnahmen auf.**	Artikel 1 **Maßnahmen für maschinenlesbare Daten:** - Artikel 32a: Maschinenlesbares Register der Europäischen Union der Anbieter von Datenvermittlungsdiensten. - Artikel 32a: Maschinenlesbares Register der Europäischen Union der datenaltruistischen Organisationen. - Artikel 32q: Öffentliche Stellen stellen ihre Daten/Dokumente soweit möglich in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zusammen mit den zugehörigen Metadaten zur Verfügung. Sowohl die Formate als auch die Metadaten müssen soweit möglich förmlichen offenen Standards entsprechen. - Artikel 32q: Die hochwertigen Datensätze werden in maschinenlesbarem Format	

	über geeignete APIs und gegebenenfalls als Massen-Download zur Weiterverwendung zugänglich gemacht. - Artikel 32t: Die Mitgliedstaaten treffen praktische Vorkehrungen, die eine Suche nach den zur Weiterverwendung verfügbaren Daten oder Dokumenten erleichtern, wie z. B. Bestandslisten der wichtigsten Daten oder Dokumente mit zugehörigen Metadaten, die, soweit möglich und sinnvoll, online verfügbar sind und in einem maschinenlesbaren Format vorliegen, sowie Internet-Portale, die mit den Bestandslisten verknüpft sind. Soweit möglich, sorgen die Mitgliedstaaten dafür, dass eine sprachübergreifende Suche nach Daten oder Dokumenten vorgenommen werden kann. - Artikel 32w: Bestimmte hochwertige Datensätze sind maschinenlesbar. In Durchführungsrechtsakten können Regelungen im Hinblick auf Daten- und Metadatenformate sowie technische Modalitäten für die Verbreitung festgelegt werden. **Maßnahmen für Maschinen-zu-Maschinen-Interaktionen:** - Artikel 32ad: Verpflichtung zur Nutzung der zentralen Informationsstelle. Die zentrale Informationsstelle ist für die Entgegennahme von Anfragen oder Anträgen zuständig und übermittelt sie, soweit möglich und angemessen, auf automatisiertem Wege an die zuständigen öffentlichen Stellen oder die zuständigen Stellen. **Sonstige einschlägige Maßnahmen:** - Artikel 48a: Änderung des Anhangs II der Verordnung (EU) 2018/1724 (zentrales digitales Zugangstor). Prüfung von Synergien. - Erwägungsgrund 52 der Omnibus-Verordnung: Soweit möglich sollte die ENISA vorhandene nationale technische Lösungen, die die Meldung von Vorfällen erleichtern, wie z. B. nationale Plattformen, bei der Ausarbeitung der Spezifikationen für die technischen, operativen und organisatorischen Maßnahmen	

	im Hinblick auf die Errichtung, die Wartung und den sicheren Betrieb der zentralen Anlaufstelle berücksichtigen. Darüber hinaus sollte die ENISA technische Protokolle und Instrumente wie Anwendungsprogrammierschnittstellen und maschinenlesbare Standards berücksichtigen, die es den Einrichtungen ermöglichen, die Integration von Meldepflichten in Geschäftsprozesse zu erleichtern, und es den Behörden ermöglichen, die zentrale Anlaufstelle mit ihren nationalen Meldesystemen zu vernetzen.	

Digitaler öffentlicher Dienst Nr. 2 – Meldung von Sicherheitsvorfällen

Bewertung	**Maßnahme(n)**	**Mögliche verbleibende Hindernisse (falls zutreffend)**
Vereinbarkeit mit bestehenden digitalen und sektorspezifischen Strategien **Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.**	Artikel 6 Die allgemeine Angleichung an bestehende digitale und sektorspezifische Strategien erfolgt durch die Richtlinie (EU) 2022/2555 (NIS-2), die nunmehr durch die Digital-Omnibus-Verordnung geändert wird. Darüber hinaus sind in der Omnibus-Verordnung Synergien mit der europäischen Unternehmensbrieftasche und der Verordnung (EU) 2024/2847 (Cyberresilienzverordnung) vorgesehen. Insbesondere gilt: • In Artikel 23 Absatz 4 ist die Nutzung der zentralen Anlaufstelle für die NIS-2-Meldung vorgeschrieben. • In Artikel 23 Absatz 1 ist festgelegt, dass eine Meldung eines schwerwiegenden Sicherheitsvorfalls gemäß Artikel 14 Absatz 3 der Verordnung (EU) 2024/2847 (Cyberresilienzverordnung) ebenfalls eine Meldung von Informationen gemäß der Richtlinie (EU) 2022/2555 (NIS-2) darstellt. Damit wird dem Einmaligkeitsgrundsatz entsprochen. • In Artikel 23a Absatz 3 Buchstabe d ist die Verknüpfung mit den europäischen Unternehmensbrieftaschen vorgesehen.	

Organisatorische Maßnahmen für eine reibungslose grenzüberschreitende Erbringung digitaler öffentlicher Dienste **Bitte führen Sie die geplanten Governance-Maßnahmen auf.**	Artikel 6 In Artikel 23a sind die Aufgaben und Zuständigkeiten festgelegt. Die ENISA hat insbesondere folgende Aufgaben: • Entwicklung und Unterhaltung einer zentralen Anlaufstelle, um die Pflicht zur Meldung von Vorfällen und damit zusammenhängenden Ereignissen gemäß den Rechtsakten der Union zu unterstützen. • Technische, operative und organisatorische Maßnahmen, um die Risiken für die Sicherheit der zentralen Anlaufstelle und der übermittelten oder verbreiteten Informationen zu steuern. Dabei konsultiert sie die Kommission, das CSIRTs-Netzwerk und die jeweils zuständigen Behörden.	
Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**	Artikel 6 Mit Artikel 23a wird die ENISA mit der Ausarbeitung von Spezifikationen beauftragt, die die erforderliche Fähigkeit zur Interoperabilität im Hinblick auf andere einschlägige Meldepflichten sicherstellen. *Hinweis: Die inhaltlichen Anforderungen für die Meldung von Vorfällen sind in den einschlägigen Rechtsakten der Union, einschließlich der Richtlinie (EU) 2022/2555 (NIS-2), näher festgelegt. In Artikel 23a Absatz 3 Buchstabe c der Omnibus-Verordnung wird klargestellt, dass die ENISA dafür Sorge trägt, dass diese gebührend berücksichtigt werden.*	
Verwendung gemeinsam vereinbarter offener technischer Spezifikationen und Standards	Artikel 6 In Artikel 23a wird die Ausarbeitung von Spezifikationen gefordert: • Die ENISA legt die Spezifikationen für die technischen Maßnahmen im Hinblick auf die Errichtung, die Wartung und den sicheren Betrieb der zentralen Anlaufstelle fest und setzt sie um. Diese Spezifikationen umfassen unter anderem	

Bitte führen Sie solche Maßnahmen auf.	Folgendes: ○ die erforderliche Fähigkeit für die Interoperabilität im Hinblick auf andere einschlägige Meldepflichten; ○ technische Vorkehrungen, damit die einschlägigen Einrichtungen und Behörden auf Informationen der zentralen Anlaufstelle zugreifen, diese übermitteln, abrufen, übertragen oder anderweitig verarbeiten können, sowie technische Protokolle und Werkzeuge, die es den Einrichtungen und Behörden ermöglichen, die erhaltenen Informationen in ihren Systemen weiter zu verarbeiten. • Soweit verfügbar, muss die zentrale Anlaufstelle mit europäischen Unternehmensbrieftaschen interoperabel und kompatibel sein.	

4.5. Unterstützungsmaßnahmen für die digitale Umsetzung

Allgemeine Beschreibung der Unterstützungsmaßnahmen für die digitale Umsetzung

Beschreibung der Maßnahme	**Anforderung(en)**	**Rolle der Kommission** (falls zutreffend)	**Zu beteiligende Akteure** (falls zutreffend)	**Voraussichtlicher Zeitplan** (falls zutreffend)
Durchführungsrechtsakt: Gestaltung eines gemeinsamen Logos für Anbieter von Datenvermittlungsdiensten	Artikel 1	Festlegung der Merkmale des gemeinsamen Logos, einschließlich seiner Gestaltung und der Modalitäten für seine Verwendung.	Ausschuss für das Prüfverfahren	//
Durchführungsrechtsakt:	Artikel 1	Festlegung der	Ausschuss für das	//

Gestaltung eines gemeinsamen Logos für anerkannten Datenaltruismus		Merkmale des gemeinsamen Logos, einschließlich seiner Gestaltung und der Modalitäten für seine Verwendung.	Prüfverfahren	
Überwachung und Compliance: Die zuständigen Behörden können die Einhaltung der Vorschriften entweder auf eigene Initiative oder auf Antrag natürlicher oder juristischer Personen überwachen.	Artikel 1	//	Zuständige Behörden, Datenvermittlungsdienste, datenaltruistische Organisationen	//
Durchführungsrechtsakt: Bestimmte hochwertige Datensätze	Artikel 1	Festlegung einer Liste bestimmter hochwertiger Datensätze. Es können die Modalitäten für die Veröffentlichung und Weiterverwendung hochwertiger Datensätze festgelegt werden.	Ausschuss für das Prüfverfahren	//
Leitlinien: • EDIB berät im Hinblick auf Leitlinien für gemeinsame europäische Datenräume • EDIB verabschiedet Leitlinien für interoperable Rahmen	Artikel 1	Unterstützung aus dem EDIB	EDIB	//

Durchführungsrechtsakt: Gemeinsame Vorlage für die Meldung einer Verletzung des Schutzes personenbezogener Daten	Artikel 3	Annahme einer gemeinsamen Vorlage auf der Grundlage des Vorschlags des EDSA.	Ausschuss für das Prüfverfahren	//
Delegierter Rechtsakt: Automatisierte und maschinenlesbare Angaben zu den Wahlentscheidungen der betroffenen Person	Artikel 3	Festlegung der Pflichten von Anbietern von Webbrowsern und Endeinrichtungen	Ausschuss für das Prüfverfahren	//
Durchführungsrechtsakt: Meldung von Vorfällen gemäß der Richtlinie über die Resilienz kritischer Einrichtungen	Artikel 9	Präzisierung der Art und des Formats der gemäß Artikel 15 Absatz 1 der Richtlinie (EU) 2022/2557 (Richtlinie über die Resilienz kritischer Einrichtungen) gemeldeten Informationen.	//	//