EUROPÄISCHE
KOMMISSION

Brüssel, den 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)

(Text von Bedeutung für den EWR)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) beigefügt.

Daten sind ein zentraler Bestandteil der digitalen Wirtschaft und eine wesentliche Ressource für die Sicherung des ökologischen und des digitalen Wandels. Die Menge der von Menschen und Maschinen erzeugten Daten hat in den letzten Jahren exponentiell zugenommen. Die meisten Daten bleiben jedoch ungenutzt oder ihr Wert liegt hauptsächlich in den Händen einer relativ geringen Anzahl großer Unternehmen. Geringes Vertrauen, widersprüchliche wirtschaftliche Anreize und technologische Hindernisse hemmen die volle Ausschöpfung des Potenzials der datengesteuerten Innovation. Es ist daher von entscheidender Bedeutung, dieses Potenzial freizusetzen, indem Möglichkeiten für die Weiterverwendung von Daten geschaffen und Hindernisse für die Entwicklung der europäischen Datenwirtschaft im Einklang mit den europäischen Vorschriften und unter uneingeschränkter Achtung der europäischen Werte sowie entsprechend dem Auftrag, die digitale Kluft zu verringern, beseitigt werden, damit alle von diesen Möglichkeiten profitieren können. Die Gewährleistung einer ausgewogeneren Verteilung der Wertschöpfung aus Daten synchron zu der neuen Welle nicht personenbezogener Industriedaten und der Verbreitung von Produkten, die mit dem Internet der Dinge vernetzt sind, bedeutet ein enormes Potenzial für die Förderung einer nachhaltigen Datenwirtschaft in Europa.

Die Regulierung des Datenzugangs und der Datennutzung ist eine Grundvoraussetzung für die Nutzung der Chancen des digitalen Zeitalters, in dem wir leben. Die Präsidentin der Kommission, Ursula von der Leyen, wies in ihren politischen Leitlinien für die Kommission 2019–2024 darauf hin, dass Europa die „*Nutzung von Daten kanalisieren und gleichzeitig hohe ethische, Datenschutz- und Sicherheitsstandards wahren*“ muss[1]. Das Arbeitsprogramm der Kommission für 2020[2] enthält mehrere strategische Ziele, darunter die im Februar 2020 verabschiedete europäische Datenstrategie[3]. Ziel dieser Strategie ist es, einen echten Binnenmarkt für Daten zu schaffen und Europa zu einem weltweit führenden Akteur in der datenagilen Wirtschaft zu machen. Daher ist das Datengesetz eine tragende Säule und die zweite wichtige Initiative, die in der Datenstrategie angekündigt wurde. Insbesondere trägt es zur Schaffung eines sektorübergreifenden Governance-Rahmens für den Datenzugang und die Datennutzung bei, indem Rechtsvorschriften zu Fragen erlassen werden, die die Beziehungen zwischen Akteuren der Datenwirtschaft betreffen, um so Anreize für eine sektorübergreifende gemeinsame Datennutzung zu schaffen.

In den Schlussfolgerungen der Tagung des Europäischen Rates vom 21. und 22. Oktober 2021 wurde unterstrichen, „*wie wichtig es ist, dass bei bestehenden und künftigen Initiativen rasch Fortschritte erzielt werden, insbesondere indem das Datenpotenzial in Europa ausgeschöpft wird, vor allem durch einen umfassenden Regelungsrahmen, der innovationsfreundlich ist, eine bessere Datenübertragbarkeit und einen fairen Zugang zu Daten ermöglicht sowie*

---

[1] Ursula von der Leyen, Eine Union, die mehr erreichen will – Meine Agenda für Europa, Politische Leitlinien für die nächste Europäische Kommission 2019–2024, 16. Juli 2019.

[2] Europäische Kommission, Anhänge zum Arbeitsprogramm der Kommission 2020 – Eine Union, die mehr erreichen will, COM(2020) 37 vom 29. Januar 2020.

[3] COM(2020) 66 final.

Interoperabilität gewährleistet“[4]. Am 25. März 2021 bekräftigte der Europäische Rat, es sei wesentlich, „*das Potenzial von Daten und digitalen Technologien einschließlich künstlicher Intelligenz zum Vorteil der Gesellschaft und der Wirtschaft besser zu nutzen*“[5]. Auf seiner Tagung am 1. und 2. Oktober 2020 betonte er, *„dass hochwertige Daten leichter verfügbar gemacht werden müssen und eine bessere gemeinsame Nutzung und Bündelung von Daten sowie Interoperabilität gefördert und ermöglicht werden müssen“*[6]. In Bezug auf Cloud-Dienste nahmen die EU-Mitgliedstaaten am 15. Oktober 2020 einstimmig eine gemeinsame Erklärung zum Aufbau der nächsten Cloud-Generation in Europa für Unternehmen und den öffentlichen Sektor an. Zu diesem Zweck wäre eine nächste Generation von Cloud-Angeboten in der EU erforderlich, die beispielsweise in Bezug auf Portabilität und Interoperabilität höchsten Standards gerecht werden[7].

In der Entschließung des Europäischen Parlaments vom 25. März 2021 zum Thema „Eine europäische Datenstrategie“ wurde die Kommission mit Nachdruck aufgefordert, einen Rechtsakt über Daten vorzulegen, um einen größeren und fairen B2B-, B2G-, G2B- und G2G-Datenfluss in allen Wirtschaftszweigen zu fördern und zu ermöglichen[8]. In der Entschließung vom 25. März 2021 betonte das Europäische Parlament ferner, dass gemeinsame europäische Datenräume geschaffen werden müssen, um den freien Verkehr nicht personenbezogener Daten über Grenzen und Branchen hinweg sicherzustellen und den Datenfluss zwischen Unternehmen, Wissenschaftlern, relevanten Interessenträgern und dem öffentlichen Sektor zu verstärken. Vor diesem Hintergrund forderte es die Kommission auf, die Nutzungsrechte zu klären, insbesondere in B2B- und B2G-Marktumgebungen. Das Parlament stellte fest, dass durch Marktungleichgewichte, die sich aus der Datenkonzentration ergeben, der Wettbewerb beschränkt, Marktzutrittsbeschränkungen verstärkt und der breitere Datenzugang und die breitere Datennutzung beeinträchtigt werden.

In der Entschließung wies das Europäische Parlament außerdem darauf hin, dass für kleine und mittlere Unternehmen (KMU) bei vertraglichen Vereinbarungen zwischen Unternehmen (B2B) nicht unbedingt ein angemessener Zugang zu Daten sichergestellt ist. Der Grund dafür sind Ungleichheiten in Bezug auf die Verhandlungsposition oder das Fachwissen. Das Europäische Parlament betonte daher, dass klare Verpflichtungen und die Haftung in Bezug auf den Zugang, die Verarbeitung, die gemeinsame Nutzung und die Speicherung von Daten in Verträgen festgelegt werden müssen, um die missbräuchliche Nutzung solcher Daten zu begrenzen.

Folglich wurden die Kommission und die EU-Mitgliedstaaten aufgefordert, die Rechte und Pflichten der Akteure in Bezug auf den Zugang zu Daten zu prüfen, an deren Erstellung sie beteiligt waren und ihr Bewusstsein in Bezug auf diese Rechte zu schärfen, insbesondere das Datenzugangsrecht, das Recht auf Übertragbarkeit, das Recht, eine andere Partei aufzufordern, die Verwendung dieser Daten einzustellen oder sie zu berichtigen oder zu löschen, wobei auch die Inhaber dieser Rechte zu benennen und die Art dieser Rechte zu beschreiben sind.

---

4 Europäischer Rat, Tagung des Europäischen Rates (21.–22. Oktober 2021) – Schlussfolgerungen, EUCO 17/21, 2021, S. 2.

5 Europäischer Rat, Erklärung der Teilnehmer der Tagung des Europäischen Rates (25. März 2021) – Erklärung SN 18/21, S. 4.

6 Tagung des Europäischen Rates (1.–2. Oktober 2020) – Schlussfolgerungen, EUCO 13/20, 2020, S. 5.

7 Europäische Kommission (2020), *Kommission begrüßt Erklärung der Mitgliedstaaten zum europäischen Cloud-Zusammenschluss*, Pressemitteilung.

8 Entschließung des Europäischen Parlaments vom 25. März 2021 zum Thema „Eine europäische Datenstrategie“ (2020/2217(INI)).

Im Hinblick auf die B2G-Datenweitergabe forderte das Europäische Parlament die Kommission auf, die Umstände, Bedingungen und Anreize näher zu definieren, unter denen die Privatwirtschaft verpflichtet sein sollte, Daten an den öffentlichen Sektor weiterzugeben, etwa weil sie für die Organisation datengesteuerter öffentlicher Dienste benötigt werden, und auch Systeme für die obligatorische gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden zu prüfen, etwa in Situationen, die sich der Kontrolle der betreffenden Personen entziehen.

Vor diesem Hintergrund unterbreitet die Kommission den Vorschlag für ein **Datengesetz** mit dem Ziel, **eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft zu gewährleisten und den Datenzugang und die Datennutzung zu fördern**.

Der Vorschlag wird dazu beitragen, die allgemeineren politischen Ziele zu erreichen, welche darin bestehen die Innovations- und Wettbewerbsfähigkeit von EU-Unternehmen sämtlicher Branchen sicherzustellen, die Handlungskompetenz der Menschen in Bezug auf ihre Daten wirksam zu stärken und Unternehmen und öffentliche Stellen besser mit einem angemessenen und vorhersehbaren Mechanismus für die Bewältigung wichtiger politischer und gesellschaftlicher Herausforderungen, einschließlich öffentlicher Notstände und anderer Ausnahmesituationen, auszustatten. Die Unternehmen werden in der Lage sein, ihre Daten und anderen digitalen Vermögenswerte problemlos zwischen konkurrierenden Anbietern von Cloud-Diensten und anderen Datenverarbeitungsdiensten zu übertragen. Der Datenaustausch innerhalb und zwischen Wirtschaftszweigen erfordert einen Interoperabilitätsrahmen mit verfahrenstechnischen und legislativen Maßnahmen zur Stärkung des Vertrauens und zur Steigerung der Effizienz. Die Schaffung gemeinsamer europäischer Datenräume für strategische Wirtschaftszweige und Bereiche von öffentlichem Interesse wird zu einem echten Binnenmarkt für Daten beitragen, der den Austausch und die sektorübergreifende Nutzung von Daten ermöglicht. Diese Verordnung trägt daher zu den Governance-Rahmen und zur Infrastruktur sowie zur gemeinsamen Nutzung von Daten außerhalb von Datenräumen bei.

Die spezifischen Ziele des Vorschlags sind nachstehend aufgeführt.

– **Erleichterung des Datenzugangs und der Datennutzung für Verbraucher und Unternehmen bei gleichzeitiger Aufrechterhaltung von Anreizen für Investitionen in die Wertschöpfung durch Daten:** Dies umfasst die Erhöhung der Rechtssicherheit im Rahmen der gemeinsamen Nutzung von Daten, die bei der Nutzung von Produkten oder verbundenen Diensten erlangt oder erzeugt werden, sowie die konkrete Anwendung von Vorschriften zur Gewährleistung der Fairness bei Verträgen über gemeinsame Datennutzung. In dem Vorschlag wird **präzisiert**, inwieweit die in der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken (Datenbankrichtlinie)[9] verankerten einschlägigen Rechte in seinem Rahmen angewandt werden.

– **Einführung der Nutzung von im Besitz von Unternehmen befindlichen Daten durch öffentliche Stellen sowie Organe, Einrichtungen oder sonstige Stellen der Union in bestimmten Situationen, in denen eine außergewöhnliche Notwendigkeit dazu besteht:** Dies betrifft in erster Linie öffentliche Notstände, aber auch andere Ausnahmesituationen, in denen eine obligatorische gemeinsame Nutzung von Daten durch Unternehmen und Behörden gerechtfertigt ist, um

[9] ABl. L 77 vom 27.3.1996, S. 20.

evidenzbasierte, wirksame, effiziente und leistungsorientierte öffentliche Maßnahmen und Dienste zu unterstützen.

– **Erleichterung des Wechsels zwischen Cloud- und Edge-Diensten:** Der Zugang zu wettbewerbsfähigen und interoperablen Datenverarbeitungsdiensten ist eine Voraussetzung für eine florierende Datenwirtschaft, in der Daten innerhalb und zwischen sektorspezifischen Ökosystemen leicht weitergegeben werden können. Die Inanspruchnahme dieser Dienste durch die Nutzer in allen Wirtschaftssektoren ist vom Grad des Vertrauens in die Datenverarbeitungsdienste abhängig.

– **Einführung von Schutzvorkehrungen gegen die unrechtmäßige Datenübermittlung ohne Meldung durch Cloud-Diensteanbieter:** Dies ist darauf zurückzuführen, dass Bedenken hinsichtlich des unrechtmäßigen Zugriffs auf Daten durch Regierungen, die nicht zur EU oder zum Europäischen Wirtschaftsraum (EWR) gehören, geäußert wurden. Solche Schutzvorkehrungen dürften das Vertrauen in die Datenverarbeitungsdienste, auf die sich die europäische Datenwirtschaft zunehmend stützt, weiter stärken.

– **Geplante Entwicklung von Interoperabilitätsstandards für Daten, die von anderen Sektoren weiterverwendet werden sollen**, um Hindernisse für die gemeinsame Nutzung von Daten über bereichsspezifische gemeinsame europäische Datenräume hinweg im Einklang mit den sektorspezifischen Interoperabilitätsanforderungen und Hindernisse für die Nutzung anderer Daten zu beseitigen, die nicht in den Geltungsbereich eines spezifischen gemeinsamen europäischen Datenraums fallen. Der Vorschlag unterstützt auch die Festlegung von Normen für „intelligente Verträge“. Dabei handelt es sich um Computerprogramme in elektronischen Vorgangsregistern, die Transaktionen zu vorab festgelegten Bedingungen ausführen und abwickeln. Sie haben das Potenzial, Dateninhabern und Datenempfängern Garantien dafür zu bieten, dass die Bedingungen für die gemeinsame Nutzung von Daten eingehalten werden.

• **Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich**

Dieser Vorschlag steht im Einklang mit den geltenden Vorschriften über die **Verarbeitung personenbezogener Daten** (einschließlich der Datenschutz-Grundverordnung (DSGVO)[10]) und den Schutz des Privatlebens und der **Vertraulichkeit der Kommunikation** sowie aller (personenbezogenen und nicht personenbezogenen) Daten, die auf Endgeräten gespeichert sind und auf die darüber zugegriffen wird (e-Datenschutzrichtlinie[11], die durch die derzeit in Legislativverhandlungen erörterte e-Datenschutzverordnung ersetzt werden soll). Dieser Vorschlag ergänzt bestehende Rechte, insbesondere Rechte in Bezug auf Daten, die durch ein Produkt eines Nutzers erzeugt werden, das an ein öffentlich zugängliches elektronisches Kommunikationsnetz angeschlossen ist.

Mit der **Verordnung über den freien Verkehr nicht personenbezogener Daten**[12] wurde ein wichtiger Baustein der europäischen Datenwirtschaft geschaffen, indem sichergestellt wird, dass nicht personenbezogene Daten überall in der Union gespeichert, verarbeitet und übermittelt werden können. Außerdem stellte sie einen Selbstregulierungsansatz für das Problem der Anbieterbindung auf der Ebene der Anbieter von Datenverarbeitungsdiensten vor, indem Verhaltenskodizes eingeführt wurden, um den Übertragung von Daten zwischen Cloud-Diensten zu erleichtern (von der Industrie entwickelte Verhaltenskodizes für den

10 ABl. L 119 vom 4.5.2016, S. 1.
11 ABl. L 201 vom 31.7.2002, S. 37.
12 ABl. L 303 vom 28.11.2018, S. 59, SWIPO (2021), siehe *Website*.

Wechsel zwischen Cloud-Diensteanbietern und die Übertragung von Daten („Switching Cloud Providers and Porting Data – SWIPO“)). Dieser Vorschlag baut darauf weiter auf und trägt so dazu bei, dass Unternehmen und Bürger das Recht auf den Wechsel des Cloud-Anbieters und die Übertragung der Daten bestmöglich nutzen können. Er steht außerdem im Hinblick auf das Vertragsrecht voll und ganz im Einklang mit der Richtlinie über missbräuchliche Vertragsklauseln[13]. In Bezug auf Cloud-Dienste scheint der Selbstregulierungsansatz die Marktdynamik nicht wesentlich beeinflusst zu haben; daher enthält dieser Vorschlag einen Regulierungsansatz für das Problem, das in der Verordnung über den freien Verkehr nicht personenbezogener Daten hervorgehoben wird.

Die internationale Datenverarbeitung, -speicherung und -übermittlung wird durch die DSGVO, die Handelsverpflichtungen im Rahmen der Welthandelsorganisation (WTO), das Allgemeine Übereinkommen über den Handel mit Dienstleistungen (GATS) und bilaterale Handelsabkommen geregelt.

Das **Wettbewerbsrecht**[14] ist u. a. im Kontext der Fusionskontrolle, der gemeinsamen Nutzung von Daten durch Unternehmen oder des Missbrauchs einer beherrschenden Stellung eines Unternehmens anwendbar.

Die **Datenbankrichtlinie**[15] sieht für Datenbanken, die das Ergebnis umfangreicher Investitionen sind, einen Schutz *sui generis* vor, auch wenn die betreffende Datenbank selbst keine eigene geistige Schöpfung mit Urheberrechtsschutz darstellt. Aufbauend auf der umfangreichen Rechtsprechung zur Auslegung der Bestimmungen der Datenbankrichtlinie werden mit diesem Vorschlag bestehende Rechtsunsicherheiten in Bezug darauf angegangen, ob Datenbanken, die Daten enthalten, die durch die Nutzung von Produkten oder verbundenen Diensten, wie z. B. Sensoren, erzeugt oder erlangt wurden, oder andere Arten von maschinengenerierten Daten, Anspruch auf einen solchen Schutz hätten.

In der **P2B-Verordnung**[16] werden Transparenzverpflichtungen festgelegt, nach denen Plattformen eine Beschreibung der bei der Bereitstellung des Dienstes erzeugten Daten für gewerbliche Nutzer liefern müssen.

Die **Richtlinie über offene Daten**[17] enthält Mindestvorschriften für die Weiterverwendung von im Besitz des öffentlichen Sektors befindlichen Daten und von öffentlich finanzierten Forschungsdaten, die über Archive öffentlich zugänglich gemacht werden.

Mit der **Initiative „Interoperables Europa“** soll eine auf Kooperation beruhende Interoperabilitätsstrategie für einen modernisierten öffentlichen Sektor eingeführt werden. Die Initiative ist aus dem Programm ISA[2] hervorgegangen, einem Finanzierungsprogramm der Union, das von 2016 bis 2021 lief und die Entwicklung digitaler Lösungen zur Ermöglichung interoperabler grenz- und sektorübergreifender öffentlicher Dienste unterstützte[18].

Dieser Vorschlag ergänzt das kürzlich verabschiedete **Daten-Governance-Gesetz**, das die freiwillige gemeinsame Nutzung von Daten durch Einzelpersonen und Unternehmen erleichtern und die Bedingungen für die Nutzung bestimmter Daten des öffentlichen Sektors harmonisieren soll, ohne dass die materiellen Rechte an den Daten oder die bestehenden

13 ABl. L 95 vom 21.4.1993, S. 29.
14 ABl. L 335 vom 18.12.2010, S. 36.
15 ABl. L 77 vom 27.3.1996, S. 20.
16 ABl. L 186 vom 11.7.2019, S. 57.
17 ABl. L 172 vom 26.6.2019, S. 56.
18 ABl. L 318 vom 4.12.2015, S. 1.

Datenzugangs- und -nutzungsrechte geändert werden[19]. Er ergänzt darüber hinaus den Vorschlag für ein **Gesetz über digitale Märkte**, nach dem bestimmte Betreiber zentraler Plattformdienste, die als „Gatekeeper“ eingestuft wurden, unter anderem für eine wirksamere Übertragbarkeit von Daten sorgen müssen, die durch Tätigkeiten von Unternehmen und Endnutzern erzeugt werden[20].

Dieser Vorschlag berührt nicht die bestehenden Vorschriften in den Bereichen geistiges Eigentum (mit Ausnahme der Anwendung des in der Datenbankrichtlinie festgelegten Schutzrechts *sui generis*), Wettbewerb, Justiz und Inneres sowie damit zusammenhängende (internationale) Zusammenarbeit, handelsbezogene Verpflichtungen oder den rechtlichen Schutz von Geschäftsgeheimnissen.

Zur Förderung des digitalen Wandels sind in verschiedenen Bereichen Anpassungen der Rechtsvorschriften erforderlich. Im Rahmen des Europäischen digitalen Produktpasses (der Teil der Initiative für nachhaltige Produkte ist) werden klare Regeln für den Zugang zu spezifischen Daten festgelegt, die für die Kreislauffähigkeit und Nachhaltigkeit bestimmter Produkte während ihres gesamten Lebenszyklus und in nicht außergewöhnlichen Situationen erforderlich sind[21]. Privatrechtliche Vorschriften sind ein zentrales Element des Gesamtrahmens. Mit dieser Verordnung werden daher das Vertragsrecht und andere Vorschriften angepasst, um die Bedingungen für die Weiterverwendung von Daten im Binnenmarkt zu verbessern und um zu verhindern, dass Vertragsparteien Ungleichgewichte in der Verhandlungsposition zum Nachteil schwächerer Parteien missbrauchen.

Da es sich um einen horizontalen Vorschlag handelt, sieht das **Datengesetz** in Bezug auf die Datennutzungsrechte **grundlegende Vorschriften für alle Sektoren** vor, z. B. für die Bereiche intelligente Maschinen oder Verbrauchsgüter. Die Rechte und Pflichten in Bezug auf den Datenzugang und die Datennutzung wurden jedoch auch auf sektoraler Ebene in unterschiedlichem Maße geregelt. Durch das Datengesetz werden solche bestehenden Rechtsvorschriften nicht geändert, doch künftige Vorschriften in diesen Bereichen sollten prinzipiell an die horizontalen Grundsätze des Datengesetzes angeglichen werden. Die Konvergenz mit den horizontalen Vorschriften des Datengesetzes sollte bei der Überarbeitung sektoraler Instrumente bewertet werden. Der vorliegende Vorschlag lässt Raum für vertikale Rechtsvorschriften, in denen detailliertere Vorschriften für die Erreichung sektorspezifischer Regulierungsziele festgelegt werden.

Angesichts der bestehenden sektorspezifischen Rechtsvorschriften wird die Überarbeitung[22] der **INSPIRE-Richtlinie**[23] im Hinblick auf die Schaffung des Datenraums für den Grünen Deal eine weitere offene Verfügbarkeit und Weiterverwendung von Raum- und Umweltdaten ermöglichen. Diese Initiative zielt darauf ab, Behörden, Bürgern und Unternehmen in der EU die Unterstützung des Übergangs zu einer umweltfreundlicheren und CO_2-neutralen Wirtschaft zu erleichtern und den Verwaltungsaufwand zu verringern. Sie soll Dienste für weiterverwendbare Daten in großem Maßstab unterstützen, um die Erhebung, gemeinsame Nutzung, Verarbeitung und Analyse großer Datenmengen zu fördern, die für die Gewährleistung der Einhaltung der Umweltvorschriften im Zusammenhang mit den im europäischen Grünen Deal festgelegten vorrangigen Maßnahmen relevant sind. Sie wird die Berichterstattung straffen und den Verwaltungsaufwand durch eine bessere

19 COM(2020) 767 final.
20 ABl. L 186 vom 11.7.2019, S. 57.
21 COM(2020) 98 final.
22 Initiative GreenData4All (REFIT) | Legislativfahrplan | Europäisches Parlament (europa.eu).
23 ABl. L 108 vom 25.4.2007, S. 1.

Weiterverwendung vorhandener Daten, eine automatische Generierung von Meldungen durch gezielte Datensuche und eine datengestützte Unternehmensführung verringern.

Gemäß der **EU-Elektrizitätsverordnung**[24] müssen die Übertragungsnetzbetreiber Daten für die Regulierungsbehörden und die Planung angemessener Ressourcen zur Verfügung stellen, während die **EU-Elektrizitätsrichtlinie**[25] einen transparenten und nichtdiskriminierenden Zugang zu Daten vorsieht und der Kommission den Auftrag erteilt, entsprechende Interoperabilitätsanforderungen und -verfahren zu entwickeln, um dies zu erleichtern. Mit der **Zahlungsdiensterichtlinie 2**[26] werden unter bestimmten Bedingungen einige Arten von Zahlungsvorgangs- und Kontoinformationen zugänglich gemacht, wodurch der Austausch von Daten zwischen Unternehmen im Bereich FinTech ermöglicht wird. Im Mobilitäts- und Verkehrssektor gibt es ein breites Spektrum an Vorschriften für den Datenzugang und die gemeinsame Datennutzung. Reparatur- und Wartungsinformationen für Kraftfahrzeuge und landwirtschaftliche Maschinen unterliegen gemäß den **Rechtsvorschriften über die Typgenehmigung**[27] besonderen Verpflichtungen in Bezug auf den Datenzugang und die gemeinsame Datennutzung. Allerdings sind neue Vorschriften erforderlich, um sicherzustellen, dass die bestehenden Rechtsvorschriften für die Typgenehmigung von Fahrzeugen für das digitale Zeitalter geeignet sind und die Entwicklung sauberer, vernetzter und automatisierter Fahrzeuge fördern. Aufbauend auf dem Datengesetz als Rahmen für den Datenzugang und die Datennutzung werden diese Vorschriften sektorspezifische Herausforderungen, einschließlich Fragen des Zugangs zu Fahrzeugfunktionen und -ressourcen, angehen.

Im Rahmen der **Richtlinie über intelligente Verkehrssysteme**[28] wurden mehrere delegierte Verordnungen ausgearbeitet, denen weitere folgen werden, insbesondere zur Festlegung der Datenzugänglichkeit für den Straßen- und den multimodalen Personenverkehr, vor allem über nationale Zugangspunkte. Im Flugverkehrsmanagement sind nichtoperative Daten wichtig, um die Intermodalität und die Konnektivität zu verbessern. Operative Daten im Zusammenhang mit dem Flugverkehrsmanagement würden unter die spezifische Regelung fallen, die im Rahmen des **einheitlichen europäischen Luftraums**[29] festgelegt wurde. Bei der Überwachung des Schiffsverkehrs sind schiffsbezogene Daten (Schiffsverfolgung und -aufspürung) wichtig, um die Intermodalität und Konnektivität zu verbessern: Diese Daten fallen unter die spezifische Regelung der VTMIS-Richtlinie[30]. Darüber hinaus fallen sie in den Bereich des digitalen Seeverkehrssystems und der digitalen Seeverkehrsdienstleistungen[31]. Der Vorschlag für eine Verordnung über den Aufbau der **Infrastruktur für alternative Kraftstoffe**[32] führt die relevanten Datenarten auf, die in Synergie mit dem in der Richtlinie über intelligente Verkehrssysteme festgelegten allgemeinen Rahmen zur Verfügung gestellt werden sollen.

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

Dieser Vorschlag steht im Einklang mit den Prioritäten der Kommission dahin gehend,

24 ABl. L 158 vom 14.6.2019, S. 54.
25 ABl. L 158 vom 14.6.2019, S. 125.
26 ABl. L 337 vom 23.12.2015, S. 35, ABl. L 337 vom 23.12.2015, S. 35.
27 ABl. L 151 vom 14.6.2018, S. 1, ABl. L 60 vom 2.3.2013, S. 1.
28 ABl. L 207 vom 6.8.2010, S 1.
29 ABl. L 96 vom 31.3.2004, S. 1, ABl. L 96 vom 31.3.2004, S. 10, ABl. L 96 vom 31.3.2004, S. 20.
30 ABl. L 308 vom 29.10.2014, S. 82.
31 ABl. L 96 vom 12.4.2016, S. 46.
32 COM(2021) 559 final.

Europa für das digitale Zeitalter zu rüsten und eine zukunftsfähige Wirtschaft im Dienste der Menschen aufzubauen[33], in der die Digitalisierung des Binnenmarkts durch ein hohes Maß an Vertrauen, Schutz, Sicherheit und Auswahlmöglichkeiten für die Verbraucher gekennzeichnet ist. Die Digitalisierung des Binnenmarkts ist dank eines Rahmens, der Transparenz, Wettbewerb und Innovation fördert und technologieneutral ist, stark wettbewerblich geprägt. Der Vorschlag unterstützt die **Aufbau- und Resilienzfazilität**[34], wobei Lehren aus der COVID-19-Pandemie und den Vorteilen von im Bedarfsfall leichter zugänglicher Daten gezogen werden.

Mit diesem Vorschlag wird die entscheidende Rolle von Daten bei der Verwirklichung der **Ziele des europäischen Grünen Deals** auf verschiedene Weise unterstützt: erstens durch die Verbesserung des Verständnisses von Regierungen, Unternehmen und Einzelpersonen für die Auswirkungen von Produkten, Dienstleistungen und Materialien auf die Gesellschaft und die Wirtschaft über die gesamten Lieferketten hinweg; zweitens durch Mobilisierung der vorhandenen Fülle an einschlägigen Daten des Privatsektors, um Fragen im Zusammenhang mit Klimaschutz, biologischer Vielfalt, Umweltverschmutzung[35] und natürlichen Ressourcen im Einklang mit den Zielen des europäischen Grünen Deals[36], den einschlägigen Schlussfolgerungen[37] des Rates und Standpunkten des Europäischen Parlaments[38] anzugehen; drittens durch Schließung von Wissenslücken und durch Krisenmanagement in diesem Bereich mithilfe verstärkter Eindämmungs-, Vorsorge-, Bewältigungs- und Wiederaufbaumaßnahmen.

Im Einklang mit der **Industriestrategie**[39] befasst sich der Vorschlag mit hochstrategischen Technologien wie Cloud-Computing und Systemen der künstlichen Intelligenz, d. h. mit Bereichen, deren Potenzial die EU erst noch voll ausschöpfen muss, während die nächste Welle von Industriedaten naht. Der Vorschlag dient der Verwirklichung des Ziels der **Datenstrategie**[40], Unternehmen besser zu Innovation und Wettbewerb auf der Grundlage der Werte der EU zu befähigen, und der Umsetzung des Grundsatzes des **freien Datenverkehrs im Binnenmarkt**. Er stimmt auch mit dem **Aktionsplan für geistiges Eigentum**[41] überein, in dem sich die Kommission verpflichtet hat, die Datenbankrichtlinie zu überarbeiten.

Dieser Vorschlag sollte darüber hinaus mit den Grundsätzen des Aktionsplans zur europäischen Säule sozialer Rechte[42] und den Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen[43] im Einklang stehen.

---

33 COM(2020) 67 final.
34 ABl. L 57 vom 18.2.2021, S. 17.
35 COM(2021) 400 final.
36 COM(2019) 640 final.
37 Digitalisierung zum Wohle der Umwelt, 11. Dezember 2020, Schlussfolgerungen des Rates zum neuen Aktionsplan für die Kreislaufwirtschaft, 11. Dezember 2020, Schlussfolgerungen des Rates zur Biodiversitätsstrategie für 2030, 16. Oktober 2020, Schlussfolgerungen zur Verbesserung der Luftqualität, 5. März 2020.
38 Klima- und Umweltnotstand – 28. November 2019 (europa.eu).
39 COM(2021) 350 final.
40 COM(2020) 66 final.
41 COM(2020) 760 final.
42 COM(2021) 102 final.
43 ABl. L 151 vom 7.6.2019.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Die Rechtsgrundlage für diesen Vorschlag ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, wonach Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten erlassen werden, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.

Mit diesem Vorschlag soll die Verwirklichung des Binnenmarkts für Daten weiter vorangebracht werden, sodass Daten des öffentlichen Sektors sowie von Unternehmen und Einzelpersonen bestmöglich genutzt und gleichzeitig die Rechte in Bezug auf diese Daten und die zu ihrer Erhebung getätigten Investitionen geachtet werden. Die Bestimmungen über den Wechsel zwischen Datenverarbeitungsdiensten zielen darauf ab, faire und wettbewerbsorientierte Marktbedingungen für den Binnenmarkt für Cloud-, Edge- und verbundene Dienste zu schaffen.

Der Schutz vertraulicher Geschäftsdaten sowie von Geschäftsgeheimnissen ist ein wichtiger Aspekt für einen reibungslos funktionierenden Binnenmarkt, wie dies auch in anderen Zusammenhängen der Fall ist, in denen Dienste erbracht und Waren gehandelt werden. Mit diesem Vorschlag wird die Wahrung von Geschäftsgeheimnissen im Zusammenhang mit der Nutzung von Daten zwischen Unternehmen oder durch Verbraucher gewährleistet. Durch diese Initiative kann die Union von der Größe des Binnenmarkts profitieren, da Produkte oder verbundene Dienste häufig unter Nutzung von Daten aus mehreren Mitgliedstaaten entwickelt und später in der gesamten Union vermarktet werden.

Einige Mitgliedstaaten haben gesetzgeberische Maßnahmen ergriffen, um die hier dargelegten Probleme in den Beziehungen zwischen Unternehmen sowie zwischen Unternehmen und Behörden zu beheben, andere haben dies nicht getan. Dies kann zu einer Fragmentierung der Rechtsvorschriften im Binnenmarkt und zu abweichenden Vorschriften und Praktiken in der Union sowie unterschiedlich hohen damit verbundenen Kosten für Unternehmen führen, die unterschiedliche Regelungen einhalten müssten. Daher muss sichergestellt werden, dass die vorgeschlagenen Maßnahmen in allen Mitgliedstaaten einheitlich angewandt werden.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Da Daten grenzüberschreitend genutzt werden und sich das Datengesetz auf zahlreiche Bereiche auswirkt, können die in diesem Vorschlag abgedeckten Aspekte nicht wirksam auf der Ebene der Mitgliedstaaten behandelt werden. Eine Fragmentierung aufgrund von Unterschieden zwischen nationalen Vorschriften sollte vermieden werden, da dies zu höheren Transaktionskosten, mangelnder Transparenz, Rechtsunsicherheit und unerwünschtem „Forum Shopping“ (Wahl des günstigsten Gerichtsstands) führen würde. Dies zu vermeiden, ist insbesondere in allen Situationen wichtig, in denen es um Daten in Geschäftsbeziehungen zwischen Unternehmen geht, einschließlich fairer Vertragsbedingungen und der Pflichten der Anbieter von Produkten und verbundenen Diensten im Zusammenhang mit dem Internet der Dinge. All dies sind Aspekte, für die ein unionsweit einheitlicher Rechtsrahmen erforderlich ist.

Eine Bewertung der grenzüberschreitenden Aspekte des Datenflusses im Bereich der gemeinsamen Nutzung von Daten zwischen Unternehmen und Behörden zeigt ebenfalls, dass Handlungsbedarf auf Unionsebene besteht. Bei vielen privaten Akteuren, die im Besitz entsprechender Daten sind, handelt es sich um multinationale Unternehmen. Diese Unternehmen sollten nicht mit uneinheitlichen rechtlichen Regelungen konfrontiert sein.

Cloud-Computing-Dienste werden selten nur in einem einzigen Mitgliedstaat angeboten. Im Einklang mit der DSGVO und der Verordnung über den freien Verkehr nicht personenbezogener Daten, wonach Verbraucher und Unternehmen personenbezogene und nicht personenbezogene Daten überall in der Union verarbeiten dürfen, ist die grenzüberschreitende Verarbeitung von Daten innerhalb der Union für eine Geschäftstätigkeit im Binnenmarkt ausschlaggebend. Daher ist es von entscheidender Bedeutung, dass die Bestimmungen über den Wechsel zwischen Datenverarbeitungsdiensten auf Unionsebene angewandt werden, um eine schädliche Fragmentierung in einem ansonsten einheitlichen Markt für Datenverarbeitungsdienste zu vermeiden.

Nur durch ein gemeinsames Vorgehen auf Unionsebene können die in diesem Vorschlag festgelegten Ziele erreicht werden, einschließlich der Schaffung eines innovativen, wettbewerbsfähigen und fairen Geschäftsumfelds für datenintensive Unternehmen und der Stärkung der Handlungskompetenz der Bürger. Diese gemeinsame Maßnahme ist ein deutlicher Schritt vorwärts bei der Verwirklichung der Vision, einen echten Binnenmarkt für Daten zu schaffen.

- **Verhältnismäßigkeit**

Mit diesem Vorschlag werden die Rechte und Interessen der betroffenen Interessenträger gegen das allgemeine Ziel abgewogen, einem breiten Spektrum von Akteuren eine umfassendere Nutzung von Daten zu erleichtern. Damit wird ein förderlicher Rahmen geschaffen, der nicht über das zur Erreichung der Ziele erforderliche Maß hinausgeht. Der Vorschlag befasst sich mit den bestehenden Hindernissen für eine bessere Nutzung des potenziellen Werts von Daten durch Unternehmen, Verbraucher und den öffentlichen Sektor. Außerdem wird ein Rahmen für künftige sektorspezifische Vorschriften festgelegt, um Fragmentierung und Rechtsunsicherheit zu vermeiden. Bestehende Rechte werden präzisiert und gegebenenfalls Datenzugangsrechte gewährt, wodurch die Entwicklung eines Binnenmarkts für die gemeinsame Datennutzung gefördert wird. Die Initiative erlaubt ein großes Maß an Flexibilität bei der sektorspezifischen Anwendung.

Dieser Vorschlag zieht finanzielle und administrative Kosten nach sich. Diese müssen hauptsächlich von den nationalen Behörden, Herstellern und Diensteanbietern getragen werden, damit sie den in dieser Verordnung festgelegten Pflichten nachkommen können. Die Auslotung verschiedener Optionen und ihrer erwarteten Kosten und Nutzeffekte hat jedoch zu einer ausgewogenen Gestaltung des Instruments geführt. Darüber hinaus werden die Kosten für die Nutzer und die Inhaber der Daten durch die Vorteile ausgeglichen, die sich aus einem breiteren Datenzugang und einer breiteren Datennutzung sowie aus der Markteinführung neuartiger Dienste ergeben.

- **Wahl des Instruments**

Die Wahl fiel auf eine Verordnung, weil dadurch die umfassenderen politischen Ziele am besten erreicht werden können, sicherzustellen, dass alle Unternehmen in der Union in die Lage versetzt werden, innovativ zu sein und im Wettbewerb zu bestehen, dass die Verbraucher mehr Kontrolle über ihre Daten erhalten und dass die Organe, Einrichtungen und sonstigen Stellen der Union besser für die Bewältigung großer politischer Herausforderungen, einschließlich öffentlicher Notstände, gerüstet sind. Angesichts des mit dem Vorschlag verfolgten Ziels einer umfassenden Harmonisierung ist eine Verordnung erforderlich, um Rechtssicherheit und Transparenz für die Wirtschaftsakteure, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, zu gewährleisten und um juristischen und natürlichen Personen in allen Mitgliedstaaten das gleiche Maß an durchsetzbaren Rechten und Pflichten zu geben, sodass für eine einheitliche Durchsetzung in

allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den zuständigen Behörden der verschiedenen Mitgliedstaaten gesorgt wird.

Der Vorschlag wird den Binnenmarkt für Daten stärken, indem er die Rechtssicherheit erhöht und einen einheitlichen und kohärenten horizontalen Rechtsrahmen gewährleistet.

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

• Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften

Dieser Vorschlag beruht teilweise auf der jüngsten Bewertung der Datenbankrichtlinie und der unterstützenden Studie der Kommission zur Überarbeitung der Richtlinie[44]. Mit der Datenbankrichtlinie wurde unter anderem ein spezifisches Schutzrecht sui generis eingeführt, um Datenbanken zu schützen, wenn der Hersteller einer Datenbank wesentlich in die Beschaffung, Überprüfung und Darstellung der Daten investiert hat. Seit ihrer ersten Annahme wurde die Richtlinie zweimal bewertet. Beide Evaluierungen wurden durch Mitteilungen der Kommission zur Politik für die Datenwirtschaft[45] ergänzt.

Der Gerichtshof der Europäischen Union hat den Begriff der wesentlichen Investitionen in eine Datenbank geschärft und dabei klargestellt, dass durch das Schutzrecht sui generis die Investitionen in die Datenerhebung geschützt werden sollen und nicht die Erzeugung von Daten[46] als Nebenprodukt einer anderen Wirtschaftstätigkeit. Es besteht jedoch nach wie vor Unsicherheit hinsichtlich der fälschlichen oder unbeabsichtigten Anwendung des Schutzrechts sui generis auf Datenbanken, die maschinengenerierte Daten enthalten, d. h. Daten, die durch die Nutzung von Produkten oder verbundenen Diensten gewonnen oder erzeugt werden. Vor dem Hintergrund der Datenwirtschaft, in der die Exklusivität von Daten als nicht rivales Gut in der Regel als Innovationshindernis angesehen wird, gilt es die politischen Ziele des Schutzes des geistigen Eigentums an solchen Datenbanken dagegen abzuwägen. Um die Kohärenz mit den in diesem Vorschlag vorgeschlagenen Regulierungsmaßnahmen zu gewährleisten, betrifft die Maßnahme zum Schutzrecht sui generis speziell die festgestellte problematische Anwendung dieses Schutzrechts im Zusammenhang mit dem Internet der Dinge. Die Kommission bereitet derzeit auch die Evaluierung der Verordnung (EU) 2018/1807 vor, die voraussichtlich im November 2022 vorgelegt wird. Erste Berichte externer Auftragnehmer haben gezeigt, dass die SWIPO-Verhaltenskodizes im Bereich des Wechsels zwischen Cloud-Diensten nur begrenzte Auswirkungen haben.

• Konsultation der Interessenträger

Während der Amtszeit der vorherigen Kommission wurden umfassende Arbeiten eingeleitet, um zu ermitteln, welche Probleme die Union daran hindern, das Potenzial datengetriebener Innovationen in der Wirtschaft voll auszuschöpfen. Der Vorschlag baut auf früheren Konsultationsmaßnahmen auf, wie der öffentlichen Konsultation aus dem Jahr 2017 zur Unterstützung der Mitteilung der Kommission „Aufbau einer europäischen Datenwirtschaft“[47], der öffentlichen Konsultation aus dem Jahr 2017 zur Bewertung der Datenbankrichtlinie, der öffentlichen Konsultation aus dem Jahr 2018 zur Überarbeitung der

---

44 COM(2017) 9 final; SWD(2018) 146 final, Abschnitt 5.4.2; unterstützende Studie für eine Folgenabschätzung zur Überarbeitung der Datenbankrichtlinie.

45 COM(2017) 9 final, COM(2020) 66 final, COM(2020) 760 final.

46 Fixtures Marketing Ltd gegen Oy Veikkaus Ab (C-46/02, 9.11.2004), Fixtures Marketing Ltd gegen Svenska Spel Ab (C-338/02, 9.11.2004) British Horseracing Board Ltd gegen William Hill (C-203/02, 9.11.2004), Fixtures Marketing Ltd gegen OPAP (C-444/02, 9.11.2004).

47 COM(2017) 9 final.

Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors, der Konsultation des KMU-Panels aus dem Jahr 2018 zu Grundsätzen und Leitlinien für den Datenaustausch zwischen Unternehmen und der offenen Online-Konsultation der Kommission zur Datenstrategie[48] von Februar bis Mai 2020.

Am 28. Mai 2021 wurde auf dem Portal „Bessere Rechtsetzung“ eine Folgenabschätzung in der Anfangsphase veröffentlicht, zu der vier Wochen lang Rückmeldungen gegeben werden konnten. Auf dem Portal „Bessere Rechtsetzung“ gingen 91 Beiträge ein[49], hauptsächlich von Unternehmen.

Am 3. Juni 2021 wurde eine öffentliche Online-Konsultation zum Datengesetz veröffentlicht. Diese lief bis zum 3. September 2021. Die Konsultation enthielt entsprechende Abschnitte und Fragen zu den von der Initiative abgedeckten Themen. Mit dieser Konsultation, die sich an alle Arten von Interessenträgern richtete, sollte Feedback zu folgenden Themen eingeholt werden: Datenweitergabe, Datenzugang und Datennutzung in Beziehungen zwischen Unternehmen sowie zwischen Unternehmen und Behörden, Stärkung der Verbraucher und Datenübertragbarkeit, mögliche Rolle technischer Maßnahmen wie intelligenter Verträge, Möglichkeit für die Nutzer, zwischen Cloud-Diensten zu wechseln, Rechte des geistigen Eigentums (d. h. Schutz von Datenbanken) und Garantien für nicht personenbezogene Daten im internationalen Kontext. Nach eingehender Analyse der Antworten veröffentlichte die Kommission auf ihrer Website einen zusammenfassenden Bericht[50].

Insgesamt gingen 449 Beiträge aus 32 Ländern ein. Die größte Zahl von Beiträgen entfiel auf Unternehmen, darunter 122 Wirtschaftsverbände und 105 Unternehmen/Unternehmensverbände. Bei 100 Konsultationsteilnehmern handelte es sich um Behörden und bei 58 um Einzelpersonen. Durch die Antworten wurde insgesamt bestätigt, dass es eine ganze Reihe von Hindernissen für eine wirksame und effiziente gemeinsame Datennutzung in allen Arten von Datenbeziehungen gibt.

Obwohl die gemeinsame Nutzung von Daten zwischen Unternehmen gängige Praxis ist, nannten die Befragten, die dabei auf Schwierigkeiten gestoßen waren, insbesondere technische Hindernisse (Formate, fehlende Standards – 69 %), die prinzipielle, nicht auf wettbewerbsrechtlichen Bedenken beruhende Verweigerung des Zugangs (55 %) oder den Missbrauch eines vertraglichen Ungleichgewichts (44 %). Was Vertragsfragen betrifft, befürwortete fast die Hälfte der Befragten die Einführung einer Missbräuchlichkeitsprüfung (46 %), während 21 % dagegen waren. Die Unterstützung für eine Missbräuchlichkeitsprüfung war bei KMU besonders hoch (50 %), aber auch eine beträchtliche Zahl großer Unternehmen sprach sich dafür aus (41 %). 46 % der Interessenträger in allen Sektoren befürworteten allgemeine Zugangsregeln auf der Grundlage fairer, angemessener und nichtdiskriminierender Bedingungen (46 %). 60 % der Befragten, insbesondere KMU und Kleinstunternehmen (78 %), stimmten zu, dass Mustervertragsbedingungen zu einer verstärkten gemeinsamen Datennutzung beitragen könnten. 70 % der Interessenträger vertraten die Auffassung, dass es bei Daten, die im Zusammenhang mit dem Internet der Dinge erzeugt werden, ein Fairnessproblem gibt und dass es den Herstellern vernetzter Produkte und verbundener Dienste nicht möglich sein sollte, einseitig darüber zu entscheiden, was mit den durch solche Produkte erzeugten Daten

[48] Europäische Kommission (2020). *Ergebnisse der Online-Konsultation zur Europäischen Datenstrategie.*

[49] *Website* der Europäischen Kommission: *Ihre Meinung zählt – Datengesetz und geänderte Vorschriften über den rechtlichen Schutz von Datenbanken.*

[50] Europäische Kommission (2021). *Öffentliche Konsultation zum Datengesetz: zusammenfassender Bericht*.

geschieht. 79 % der Befragten waren der Ansicht, dass intelligente Verträge ein wirksames Instrument sein könnten, um die technische Umsetzung des Datenzugangs und der Datennutzung bei im Internet der Dinge gemeinsam erzeugten Daten zu regeln.

Rechtsunsicherheit und rechtliche Hindernisse, kommerzielle Negativanreize und das Fehlen einer angemessenen Infrastruktur wurden von den Befragten am häufigsten als Faktoren genannt, die die gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden verhinderten. Fast alle Behörden sind der Ansicht, dass (auf Ebene der Union oder der Mitgliedstaaten) Maßnahmen für die gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden ergriffen werden müssen, bei Hochschulen/Forschungseinrichtungen sind es 80 % und bei Unternehmen/Unternehmensverbänden/Wirtschaftsverbänden 38 %. Eine klare Mehrheit der Interessenträger (insbesondere Bürgerinnen und Bürger und öffentliche Verwaltungen) vertrat auch die Auffassung, dass die gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden obligatorisch sein sollte, wobei es eindeutige Schutzvorkehrungen für spezifische Anwendungsfälle mit einem klaren öffentlichen Interesse in Notfällen und für das Krisenmanagement, für amtliche Statistiken, für den Umweltschutz und für eine gesündere Gesellschaft im Allgemeinen geben sollte.

Die Befragten bestätigten auch, dass es für gewerbliche Nutzer von Cloud-Computing-Diensten hilfreich wäre, ein Recht auf einen Wechsel des Dienstes zu haben. Was Schutzvorkehrungen für nicht personenbezogene Daten im internationalen Umfeld betrifft, so sehen 76 % der Befragten den auf der Grundlage ausländischer Rechtsvorschriften erfolgenden möglichen Zugang ausländischer Behörden zu Daten als Risiko für ihre Organisation an, wobei 19 % dieses Risiko für erheblich halten.

- **Einholung und Nutzung von Expertenwissen**

Der Vorschlag stützt sich auch auf mehrere Studien, Workshops und andere Expertenbeiträge:

– **Unterstützende Studie für die Folgenabschätzung zur Ausweitung der Datennutzung in Europa**, einschließlich Interviews mit ausgewählten Interessenträgern. In diesem Zusammenhang wurden auch zwei sektorübergreifende Workshops zur gemeinsamen Nutzung von Daten zwischen Unternehmen sowie zwischen Unternehmen und Behörden und ein abschließender Validierungsworkshop im Frühjahr 2021 abgehalten.

– **Studie zu Mustervertragsbedingungen, zur Kontrolle der Fairness bei der gemeinsamen Datennutzung und in Cloud-Verträgen sowie zu Datenzugangsrechten**, mit der insbesondere Aspekte der Fairness bei der gemeinsamen Datennutzung zwischen Unternehmen bewertet wurden und die auch gezielte Interviews mit Interessenträgern und einen Validierungsworkshop umfasste.

– **Studie über die wirtschaftlichen Nachteile unfairer und unausgewogener Verträge beim Cloud-Computing**. Dazu gehörte eine Online-Umfrage bei einer Stichprobe von KMU und Start-up-Unternehmen, die Cloud-Computing für ihre Geschäftstätigkeit nutzen.

– **Studie über den Wechsel des Anbieters von Cloud-Diensten**, einschließlich eines sektorübergreifenden Workshops im zweiten Quartal 2017.

– **Unterstützende Studie zur Überarbeitung der Datenbankrichtlinie**, einschließlich Interviews mit ausgewählten Interessenträgern. Diese Studie half der Kommission bei der Vorbereitung der Folgenabschätzung zur Überarbeitung der Datenbankrichtlinie im Zusammenhang mit dem Datengesetz und bei der Verwirklichung der miteinander verwobenen Ziele dieser beiden Rechtsakte.

– **Methodische Unterstützung für die Folgenabschätzung zur Nutzung von in privatem Besitz befindlichen Daten in amtlichen Statistiken**. Dadurch soll Input für die Bewertung der Auswirkungen der Weiterverwendung von Daten zwischen Unternehmen und Behörden in amtlichen Statistiken gewonnen werden, indem ein methodischer Ansatz entwickelt und der Nutzen und die Kosten der Wiederverwendung von Daten und ausgewählter Anwendungsfälle für verschiedene statistische Bereiche und verschiedene Arten von Daten aus dem Privatsektor beschrieben werden. Darüber hinaus wird ein Beitrag zu laufenden Forschungsarbeiten und Beratungen geleistet, um zu einem besseren Verständnis der gemeinsamen Nutzung von Daten zwischen Unternehmen und Behörden zu gelangen.

– **Webinare zu Plattformen personenbezogener Daten und Plattformen für Industriedaten**. Es fanden drei Webinare statt, und zwar am 6., 7. und 8. Mai 2020. Dabei kamen die einschlägigen Datenplattformprojekte im Portfolio der öffentlich-privaten Partnerschaft zum Wert von Big Data zusammen.

– **Bericht der hochrangigen Expertengruppe zur gemeinsamen Nutzung von Daten zwischen Unternehmen und Behörden.** Der Bericht enthält eine Analyse der Probleme im Zusammenhang mit der gemeinsamen Nutzung von Daten zwischen Unternehmen und Behörden in der Union sowie eine Reihe von Empfehlungen, um eine skalierbare, verantwortungsvolle und nachhaltige gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden im öffentlichen Interesse zu gewährleisten. Neben der Empfehlung an die Kommission, die Option eines Rechtsrahmens in diesem Bereich zu prüfen, werden verschiedene Möglichkeiten vorgestellt, um private Unternehmen zur Weitergabe ihrer Daten zu bewegen. Dazu gehören monetäre wie auch nicht monetäre Anreize, z. B. steuerliche Anreize, Investitionen öffentlicher Mittel zur Unterstützung der Entwicklung von vertrauenswürdigen technischen Instrumenten und Regelungen zur Anerkennung der gemeinsamen Datennutzung.

– **Workshop zur Kennzeichnung/Zertifizierung von Anbietern technischer Lösungen für die gemeinsame Datennutzung**. An diesem Webinar nahmen am 12. Mai 2020 rund 100 Vertreter von Unternehmen (einschließlich KMU), europäischen Institutionen und Hochschulen teil. Ziel war es zu prüfen, ob durch ein Kennzeichnungs- oder Zertifizierungssystem, das das Vertrauen in das Datenökosystem erhöht, die Geschäftstätigkeit von Datenmittlern ausgebaut werden könnte.

– **Durchführung von zehn Workshops zwischen Juli und November 2019 mit mehr als 300 Interessenträgern aus verschiedenen Sektoren**. Bei den Workshops wurde darüber diskutiert, wie die **gemeinsame Datennutzung in bestimmten Bereichen** wie Umwelt, Landwirtschaft, Energie oder Gesundheitswesen der Gesellschaft als Ganzes zugutekommen könnte, indem öffentlichen Akteuren geholfen wird, bessere Strategien zu konzipieren und öffentliche Dienstleistungen zu verbessern, und private Akteure dabei unterstützt werden, Dienstleistungen zu erbringen, die zur Bewältigung gesellschaftlicher Herausforderungen beitragen.

– **Konsultation des KMU-Panels.** Bei dieser von Oktober 2018 bis Januar 2019 durchgeführten Panel-Konsultation wurden die Ansichten von KMU zu den Grundsätzen und Leitlinien der Kommission für die gemeinsame Datennutzung zwischen Unternehmen eingeholt, die in der Mitteilung „Aufbau eines gemeinsamen

europäischen Datenraums“ und in der Begleitunterlage der Kommissionsdienststellen vom 25. April 2018[51] veröffentlicht wurden.

– **Neueste Eurobarometer-Umfrage zu den Auswirkungen der Digitalisierung.** Diese allgemeine Umfrage zum Alltag der Europäerinnen und Europäer enthält Fragen zur Kontrolle über personenbezogene Informationen und deren Weitergabe durch die Menschen. Sie wurde am 5. März 2020 veröffentlicht und enthält Ergebnisse dazu, inwieweit – und unter welchen Bedingungen – die Bürgerinnen und Bürger in Europa bereit sind, ihre personenbezogenen Informationen weiterzugeben.

– **Stellungnahme des Europäischen Datenschutzbeauftragten** (EDSB) zur Europäischen Datenstrategie[52]. Am 16. Juni 2020 nahm der EDSB die Stellungnahme 3/2020 zur Europäischen Datenstrategie an. Er begrüßte die Strategie und sah in ihrer Umsetzung eine Gelegenheit, eine Vorbildfunktion für ein alternatives Modell der Datenwirtschaft zu übernehmen.

• **Folgenabschätzung**

Diesem Vorschlag liegt eine Folgenabschätzung bei[53], die dem Ausschuss für Regulierungskontrolle (RSB) am 29. September 2021 und am 13. Dezember 2021 vorgelegt wurde. Am 21. Januar 2022 gab der Ausschuss eine befürwortende Stellungnahme mit Vorbehalten ab.

• **Effizienz der Rechtsetzung und Vereinfachung**

Durch die Klarstellung, dass das Schutzrecht sui generis gemäß der Datenbankrichtlinie (Richtlinie 96/9/EG) nicht für Datenbanken mit Daten gilt, die durch die Nutzung von Produkten und verbundenen Diensten erzeugt oder gewonnen wurden, stellt der Vorschlag sicher, dass dieses Schutzrecht nicht in die in dieser Verordnung vorgesehenen Rechte von Unternehmen und Verbrauchern auf Zugang zu sowie Nutzung und Weitergabe von Daten eingreift. Mit dieser Klarstellung wird die Anwendung des Schutzrechts sui generis mit dem Ziel des Legislativvorschlags in Einklang gebracht, was sich positiv auf die einheitliche Anwendung der Vorschriften im Binnenmarkt und auf die Datenwirtschaft auswirkt.

Durch das Datengesetz werden der Datenzugang und die Datennutzung erleichtert, wodurch Belastungen sowohl im öffentlichen Sektor als auch bei den Unternehmen verringert werden, was vor allem auf niedrigere Transaktionskosten und Effizienzgewinne zurückzuführen ist. Gemäß dem „One-in-one-out“-Ansatz[54], durch den für Bürgerinnen und Bürger sowie für Unternehmen die Belastungen durch die Auswirkungen und Kosten der Anwendung von Rechtsvorschriften so gering wie möglich gehalten werden sollen, steht der voraussichtliche Netto-Verwaltungsaufwand für das Datengesetz entsprechend der Folgenabschätzung einem Nutzen gegenüber, der die damit verbundenen Verwaltungskosten wahrscheinlich nicht nur ausgleicht, sondern bei Weitem überwiegt.

• **Grundrechte**

Der Vorschlag steht im Einklang mit den Rechtsvorschriften der Union über den Schutz personenbezogener Daten und den Schutz der Privatsphäre in der Kommunikation und bei Endgeräten und sieht zusätzliche Schutzvorkehrungen im Zusammenhang mit dem Zugang zu personenbezogenen Daten sowie für Fälle vor, die Rechten des geistigen Eigentums

---

51 COM(2018) 232 final, SWD(2018) 125 final vom 25.4.2018.

52 Stellungnahme 3/2020 des EDSB zur Europäischen Datenstrategie.

53 **[Links zum endgültigen Dokument und zur Zusammenfassung einfügen.]**

54 SWD(2021) 305 final.

unterliegen.

Das bereits hohe Verbraucherschutzniveau wird in Kapitel II durch das neue Recht auf Zugang zu von Nutzern erzeugten Daten in Situationen gestärkt, die zuvor nicht durch Unionsrecht geregelt waren. Das Recht, rechtmäßig erworbenes Eigentum zu nutzen und darüber zu verfügen, wird durch das Recht auf Zugang zu Daten gestärkt, die durch die Nutzung eines Gegenstands im Internet der Dinge erzeugt wurden. Dadurch kommt der Eigentümer in den Genuss eines besseren Nutzererlebnisses und eines breiteren Spektrums von z. B. Reparatur- und Wartungsdiensten. Was den Verbraucherschutz betrifft, verdienen die Rechte von Kindern als schutzbedürftige Verbraucher besondere Aufmerksamkeit, und die Vorschriften des Datengesetzes werden für mehr Klarheit in Bezug auf den Datenzugang und die Datennutzung sorgen.

Das Recht Dritter, auf Verlangen des Nutzers Zugang zu Daten des Internets der Dinge zu gewähren, schränkt die unternehmerische Freiheit und die Vertragsfreiheit des Herstellers oder Entwicklers eines Produkts oder verbundenen Dienstes ein. Die Beschränkung ist gerechtfertigt, um den Verbraucherschutz zu verbessern und insbesondere die wirtschaftlichen Interessen der Verbraucherinnen und Verbraucher zu fördern. Der Hersteller oder Entwickler eines Produkts und verbundener Dienste hat in der Regel die ausschließliche Kontrolle über die Nutzung der Daten, die bei der Nutzung eines Produkts oder eines verbundenen Dienstes erzeugt werden, was zu „Lock-in"-Effekten beiträgt und Marktteilnehmern, die Anschlussdienste anbieten, den Markteintritt erschwert. Das Zugangsrecht für Daten des Internets der Dinge trägt dieser Situation Rechnung, indem es Verbraucherinnen und Verbrauchern, die Produkte und verbundene Dienste nutzen, stärker dazu befähigt, sinnvoll zu kontrollieren, wie die durch die Nutzung des Produkts und verbundenen Dienstes erzeugten Daten genutzt werden, und indem Innovationen durch mehr Marktteilnehmer ermöglicht werden. Den Verbraucherinnen und Verbrauchern steht damit eine größere Auswahl an Anschlussdiensten wie Reparatur und Wartung zur Verfügung und sie sind nicht mehr ausschließlich von den Diensten des Herstellers abhängig. Durch den Vorschlag können die Daten des Nutzers leichter auf Dritte übertragen werden, sodass ein wettbewerbsorientiertes Angebot von Anschlussdiensten entsteht und umfassendere datengestützte Innovationen sowie die Entwicklung von Produkten oder Diensten möglich werden, die mit den ursprünglich vom Nutzer erworbenen oder abonnierten Produkten oder Diensten nichts zu tun haben.

Die Einschränkung der Vertragsfreiheit und der unternehmerischen Freiheit des Herstellers oder Entwicklers ist verhältnismäßig und wird dadurch abgemildert, dass der Hersteller oder Entwickler die Daten weiterhin ebenfalls nutzen kann, sofern diese Nutzung im Einklang mit den geltenden Rechtsvorschriften und der Vereinbarung mit dem Nutzer steht. Darüber hinaus wird dem Hersteller oder Entwickler das Recht eingeräumt, eine Gegenleistung dafür zu verlangen, dass er Dritten Zugang gewährt. Dieses Zugangsrecht lässt die bestehenden Zugangs- und Übertragbarkeitsrechte für betroffene Personen gemäß der DSGVO unberührt. Zusätzliche Schutzvorkehrungen gewährleisten, dass der Dritte die Daten verhältnismäßig nutzt.

Das in Kapitel IV vorgesehene faire und wirksame System zum Schutz vor missbräuchlichen Vertragsklauseln bei der gemeinsamen Datennutzung wird dazu beitragen, dass Kleinstunternehmen sowie kleine und mittlere Unternehmen unternehmerisch tätig werden können. Diese Bestimmung schränkt die Vertragsfreiheit von Unternehmen im Anwendungsbereich nur in begrenztem Umfang ein, da sie lediglich für missbräuchliche Vertragsklauseln im Zusammenhang mit dem Datenzugang und der Datennutzung gilt, die einem Kleinstunternehmen, einem kleinen oder mittleren Unternehmen einseitig von einer

Vertragspartei auferlegt werden. Dies ist gerechtfertigt, da KMU in der Regel in einer schwächeren Verhandlungsposition sind und oft keine andere Wahl haben, als nicht verhandelbare Vertragsbedingungen zu akzeptieren. Die Vertragsfreiheit bleibt weitgehend unberührt, da nur unverhältnismäßige und missbräuchliche Klauseln für ungültig erklärt werden und der geschlossene Vertrag, soweit möglich, mit Ausnahme der missbräuchlichen Klauseln gültig bleibt. Darüber hinaus können die Parteien auch künftig bestimmte Vertragsklauseln[55] individuell aushandeln.

Aufgrund der Bestimmungen in Kapitel V über die gemeinsame Nutzung von Daten zwischen Unternehmen und Behörden wegen außergewöhnlicher Notwendigkeit können Behörden künftig leichter Maßnahmen zum Wohle der Allgemeinheit ergreifen und z. B. einem öffentlichen Notstand vorbeugen, auf einen solchen reagieren oder bei dessen Bewältigung unterstützen. Auch der Privatsektor dürfte von der Straffung der Verfahren für Datenanforderungen profitieren.

Durch die Bestimmungen in Kapitel VI über den Wechsel zwischen Anbietern von Datenverarbeitungsdiensten wird die Position von Geschäftskunden gestärkt und ihnen die Möglichkeit gegeben, den Anbieter zu wechseln. Die Einschränkung des Rechts auf unternehmerische Betätigung von Anbietern von Datenverarbeitungsdiensten ist gerechtfertigt, da die neuen Vorschriften zur Vermeidung von Lock-in-Effekten auf dem Cloud- und Edge-Markt beitragen und gewerblichen und privaten Nutzern von Datenverarbeitungsdiensten mehr Auswahl bieten.

Die in Kapitel X vorgesehene Änderung des Datenbankrechts sui generis der Datenbankrichtlinie schränkt den darin enthaltenen Schutz des geistigen Eigentums nicht ein. Sie führt vielmehr zu mehr Rechtssicherheit in Fällen, in denen das Schutzrecht sui generis zuvor unklar war.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Dieser Vorschlag hat keine Auswirkungen auf den Haushalt.

5. WEITERE ANGABEN

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

Auf sektoraler und makroökonomischer Ebene wird die laufende Studie zur Beobachtung des Datenmarkts dazu beitragen, die wirtschaftlichen Auswirkungen des vorliegenden Vorschlags auf das Wachstum des Datenmarkts in der Union zu ermitteln.

Die Auswirkungen auf KMU, insbesondere deren Wahrnehmung von Problemen im Zusammenhang mit dem Datenzugang und der Datennutzung, werden fünf Jahre nach Annahme des Datengesetzes im Rahmen einer Konsultation des KMU-Panels bewertet.

Angesichts der zentralen Rolle der gemeinsamen europäischen Datenräume bei der Umsetzung der europäischen Datenstrategie werden viele der Auswirkungen dieser Initiative auf der Ebene der sektorspezifischen Datenräume überwacht und die vom Unterstützungszentrum für Datenräume gewonnenen Erkenntnisse im Rahmen des Programms „Digitales Europa“ finanziert werden. Die regelmäßige Interaktion zwischen den

[55] Weitere Erläuterungen zur Missbräuchlichkeitsprüfung und zum Grundsatz der Vertragsfreiheit siehe Anhang 11 der Folgenabschätzung.

Kommissionsdienststellen, dem Unterstützungszentrum und dem Europäischen Dateninnovationsrat (der nach Inkrafttreten des Daten-Governance-Gesetzes einzurichten ist) sollte eine zuverlässige Informationsquelle darstellen, auf deren Grundlage die Fortschritte bewertet werden können.

Schließlich wird vier Jahre nach der Annahme des Datengesetzes eine Evaluierung eingeleitet, um die Initiative zu bewerten und gegebenenfalls weitere Maßnahmen vorzubereiten.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

In Kapitel I werden der Gegenstand und der Anwendungsbereich der Verordnung und die Begriffsbestimmungen für den gesamten Rechtsakt festgelegt.

Durch Kapitel II wird die Rechtssicherheit für Verbraucherinnen und Verbraucher sowie Unternehmen beim Zugang zu Daten erhöht, die durch Produkte oder verbundene Dienste erzeugt werden, die sie besitzen, mieten oder leasen. Hersteller und Entwickler müssen ihre Produkte so gestalten, dass die Daten standardmäßig leicht zugänglich sind, und sie müssen offenlegen, welche Daten zugänglich sind und wie darauf zugegriffen werden kann. Die Bestimmungen dieses Kapitels berühren nicht die Möglichkeit der Hersteller, auf Daten aus von ihnen angebotenen Produkten oder verbundenen Diensten zuzugreifen und diese zu nutzen, sofern dies mit dem Nutzer vereinbart wurde. Der Dateninhaber ist verpflichtet, diese Daten auf Verlangen des Nutzers Dritten bereitzustellen. Die Nutzer sind berechtigt, dem Dateninhaber zu gestatten, Drittanbietern, wie z. B. Anbietern von Anschlussdiensten, Zugang zu den Daten zu gewähren. Kleinst- und Kleinunternehmen sind von diesen Pflichten ausgenommen.

Kapitel III enthält allgemeine Vorschriften für die Datenbereitstellungspflichten. Ist ein Dateninhaber verpflichtet, einem Datenempfänger Daten gemäß Kapitel II oder anderen Rechtsvorschriften der Union oder der Mitgliedstaaten bereitzustellen, so sind in dem allgemeinen Rahmen die Bedingungen für die Bereitstellung von Daten sowie die entsprechende Gegenleistung festgelegt. Alle Bedingungen müssen fair und nicht diskriminierend und alle Gegenleistungen angemessen sein und dürfen anderen Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts nicht entgegenstehen, die eine Gegenleistung ausschließen oder eine geringere Gegenleistung für die Bereitstellung von Daten vorsehen. Von KMU zu erbringende Gegenleistungen dürfen die Kosten für die Bereitstellung der Daten nicht übersteigen, es sei denn, die sektorspezifischen Rechtsvorschriften sehen etwas anderes vor. Von den Mitgliedstaaten zugelassene Streitbeilegungsstellen können Parteien unterstützen, die sich über die Gegenleistung oder andere Bedingungen nicht einig sind.

In Kapitel IV geht es um missbräuchliche Vertragsklauseln in Verträgen über die gemeinsame Datennutzung zwischen Unternehmen in Fällen, in denen eine Vertragspartei einem Kleinstunternehmen, kleinen oder mittleren Unternehmen einseitig eine Vertragsklausel auferlegt. Dieses Kapitel gewährleistet, dass bei vertraglichen Vereinbarungen über den Datenzugang und die Datennutzung ungleiche Verhandlungspositionen der Vertragsparteien nicht ausgenutzt werden. Das Instrument der Missbräuchlichkeitsprüfung umfasst eine allgemeine Bestimmung, in der die Missbräuchlichkeit einer Vertragsklausel im Zusammenhang mit der gemeinsamen Datennutzung definiert ist und die eine Liste von Klauseln enthält, die stets missbräuchlich sind oder als missbräuchlich gelten. In Fällen ungleicher Verhandlungspositionen schützt diese Prüfung die schwächere Vertragspartei, um missbräuchliche Verträge zu vermeiden. Im Falle eines solchen Missbrauchs dürfen die Daten

von keiner der beiden Vertragsparteien genutzt werden. Damit gewährleisten die Bestimmungen eine gerechtere Verteilung der Wertschöpfung in der Datenwirtschaft.[56] Von der Kommission empfohlene Mustervertragsbedingungen können Geschäftspartnern dabei helfen, Verträge mit fairen Bedingungen zu schließen.

Mit Kapitel V wird ein harmonisierter Rahmen geschaffen, der die Nutzung von im Besitz von Unternehmen befindlichen Daten durch öffentliche Stellen sowie Organe, Einrichtungen und sonstige Stellen der Union in Situationen regelt, in denen eine außergewöhnliche Notwendigkeit für die verlangten Daten besteht Der Rahmen enthält eine Pflicht zur Bereitstellung von Daten und würde nur im Falle eines öffentlichen Notstands oder in Situationen gelten, in denen bei öffentlichen Stellen eine außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten besteht, diese Daten aber nicht rechtzeitig durch den Erlass neuer Rechtsvorschriften oder durch bestehende Berichtspflichten auf dem Markt erlangt werden können. Im Falle einer außergewöhnlichen Notwendigkeit zur Bewältigung öffentlicher Notstände, wie Notlagen im Bereich der öffentlichen Gesundheit, größere Naturkatastrophen oder vom Menschen verursachte Katastrophen, würden die Daten kostenlos bereitgestellt. In anderen Fällen, in denen eine außergewöhnliche Notwendigkeit besteht, einschließlich der Verhinderung eines öffentlichen Notstands oder Unterstützung bei der Erholung von einem solchen Notstand, sollte der Dateninhaber, der die Daten bereitstellt, Anspruch auf einen Ausgleich haben, der die Kosten für die Bereitstellung der betreffenden Daten zuzüglich einer angemessenen Marge umfasst. Um sicherzustellen, dass das Recht, Daten zu verlangen, nicht missbraucht wird und der öffentliche Sektor für ihre Nutzung rechenschaftspflichtig bleibt, müssen die Datenverlangen verhältnismäßig sein, das zu erreichende Ziel klar angeben und die Interessen des Unternehmens gewahrt werden, das die Daten bereitstellt. Die zuständigen Behörden würden für Transparenz und dafür sorgen, dass alle Datenverlangen öffentlich verfügbar sind. Sie würden auch alle daraus resultierenden Beschwerden bearbeiten.

Mit Kapitel VI werden rechtliche Mindestanforderungen vertraglicher, gewerblicher und technischer Art eingeführt, die Anbietern von Cloud-, Edge- und anderen Datenverarbeitungsdiensten auferlegt werden, um den Wechsel zwischen solchen Diensten zu ermöglichen. Mit dem Vorschlag wird insbesondere sichergestellt, dass für Kunden nach dem Wechsel zu einem anderen Diensteanbieter Funktionsäquivalenz (ein Mindestfunktionsumfang) des Dienstes gegeben ist. Der Vorschlag enthält eine Ausnahme im Falle technischer Undurchführbarkeit, wobei die diesbezügliche Beweislast jedoch beim Diensteanbieter liegt. Der Vorschlag schreibt keine spezifischen technischen Normen oder Schnittstellen vor. Allerdings wird vorgeschrieben, dass die Dienste mit europäischen Normen oder, soweit vorhanden, mit offenen technischen Interoperabilitätsspezifikationen kompatibel sein müssen.

In Kapitel VII geht es um den unrechtmäßigen Zugang Dritter zu nicht personenbezogenen Daten, die in der Union im Besitz von auf dem Unionsmarkt angebotenen Datenverarbeitungsdiensten sind. Der Vorschlag berührt nicht die Rechtsgrundlage für Verlangen auf den Zugang zu Daten, die sich im Besitz von EU-Bürgerinnen und -Bürgern oder -Unternehmen befinden, und lässt den Rechtsrahmen der Union für den Datenschutz und den Schutz der Privatsphäre unberührt. Er bietet spezifische Schutzvorkehrungen, indem Anbieter alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen ergreifen müssen, um einen solchen Zugang zu verhindern, wenn dieser im Widerspruch zu konkurrierenden Pflichten steht, wonach diese Daten nach dem Unionsrecht zu schützen sind,

[56] Weitere Erläuterungen zur Missbräuchlichkeitsprüfung, einschließlich ihrer praktischen Umsetzung, siehe Anhang 11 der Folgenabschätzung.

es sei denn, es sind strenge Bedingungen erfüllt. Die Verordnung steht mit den internationalen Verpflichtungen der Union in der WTO und gemäß bilateralen Handelsabkommen im Einklang.

Kapitel VIII enthält wesentliche Anforderungen an die Interoperabilität, die von Anbietern von Datenräumen und Datenverarbeitungsdiensten einzuhalten sind, sowie wesentliche Anforderungen an intelligente Verträge. Gemäß diesem Kapitel werden auch offene Interoperabilitätsspezifikationen und europäische Normen für die Interoperabilität von Datenverarbeitungsdiensten ermöglicht, um eine nahtlose Cloud-Umgebung mit mehreren Anbietern zu fördern.

Kapitel IX enthält den Umsetzungs- und Durchsetzungsrahmen in Zusammenarbeit mit den zuständigen Behörden in den einzelnen Mitgliedstaaten, einschließlich eines Beschwerdeverfahrens. Die Kommission empfiehlt freiwillige Mustervertragsbedingungen für den Datenzugang und die Datennutzung. Bei Verstößen gegen diese Verordnung werden Sanktionen verhängt.

Kapitel X enthält eine Bestimmung, wonach das spezifische Schutzrecht sui generis gemäß der Richtlinie 96/9/EG keine Anwendung auf Datenbanken findet, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden, insofern es der wirksamen Ausübung des Rechts der Nutzer auf Datenzugang und Datennutzung gemäß Artikel 4 dieser Verordnung oder des Rechts auf Weitergabe dieser Daten an Dritte gemäß Artikel 5 dieser Verordnung entgegensteht.

Gemäß Kapitel XI kann die Kommission delegierte Rechtsakte erlassen, um einen Mechanismus zur Überwachung der von den Anbietern von Datenverarbeitungsdiensten verlangten Wechselentgelte einzuführen, um die wesentlichen Anforderungen an die Interoperabilität weiter zu präzisieren und um die Fundstelle offener Interoperabilitätsspezifikationen und europäischer Normen für die Interoperabilität von Datenverarbeitungsdiensten zu veröffentlichen. Darin ist außerdem vorgesehen, dass Durchführungsrechtsakte im Ausschussverfahren erlassen werden, um die Annahme gemeinsamer Spezifikationen für die Interoperabilität und intelligente Verträge zu erleichtern, wenn es keine harmonisierten Normen gibt oder diese nicht ausreichen, um zu gewährleisten, dass die wesentlichen Anforderungen eingehalten werden. Mit dem Vorschlag wird auch das Verhältnis zu anderen Rechtsakten der Union klargestellt, in denen Rechte und Pflichten im Bereich der gemeinsamen Datennutzung geregelt sind.

2022/0047 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[57],

nach Stellungnahme des Ausschusses der Regionen[58],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) In den letzten Jahren haben datengetriebene Technologien transformative Wirkung auf alle Wirtschaftssektoren gehabt. Insbesondere die rasche Verbreitung von Produkten, die mit dem Internet der Dinge vernetzt sind, hat den Umfang und den potenziellen Wert von Daten für Verbraucher, Unternehmen und Gesellschaft erhöht. Hochwertige und interoperable Daten aus verschiedenen Bereichen steigern die Wettbewerbsfähigkeit und Innovation und sorgen für ein nachhaltiges Wirtschaftswachstum. Ein und derselbe Datensatz kann potenziell unbegrenzt für verschiedene Zwecke verwendet und weiterverwendet werden, ohne dass dadurch seine Qualität oder Quantität beeinträchtigt wird.

(2) Hindernisse bei der gemeinsamen Datennutzung verhindern jedoch eine optimale Verteilung der Daten zum Nutzen der Gesellschaft. Zu diesen Hindernissen gehören der Mangel an Anreizen für Dateninhaber, freiwillig Vereinbarungen über die gemeinsame Datennutzung einzugehen, Unsicherheiten in Bezug auf Rechte und Pflichten in Verbindung mit Daten, Kosten für die Beauftragung und Umsetzung technischer Schnittstellen, die starke Fragmentierung von Informationen in Datensilos, schlechte Verwaltung von Metadaten, fehlende Normen für die semantische und technische Interoperabilität, Engpässe beim Datenzugang, das Fehlen einheitlicher Verfahren für die gemeinsame Datennutzung und der Missbrauch vertraglicher Ungleichgewichte bei Datenzugang und Datennutzung.

(3) In Sektoren mit zahlreichen Kleinstunternehmen sowie kleinen und mittleren Unternehmen mangelt es häufig an digitalen Kapazitäten und Kompetenzen für die

[57] ABl. C … vom …, S. ….
[58] ABl. C … vom …, S. ….

Erhebung, Analyse und Nutzung von Daten, und der Zugang ist häufig eingeschränkt, wenn ein einziger Akteur im System im Besitz der Daten ist oder weil Daten oder Datendienste an sich bzw. über Grenzen hinweg nicht interoperabel sind.

(4) Um den Bedürfnissen der digitalen Wirtschaft gerecht zu werden und Hindernisse für einen gut funktionierenden Binnenmarkt für Daten zu beseitigen, muss ein harmonisierter Rahmen geschaffen werden, in dem festgelegt wird, wer – außer dem Hersteller oder einem anderen Dateninhaber – unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, auf die Daten zuzugreifen, die durch Produkte oder verbundene Dienste erzeugt werden. Dementsprechend sollten die Mitgliedstaaten in den Angelegenheiten, die in den Anwendungsbereich der vorliegenden Verordnung fallen, keine zusätzlichen nationalen Anforderungen annehmen oder aufrechterhalten, sofern in dieser Verordnung nicht ausdrücklich vorgesehen, da dies die direkte und einheitliche Anwendung dieser Verordnung beeinträchtigen würde.

(5) Mit dieser Verordnung wird sichergestellt, dass die Nutzer eines Produkts oder verbundenen Dienstes in der Union zeitnah auf die Daten zugreifen können, die bei der Nutzung dieses Produkts oder verbundenen Dienstes erzeugt werden, und dass diese Nutzer die Daten verwenden und auch an Dritte ihrer Wahl weitergeben können. Sie verpflichtet den Dateninhaber, die Daten unter bestimmten Umständen den Nutzern und den von ihnen benannten Dritten bereitzustellen. Sie sorgt ferner dafür, dass Dateninhaber den Datenempfängern in der Union Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und auf transparente Weise bereitstellen. Privatrechtliche Vorschriften sind im Gesamtrahmen der gemeinsamen Datennutzung von entscheidender Bedeutung. Daher werden mit dieser Verordnung die vertragsrechtlichen Vorschriften angepasst und die Ausnutzung vertraglicher Ungleichgewichte verhindert, die Kleinstunternehmen, kleinen und mittleren Unternehmen im Sinne der Empfehlung 2003/361/EG einen fairen Datenzugang und eine faire Datennutzung erschweren. Mit dieser Verordnung wird auch sichergestellt, dass die Dateninhaber den öffentlichen Stellen der Mitgliedstaaten und den Organen, Einrichtungen oder sonstigen Stellen der Union die Daten bereitstellen, die wegen außergewöhnlicher Notwendigkeit für die Wahrnehmung von Aufgaben im öffentlichen Interesse erforderlich sind. Darüber hinaus soll mit dieser Verordnung der Wechsel zwischen Datenverarbeitungsdiensten erleichtert und die Interoperabilität von Daten sowie von Mechanismen und Diensten für die gemeinsame Datennutzung in der Union verbessert werden. Diese Verordnung sollte nicht so ausgelegt werden, dass sie eine Rechtsgrundlage für den Dateninhaber anerkennt oder schafft, nach der er Daten besitzen, auf sie zugreifen oder sie verarbeiten darf, oder dass sie dem Dateninhaber ein neues Recht auf Nutzung von Daten verleiht, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden. Ausgangspunkt ist vielmehr die Kontrolle, über die der Dateninhaber tatsächlich oder rechtlich über Daten ausübt, die durch Produkte oder verbundene Dienste erzeugt werden.

(6) Die Datenerzeugung ist das Ergebnis der Handlungen mindestens zweier Akteure, nämlich des Entwicklers oder Herstellers eines Produkts und des Nutzers des Produkts. Es stellen sich Fragen der Fairness in der digitalen Wirtschaft, da die von solchen Produkten oder verbundenen Diensten erfassten Daten ein wichtiges Gut für Anschluss-, Neben- und sonstige Dienste sind. Um die wichtigen wirtschaftlichen Vorteile von Daten als nicht rivales Gut für Wirtschaft und Gesellschaft zu nutzen, ist ein allgemeiner Ansatz für die Zuweisung von Zugangs- und Nutzungsrechten für Daten der Gewährung ausschließlicher Zugangs- und Nutzungsrechte vorzuziehen.

(7) Das Grundrecht auf Schutz personenbezogener Daten wird insbesondere durch die Verordnung (EU) 2016/679 und die Verordnung (EU) 2018/1725 gewahrt. Die Richtlinie 2002/58/EG schützt darüber hinaus die Privatsphäre und die Vertraulichkeit der Kommunikation und enthält Bedingungen für die Speicherung personenbezogener und nicht personenbezogener Daten auf Endgeräten und den Zugang dazu. Diese Instrumente bilden die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung, auch wenn Datensätze eine Mischung aus personenbezogenen und nicht personenbezogenen Daten enthalten. Die vorliegende Verordnung ergänzt das Unionsrecht zum Datenschutz und zum Schutz der Privatsphäre, insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG, und lässt es unberührt. Keine Bestimmung dieser Verordnung sollte so angewandt oder ausgelegt werden, dass das Recht auf Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation geschwächt oder eingeschränkt wird.

(8) Die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sind von wesentlicher Bedeutung, wenn die Verarbeitung erhebliche Risiken für die Grundrechte des Einzelnen mit sich bringt. Unter Berücksichtigung des Stands der Technik sollten alle an der gemeinsamen Datennutzung Beteiligten auch im Anwendungsbereich dieser Verordnung technische und organisatorische Maßnahmen zum Schutz dieser Rechte ergreifen. Zu diesen Maßnahmen gehören nicht nur die Pseudonymisierung und Verschlüsselung, sondern auch der Einsatz zunehmend verfügbarer Technik, die es ermöglicht, Algorithmen direkt am Ort der Datenerzeugung einzusetzen und wertvolle Erkenntnisse zu gewinnen, ohne dass die Daten zwischen den Parteien übertragen bzw. die Rohdaten oder strukturierten Daten selbst unnötig kopiert werden.

(9) Die vorliegende Verordnung ergänzt das Unionsrecht zur Förderung der Interessen der Verbraucher und zur Gewährleistung eines hohen Verbraucherschutzniveaus, zum Schutz ihrer Gesundheit, Sicherheit und wirtschaftlichen Interessen, insbesondere die Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates[59], die Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates[60] und die Richtlinie 93/13/EWG des Europäischen Parlaments und des Rates[61], und lässt es unberührt.

(10) Diese Verordnung berührt nicht Rechtsvorschriften der Union über die Datenweitergabe, den Datenzugang und die Datennutzung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der

---

59 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken) (ABl. L 149 vom 11.6.2005, S. 22).

60 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates.

61 Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen. Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union.

Strafvollstreckung oder für Zoll- und Steuerzwecke, unabhängig davon, auf welcher Rechtsgrundlage diese nach dem Vertrag über die Arbeitsweise der Europäischen Union erlassen wurden. Zu diesen Rechtsakten gehören die Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, die [Vorschläge für elektronische Beweismittel [COM(2018) 225 und COM(2018) 226], sobald diese angenommen sind], [der Vorschlag für] eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG sowie die internationale Zusammenarbeit in diesem Bereich, insbesondere auf der Grundlage des Übereinkommens des Europarats von 2001 über Computerkriminalität („Budapester Übereinkommen“). Diese Verordnung berührt nicht die Zuständigkeiten der Mitgliedstaaten in Bezug auf Tätigkeiten in den Bereichen öffentliche Sicherheit, Verteidigung und nationale Sicherheit im Einklang mit dem Unionsrecht sowie Tätigkeiten des Zolls im Bereich des Risikomanagements und allgemein der Überprüfung der Einhaltung des Zollkodex durch die Wirtschaftsteilnehmer.

(11) Rechtsvorschriften der Union, in denen Anforderungen an die physische Konzeption und die Daten für Produkte, die in der Union in Verkehr gebracht werden sollen, festgelegt werden, sollten von dieser Verordnung unberührt bleiben.

(12) Diese Verordnung ergänzt das Unionsrecht zur Festlegung von Barrierefreiheitsanforderungen für bestimmte Produkte und Dienstleistungen, insbesondere die Richtlinie (EU) 2019/882[62], und lässt es unberührt.

(13) Diese Verordnung berührt nicht die Zuständigkeiten der Mitgliedstaaten in Bezug auf Tätigkeiten in den Bereichen öffentliche Sicherheit, Verteidigung und nationale Sicherheit im Einklang mit dem Unionsrecht sowie Tätigkeiten des Zolls im Bereich des Risikomanagements und allgemein der Überprüfung der Einhaltung des Zollkodex durch die Wirtschaftsteilnehmer.

(14) Physische Produkte, die mittels ihrer Komponenten Daten über ihre Leistung, Nutzung oder Umgebung erlangen, erzeugen oder sammeln und die diese Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln können (häufig als Internet der Dinge bezeichnet), sollten unter diese Verordnung fallen. Zu den elektronischen Kommunikationsdiensten gehören terrestrische Telefonnetze, Fernsehkabelnetze, Satellitennetze und Nahfeldkommunikationsnetze. Derartige Produkte können Fahrzeuge, Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsprodukte oder landwirtschaftliche und industrielle Maschinen umfassen. Die Daten stellen die digitalisierten Nutzerhandlungen und -vorgänge dar und sollten daher für den Nutzer zugänglich sein; gleichzeitig sollten aus diesen Daten abgeleitete oder gefolgerte Informationen, sofern sie rechtmäßig erlangt wurden, nicht in den Anwendungsbereich dieser Verordnung fallen. Solche Daten sind potenziell wertvoll für die Nutzer und unterstützen Innovationen und die Entwicklung digitaler und anderer Dienste zum Schutz der Umwelt, der Gesundheit und der Kreislaufwirtschaft, insbesondere indem sie die Wartung und Reparatur der betreffenden Produkte erleichtern.

(15) Dagegen sollten bestimmte Produkte, die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen oder diese – unter anderem für die Nutzung durch einen Online-Dienst – aufzuzeichnen und zu übertragen, nicht unter diese Verordnung

[62] Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019).

fallen. Zu diesen Produkten gehören beispielsweise Personalcomputer, Server, Tablets und Smartphones, Kameras, Webcams, Tonaufnahmesysteme und Textscanner. Sie erfordern einen menschlichen Beitrag, um verschiedene Arten von Inhalten wie Textdokumente, Tondateien, Videodateien, Spiele und digitale Karten zu erstellen.

(16) Es müssen Vorschriften für vernetzte Produkte festgelegt werden, in die ein Dienst so integriert oder die so mit ihm verbunden sind, dass das Produkt ohne ihn seine Funktionen nicht ausführen könnte. Derartige verbundene Dienste können Teil von Kauf-, Miet- oder Leasingverträgen sein, oder sie werden üblicherweise für Produkte der gleichen Art erbracht und können – in Anbetracht der Beschaffenheit des Produkts und unter Berücksichtigung öffentlicher Erklärungen, die im Vorfeld des Vertragsschlusses von dem Verkäufer oder im Auftrag des Verkäufers, Vermieters, Leasinggebers oder anderer Personen in vorhergehenden Gliedern der Vertragskette, einschließlich des Herstellers abgegeben wurden – vom Verbraucher vernünftigerweise erwartet werden. Diese verbundenen Dienste können selbst, unabhängig von den Datenerhebungsmöglichkeiten des Produkts, mit dem sie verbunden sind, Daten erzeugen, die für den Nutzer von Wert sind. Diese Verordnung sollte auch für verbundene Dienste gelten, die nicht vom Verkäufer, Vermieter oder Leasinggeber selbst, sondern im Rahmen des Kauf-, Miet- oder Leasingvertrags von einem Dritten erbracht werden. Bei Zweifeln, ob die Erbringung des Dienstes Teil des Kauf-, Miet- oder Leasingvertrags ist, sollte diese Verordnung Anwendung finden.

(17) Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, umfassen auch vom Nutzer absichtlich aufgezeichnete Daten. Zu diesen Daten gehören auch Daten, die als Nebenprodukt von Nutzeraktionen, wie z. B. Diagnosedaten, und ohne jegliche Nutzeraktion, z. B. wenn sich das Produkt im Bereitschaftszustand befindet, erzeugt werden sowie Daten, die aufgezeichnet werden, während das Produkt ausgeschaltet ist. Derartige Daten sollten auch solche in der Form und dem Format umfassen, in denen sie vom Produkt erzeugt werden, jedoch nicht Daten, die sich aus einem Softwareprozess ergeben, mit dem abgeleitete Daten aus solchen Daten berechnet werden, da ein solcher Softwareprozess Rechten des geistigen Eigentums unterliegen kann.

(18) Als Nutzer eines Produkts sollte die juristische oder natürliche Person, z. B. ein Unternehmen oder Verbraucher, verstanden werden, die das Produkt gekauft, gemietet oder geleast hat. Je nach dem Rechtstitel, unter dem er es nutzt, trägt ein solcher Nutzer die Risiken und genießt die Vorteile der Nutzung des vernetzten Produkts und sollte auch Zugang zu den von ihm erzeugten Daten haben. Der Nutzer sollte daher berechtigt sein, aus den von diesem Produkt und allen verbundenen Diensten erzeugten Daten Nutzen zu ziehen.

(19) In der Praxis sind nicht alle Daten, die durch Produkte oder verbundene Dienste erzeugt werden, für ihre Nutzer leicht zugänglich, und es gibt häufig nur begrenzte Möglichkeiten für die Übertragbarkeit von Daten, die durch mit dem Internet der Dinge vernetzte Produkte erzeugt werden. Die Nutzer sind daher nicht in der Lage, die Daten zu erlangen, die erforderlich sind, um Reparatur- und andere Dienste in Anspruch zu nehmen, und Unternehmen sind nicht in der Lage, innovative, effizientere und bequemere Dienste anzubieten. In vielen Sektoren können die Hersteller oftmals durch ihre Kontrolle über die technische Konzeption des Produkts oder verbundener Dienste bestimmen, welche Daten erzeugt werden und wie darauf zugegriffen werden kann, auch wenn sie keinen Rechtsanspruch auf die Daten haben. Daher muss sichergestellt werden, dass die Produkte so konzipiert und hergestellt

sowie damit verbundene Dienste so erbracht werden, dass die bei ihrer Nutzung erzeugten Daten für den Nutzer stets leicht zugänglich sind.

(20) Wenn mehrere Personen oder Einrichtungen Eigentümer eines Produkts oder Beteiligte eines Leasing- oder Mietvertrags sind und Zugang zu einem verbundenen Dienst haben, sollten angemessene Anstrengungen bei der Konzeption des Produkts oder verbundenen Dienstes oder der entsprechenden Schnittstelle unternommen werden, damit alle Personen Zugang zu den erzeugten Daten haben. Nutzer von Produkten, die Daten erzeugen, müssen in der Regel ein Nutzerkonto einrichten. Dies ermöglicht die Identifizierung des Nutzers durch den Hersteller sowie die Kommunikation zur Ausführung und Bearbeitung von Datenzugangsverlangen. Hersteller oder Entwickler eines Produkts, das in der Regel von mehreren Personen verwendet wird, sollten den erforderlichen Mechanismus einrichten, der getrennte Nutzerkonten für einzelne Personen oder gegebenenfalls den Zugriff mehrerer Personen auf dasselbe Nutzerkonto ermöglicht. Der Zugang sollte dem Nutzer mithilfe einfacher Verfahren gewährt werden, die eine automatische Ausführung ermöglichen und keine Prüfung oder Freigabe durch den Hersteller oder Dateninhaber erfordern. Dies bedeutet, dass Daten nur bereitgestellt werden sollten, wenn der Nutzer dies tatsächlich wünscht. Ist die automatische Ausführung des Datenzugangsverlangens, beispielsweise über ein Nutzerkonto oder die mit dem Produkt oder dem Dienst bereitgestellte mobile Anwendung nicht möglich, sollte der Hersteller den Nutzer darüber informieren, wie auf die Daten zugegriffen werden kann.

(21) Die Produkte können so konzipiert sein, dass bestimmte Daten direkt von einem Datenspeicher auf dem Gerät oder von einem entfernten Server, an den die Daten übermittelt werden, bereitgestellt werden. Der Zugang zu Datenspeichern auf dem Gerät kann über kabelgebundene oder drahtlose lokale Funknetze ermöglicht werden, die mit einem öffentlich zugänglichen elektronischen Kommunikationsdienst oder einem Mobilfunknetz verbunden sind. Bei dem Server kann es sich um die eigenen lokalen Serverkapazitäten des Herstellers oder um die eines Dritten oder eines Cloud-Diensteanbieters handeln, der als Dateninhaber fungiert. Er kann so ausgelegt sein, dass der Nutzer oder ein Dritter die Daten auf dem Produkt oder auf einer Rechnerinstanz des Herstellers verarbeiten kann.

(22) Virtuelle Assistenten spielen eine immer wichtigere Rolle bei der Digitalisierung des Verbraucherumfelds und dienen als benutzerfreundliche Schnittstelle für das Abspielen von Inhalten, den Abruf von Informationen oder die Aktivierung materieller Gegenstände, die mit dem Internet der Dinge verbunden sind. Virtuelle Assistenten können beispielsweise in einer Smart-Home-Umgebung als zentrales Zugangstor dienen und erhebliche Mengen relevanter Daten darüber erfassen, wie Nutzer mit Produkten interagieren, die mit dem Internet der Dinge verbunden sind, einschließlich solcher, die von Dritten hergestellt werden, und können die Nutzung der vom Hersteller bereitgestellten Schnittstellen wie Touchscreens oder Smartphone-Apps ersetzen. Der Nutzer möchte diese Daten möglicherweise Drittherstellern bereitstellen, um neuartige Smart-Home-Dienste zu ermöglichen. Solche virtuellen Assistenten sollten unter das in dieser Verordnung vorgesehene Datenzugangsrecht fallen, auch in Bezug auf Daten, die vor der Aktivierung des virtuellen Assistenten durch das Aktivierungswort aufgezeichnet wurden, und Daten, die erzeugt werden, wenn ein Nutzer über einen virtuellen Assistenten mit einem Produkt interagiert, der von einer anderen Stelle als dem Hersteller des Produkts bereitgestellt wird. Allerdings fallen nur die Daten, die aus der Interaktion zwischen dem Nutzer und dem Produkt über den virtuellen Assistenten stammen, in den Anwendungsbereich dieser Verordnung. Vom

virtuellen Assistenten erstellte Daten, die nicht mit der Verwendung eines Produkts zusammenhängen, sind nicht Gegenstand dieser Verordnung.

(23) Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder die Erbringung eines verbundenen Dienstes sollten dem Nutzer klare und ausreichende Informationen darüber bereitgestellt werden, wie auf die erzeugten Daten zugegriffen werden kann. Diese Pflicht sorgt für Transparenz in Bezug auf die erzeugten Daten und verbessert den einfachen Zugang für den Nutzer. Diese Informationspflicht berührt nicht die Pflicht des Datenverantwortlichen, der betroffenen Person Informationen gemäß den Artikeln 12, 13 und 14 der Verordnung (EU) 2016/679 zu übermitteln.

(24) Mit dieser Verordnung wird den Dateninhabern die Pflicht auferlegt, Daten unter bestimmten Umständen bereitzustellen. Soweit personenbezogene Daten verarbeitet werden, sollte der Dateninhaber auch ein Datenverantwortlicher im Sinne der Verordnung (EU) 2016/679 sein. Wenn Nutzer betroffene Personen sind, sollten die Dateninhaber verpflichtet sein, den Nutzern Zugang zu ihren Daten zu gewähren und die Daten vom Nutzer ausgewählten Dritten im Einklang mit dieser Verordnung bereitzustellen. Mit dieser Verordnung wird jedoch keine Rechtsgrundlage gemäß der Verordnung (EU) 2016/679 geschaffen, die es dem Dateninhaber ermöglicht, Dritten auf Verlangen eines Nutzers, der keine betroffene Person ist, Zugang zu personenbezogenen Daten zu gewähren oder diese bereitzustellen, und sollte nicht so verstanden werden, dass dem Dateninhaber ein neues Recht auf die Nutzung von Daten eingeräumt wird, die bei der eines Produkts oder verbundenen Dienstes erzeugt wurden. Dies gilt insbesondere dann, wenn der Hersteller der Dateninhaber ist. In diesem Fall sollte eine vertragliche Vereinbarung zwischen dem Hersteller und dem Nutzer die Grundlage für die Nutzung nicht personenbezogener Daten durch den Hersteller bilden. Diese Vereinbarung kann Teil des Kauf-, Miet- oder Leasingvertrags für das Produkt sein. Jede Vertragsbedingung in der Vereinbarung, nach der der Dateninhaber die vom Nutzer eines Produkts oder verbundenen Dienstes erzeugten Daten nutzen darf, sollte für den Nutzer transparent sein, auch in Bezug auf den Zweck, für den der Dateninhaber die Daten zu verwenden beabsichtigt. Diese Verordnung sollte Vertragsbedingungen nicht entgegenstehen, die dazu führen, dass die Nutzung der Daten oder bestimmter Kategorien von Daten durch den Dateninhaber ausgeschlossen oder eingeschränkt wird. Diese Verordnung sollte auch sektorspezifischen Regulierungsanforderungen nach Unionsrecht oder nach mit dem Unionsrecht im Einklang stehenden nationalen Rechtsvorschriften nicht entgegenstehen, die die Nutzung bestimmter Daten durch den Dateninhaber aus genau festgelegten Gründen der öffentlichen Ordnung ausschließen oder einschränken würden.

(25) In konzentrierten Sektoren, in denen die Endnutzer durch eine kleine Zahl von Herstellern versorgt werden, stehen den Nutzern nur begrenzte Möglichkeiten für den Austausch von Daten mit diesen Herstellern zur Verfügung. Unter solchen Umständen können vertragliche Vereinbarungen nicht ausreichen, um das Ziel der Stärkung der Handlungsfähigkeit der Nutzer zu erreichen. Die Daten verbleiben in der Regel unter der Kontrolle der Hersteller, was es den Nutzern erschwert, aus den Daten, die sie mit den von ihnen gekauften oder geleasten Geräten erzeugt haben, Wert zu schöpfen. Folglich ist das Potenzial für innovative kleinere Unternehmen, datengestützte Lösungen auf wettbewerbsfähige Weise anzubieten, und für eine vielfältige Datenwirtschaft in Europa begrenzt. Diese Verordnung sollte daher auf den jüngsten Entwicklungen in bestimmten Sektoren aufbauen, wie dem Verhaltenskodex für die

gemeinsame Nutzung von Agrardaten im Wege einer vertraglichen Vereinbarung. Sektorspezifische Rechtsvorschriften können vorgeschlagen werden, um sektorspezifischen Bedürfnissen und Zielen Rechnung zu tragen. Darüber hinaus sollte der Dateninhaber die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugten Daten nicht verwenden, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Nutzers zu erlangen, und auch nicht anderweitig verwenden, wenn dies die gewerbliche Position des Nutzers auf den Märkten, auf denen dieser tätig ist, untergraben könnte. Dies würde beispielsweise bedeuten, dass Wissen über die Gesamtleistung eines Unternehmens oder eines landwirtschaftlichen Betriebs in Vertragsverhandlungen mit dem Nutzer über den potenziellen Erwerb des Produkts oder landwirtschaftlicher Erzeugnisse des Nutzers zum seinem Nachteil eingesetzt würde oder dass solche Informationen z. B. in größere aggregierte Datenbanken über bestimmte Märkte (z. B. Datenbanken über Ernteerträge für die kommende Erntesaison) eingegeben würden, da sich eine solche Verwendung indirekt negativ auf den Nutzer auswirken könnte. Dem Nutzer sollte die für die Verwaltung der Berechtigungen erforderliche technische Schnittstelle zur Verfügung gestellt werden, vorzugsweise mit fein abgestimmten Berechtigungsoptionen (z. B. „Zugriff einmalig zulassen“ oder „Zugriff nur während der Nutzung der App oder des Dienstes zulassen“), einschließlich der Möglichkeit, Berechtigungen zu widerrufen.

(26) Bei Verträgen zwischen einem Dateninhaber und einem Verbraucher als Nutzer eines Produkts oder verbundenen Dienstes, das bzw. der Daten erzeugt, findet auf die Vertragsklauseln die Richtlinie 93/13/EWG Anwendung, damit ein Verbraucher keinen missbräuchlichen Vertragsklauseln unterliegt. Bei missbräuchlichen Vertragsklauseln, die einem Kleinstunternehmen bzw. einem kleinen oder mittleren Unternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG[63] einseitig auferlegt werden, sieht diese Verordnung vor, dass diese missbräuchlichen Klauseln für dieses Unternehmen unverbindlich sein sollten.

(27) Der Dateninhaber kann eine geeignete Nutzeridentifizierung verlangen, um die Berechtigung des Nutzers auf Zugang zu den Daten zu überprüfen. Im Falle personenbezogener Daten, die von einem Auftragsverarbeiter im Namen des Datenverantwortlichen verarbeitet werden, sollte der Dateninhaber sicherstellen, dass das Zugangsverlangen vom Auftragsverarbeiter empfangen und bearbeitet wird.

(28) Dem Nutzer sollte es freistehen, die Daten für jeden rechtmäßigen Zweck zu verwenden. Dazu gehören die Bereitstellung der Daten, die der Nutzer im Rahmen der Ausübung des Rechts nach dieser Verordnung erhalten hat, für einen Dritten, der einen anschließenden Dienst anbietet, der möglicherweise mit einem vom Dateninhaber bereitgestellten Dienst im Wettbewerb steht, oder die Anweisung hierzu an den Dateninhaber. Der Dateninhaber sollte sicherstellen, dass die dem Dritten bereitgestellten Daten so genau, vollständig, zuverlässig, relevant und aktuell sind wie die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugten Daten, auf die der Dateninhaber selbst zugreifen kann oder darf. Geschäftsgeheimnisse oder Rechte des geistigen Eigentums sollten bei der Verarbeitung der Daten gewahrt werden. Es ist wichtig, Anreize für Investitionen in Produkte mit Funktionen zu erhalten, die auf der Nutzung von Daten von Sensoren basieren, die in dieses Produkt eingebaut sind. Das Ziel dieser Verordnung sollte daher so verstanden werden, dass sie die Entwicklung neuer, innovativer Produkte oder verbundener Dienste fördert und Innovationen auf den Anschlussmärkten vorantreibt, aber auch die Entwicklung völlig neuartiger

[63] Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen.

Dienste unter Nutzung der Daten anregt, auch auf der Grundlage von Daten aus einer Vielzahl von Produkten oder verbundenen Diensten. Gleichzeitig soll damit verhindert werden, dass die Investitionsanreize für den Produkttyp, von dem die Daten erlangt werden, z. B. durch die Verwendung von Daten zur Entwicklung eines konkurrierenden Produkts, untergraben werden.

(29) Ein Dritter, dem Daten bereitgestellt werden, kann ein Unternehmen, eine Forschungseinrichtung oder eine gemeinnützige Organisation sein. Wenn der Dateninhaber dem Dritten die Daten breitstellt, sollte er seine Position nicht missbrauchen, um einen Wettbewerbsvorteil auf Märkten zu erlangen, auf denen der Dateninhaber und der Dritte möglicherweise in direktem Wettbewerb stehen. Der Dateninhaber sollte die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugten Daten daher nicht verwenden, um Einblicke in die wirtschaftliche Lage des Dritten, dessen Vermögenswerte und Produktionsmethoden zu erlangen, und auch nicht anderweitig verwenden, wenn dies die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte.

(30) Bei der Nutzung eines Produkts oder verbundenen Dienstes können, insbesondere wenn es sich bei dem Nutzer um eine natürliche Person handelt, Daten erzeugt werden, die sich auf eine identifizierte oder identifizierbare natürliche Person (die betroffene Person) beziehen. Die Verarbeitung solcher Daten unterliegt den Vorschriften der Verordnung (EU) 2016/679, auch wenn personenbezogene und nicht personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden sind[64]. Die betroffene Person kann der Nutzer oder eine andere natürliche Person sein. Zugang zu personenbezogenen Daten darf nur von einem Datenverantwortlichen oder einer betroffenen Person verlangt werden. Ein Nutzer, der die betroffene Person ist, ist unter bestimmten Umständen gemäß der Verordnung (EU) 2016/679 berechtigt, auf die ihn betreffenden personenbezogene Daten zuzugreifen; diese Rechte bleiben von der vorliegenden Verordnung unberührt. Nach der vorliegenden Verordnung hat der Nutzer, der eine natürliche Person ist, ferner das Recht auf Zugang zu allen durch das Produkt erzeugten personenbezogenen und nicht personenbezogenen Daten. Handelt es sich beim Nutzer nicht um die betroffene Person, sondern um ein Unternehmen, einschließlich eines Einzelunternehmers, und wird das Produkt nicht gemeinsam in einem Haushalt verwendet, so ist der Nutzer ein Datenverantwortlicher im Sinne der Verordnung (EU) 2016/679. Dementsprechend braucht ein Nutzer, der als Datenverantwortlicher Zugang zu personenbezogenen Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, verlangen will, für die Verarbeitung der Daten gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 eine Rechtsgrundlage, wie etwa die Einwilligung der betroffenen Person oder ein berechtigtes Interesse. Dieser Nutzer sollte sicherstellen, dass die betroffene Person angemessen über die festgelegten, eindeutigen und rechtmäßigen Zwecke der Verarbeitung dieser Daten und darüber informiert wird, wie die betroffene Person ihre Rechte wirksam ausüben kann. Handelt es sich bei dem Dateninhaber und dem Nutzer um gemeinsam Verantwortliche im Sinne des Artikels 26 der Verordnung (EU) 2016/679, so müssen sie in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Pflichten zur Einhaltung dieser Verordnung erfüllt. Es sollte davon ausgegangen werden, dass ein solcher Nutzer, sobald Daten bereitgestellt wurden, seinerseits Dateninhaber werden kann, wenn er die Kriterien dieser Verordnung erfüllt, und damit seinerseits den Pflichten zur Bereitstellung von Daten im Rahmen dieser Verordnung unterliegen kann.

64 ABl. L 303 vom 28.11.2018, S. 59.

(31) Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden, sollten Dritten nur auf Verlangen des Nutzers bereitgestellt werden. Die vorliegende Verordnung ergänzt daher das in Artikel 20 der Verordnung (EU) 2016/679 vorgesehene Recht. Der Artikel sieht vor, dass betroffene Personen berechtigt sind, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übertragen, wenn diese Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder eines Vertrags gemäß Artikel 6 Absatz 1 Buchstabe b verarbeitet werden. Betroffene Personen haben ebenfalls das Recht, zu erwirken, dass die personenbezogenen Daten von einem Verantwortlichen direkt an einen anderen Verantwortlichen übermittelt werden, jedoch nur sofern dies technisch machbar ist. In Artikel 20 wird präzisiert, dass dies Daten betrifft, die die betroffene Person bereitgestellt hat, ohne jedoch anzugeben, ob dies ein aktives Verhalten der betroffenen Person erfordert oder ob dies auch für Situationen gilt, in denen ein Produkt oder verbundener Dienst durch seine Konzeption passiv das Verhalten einer betroffenen Person oder andere Informationen in Bezug auf eine betroffene Person überwacht. Das Recht nach dieser Verordnung ergänzt das Recht, personenbezogene Daten gemäß Artikel 20 der Verordnung (EU) 2016/679 auf verschiedene Weise zu erhalten und zu übertragen. Es gewährt Nutzern das Recht auf Zugang und darauf, einem Dritten alle Daten bereitzustellen, die bei der Nutzung eines Produkts und verbundenen Dienstes erzeugt werden, unabhängig davon, ob es sich um personenbezogene Daten handelt, von der Unterscheidung zwischen aktiv bereitgestellten oder passiv aufgezeichneten Daten und von der Rechtsgrundlage für die Verarbeitung. Im Gegensatz zu den in Artikel 20 der Verordnung (EU) 2016/679 vorgesehenen technischen Verpflichtungen wird mit dieser Verordnung die technische Machbarkeit des Zugangs Dritter zu allen Arten von Daten, die in ihren Anwendungsbereich fallen – ob personenbezogen oder nicht personenbezogen –, vorgeschrieben und gewährleistet. Außerdem kann der Dateninhaber eine angemessene Gegenleistung für etwaige Kosten, die durch die Bereitstellung des direkten Zugangs zu den bei der Nutzung des Produkts durch den Nutzer erzeugten Daten entstehen, festlegen, die von Dritten, nicht aber vom Nutzer zu tragen ist. Wenn ein Dateninhaber und ein Dritter nicht in der Lage sind, Bedingungen für einen solchen direkten Zugang zu vereinbaren, sollte die betroffene Person in keiner Weise daran gehindert werden, die in der Verordnung (EU) 2016/679 vorgesehenen Rechte, einschließlich des Rechts auf Datenübertragbarkeit, durch Einlegung von Rechtsbehelfen gemäß der genannten Verordnung auszuüben. In diesem Zusammenhang gilt, dass im Einklang mit der Verordnung (EU) 2016/679 durch eine vertragliche Vereinbarung nicht die Verarbeitung besonderer Kategorien personenbezogener Daten durch den Dateninhaber oder den Dritten gestattet werden kann.

(32) Der Zugang zu Daten, die auf Endgeräten gespeichert sind und auf die darüber zugegriffen wird, unterliegt der Richtlinie 2002/58/EG und erfordert die Einwilligung des Teilnehmers oder Nutzers im Sinne der genannten Richtlinie, es sei denn, dies ist unbedingt für die Bereitstellung eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Teilnehmer ausdrücklich gewünscht wurde, (oder zum alleinigen Zweck der Übertragung einer Nachricht) erforderlich. Die Richtlinie 2002/58/EG (e-Datenschutzrichtlinie) (und die vorgeschlagene e-Datenschutzverordnung) schützen die Integrität der Endgeräte des Nutzers im Hinblick auf die Nutzung von Verarbeitungs- und Speicherfunktionen und die Sammlung von Informationen. Geräte

des Internets der Dinge gelten als Endgeräte, wenn sie direkt oder indirekt mit einem öffentlichen Kommunikationsnetz verbunden sind.

(33) Um die Ausnutzung der Nutzer zu verhindern, sollten Dritte, denen die Daten auf Verlangen des Nutzers bereitgestellt wurden, die Daten nur für die mit dem Nutzer vereinbarten Zwecke verarbeiten und sie nur dann an andere Dritte weitergeben, wenn dies für die Erbringung des vom Nutzer gewünschten Dienstes erforderlich ist.

(34) Im Einklang mit dem Grundsatz der Datenminimierung sollte der Dritte nur auf solche zusätzlichen Informationen zugreifen, die für die Erbringung des vom Nutzer gewünschten Dienstes erforderlich sind. Nachdem der Dritte Zugang zu den Daten erhalten hat, sollte er diese ausschließlich für die mit dem Nutzer vereinbarten Zwecke verarbeiten, ohne dass der Dateninhaber eingreift. Es sollte für den Nutzer genauso einfach sein, den Zugang Dritter zu den Daten zu verweigern oder zu beenden, wie es für ihn ist, den Zugang zu den Daten zu erlauben. Der Dritte sollte den Nutzer nicht in irgendeiner Weise zwingen, täuschen oder manipulieren, indem er – auch mittels einer digitalen Schnittstelle mit dem Nutzer – die Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten des Nutzers untergräbt oder beeinträchtigt. In diesem Zusammenhang sollten Dritte bei der Gestaltung ihrer digitalen Schnittstellen nicht auf sogenannte „Dark Patterns“ zurückgreifen. „Dark Patterns“ sind Gestaltungstechniken, die dazu dienen, die Verbraucher zu Entscheidungen, die negative Folgen für sie haben, zu verleiten oder sie zu täuschen. Diese manipulativen Techniken können eingesetzt werden, um Nutzer, insbesondere schutzbedürftige Verbraucher, zu unerwünschten Verhaltensweisen zu bewegen und zu täuschen, indem sie zu Entscheidungen über die Datenoffenlegung gedrängt werden, sowie um die Entscheidungsfindung der Nutzer des Dienstes unverhältnismäßig in einer Weise zu beeinflussen, die ihre Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten untergräbt und beeinträchtigt. Übliche und rechtmäßige Geschäftspraktiken, die mit dem Unionsrecht im Einklang stehen, als solche sollten nicht als „Dark Patterns“ angesehen werden. Dritte sollten ihren Pflichten nach dem einschlägigen Unionsrecht nachkommen, insbesondere den Anforderungen der Richtlinie 2005/29/EG, der Richtlinie 2011/83/EU, der Richtlinie 2000/31/EG und der Richtlinie 98/6/EG.

(35) Dritte sollten auch davon absehen, die Daten für das Profiling einer Person zu verwenden, es sei denn, diese Verarbeitungstätigkeiten sind unbedingt erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen. Die Anforderung, Daten zu löschen, wenn diese für den mit dem Nutzer vereinbarten Zweck nicht mehr erforderlich ist, ergänzt das Recht der betroffenen Person auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679. Wenn der Dritte ein Anbieter eines Datenvermittlungsdienstes im Sinne des [Daten-Governance-Gesetzes] ist, gelten die in der genannten Verordnung für die betroffene Person vorgesehenen Schutzvorkehrungen. Der Dritte kann die Daten für die Entwicklung eines neuen und innovativen Produkts oder verbundenen Dienstes, nicht aber für die Entwicklung eines konkurrierenden Produkts verwenden.

(36) Start-ups, kleine und mittlere Unternehmen und Unternehmen aus traditionellen Branchen mit weniger entwickelten digitalen Fähigkeiten haben Schwierigkeiten, Zugang zu einschlägigen Daten zu erlangen. Ziel dieser Verordnung ist es, diesen Stellen den Zugang zu Daten zu erleichtern und gleichzeitig sicherzustellen, dass die entsprechenden Pflichten so verhältnismäßig wie möglich gefasst werden, um eine Übervorteilung zu vermeiden. Durch die Anhäufung und Aggregation großer Datenmengen und die technologische Infrastruktur für ihre gewinnbringende Verwertung ist in der digitalen Wirtschaft gleichzeitig eine kleine Zahl sehr großer

Unternehmen mit beträchtlicher wirtschaftlicher Macht entstanden. Zu diesen Unternehmen gehören Unternehmen, die zentrale Plattformdienste erbringen und die ganze Plattformökosysteme in der digitalen Wirtschaft kontrollieren, sodass es bestehenden oder neuen Marktteilnehmern nicht möglich ist, ihnen ihre Position streitig zu machen oder mit ihnen in Wettbewerb zu treten. Die [Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte)] zielt darauf ab, diese Ineffizienzen und Ungleichgewichte zu beheben, indem die Kommission einen Anbieter als „Gatekeeper“ benennen kann und diesen benannten Gatekeepern eine Reihe von Pflichten auferlegt wird, darunter das Verbot, bestimmte Daten ohne Einwilligung zusammenzuführen, und die Pflicht, ein wirksames Recht auf Datenübertragbarkeit gemäß Artikel 20 der Verordnung (EU) 2016/679 zu gewährleisten. Im Einklang mit der [Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte)] und angesichts der einzigartigen Fähigkeit dieser Unternehmen, Daten zu erwerben, wäre es zur Erreichung des Ziels dieser Verordnung nicht erforderlich und somit in Bezug auf die entsprechenden Pflichten unterliegenden Dateninhaber unverhältnismäßig, solchen Gatekeeper-Unternehmen ein Datenzugangsrecht einzuräumen. Dies bedeutet, dass ein als Gatekeeper benanntes Unternehmen, das zentrale Plattformdienste erbringt, auf der Grundlage der Bestimmungen des Kapitels II dieser Verordnung keinen Zugang zu den Daten der Nutzer verlangen oder erhalten kann, die bei der Nutzung eines Produkts oder verbundenen Dienstes oder eines virtuellen Assistenten erzeugt werden. Ein Unternehmen, das zentrale Plattformdienste erbringt und das nach dem Gesetz über digitale Märkte als Gatekeeper benannt wurde, sollte dem Verständnis nach alle juristischen Personen einer Unternehmensgruppe umfassen, wenn eine der juristischen Personen einen zentralen Plattformdienst erbringt. Darüber hinaus dürfen Dritte, denen die Daten auf Verlangen des Nutzers bereitgestellt werden, die Daten keinem benannten Gatekeeper bereitstellen. Beispielsweise darf der Dritte keinen Gatekeeper mit der Erbringung des Dienstes beauftragen. Dies hindert Dritte jedoch nicht daran, Datenverarbeitungsdienste in Anspruch zu nehmen, die von einem benannten Gatekeeper angeboten werden. Dieser Ausschluss benannter Gatekeeper vom Anwendungsbereich des Zugangsrechts nach dieser Verordnung hindert diese Unternehmen nicht daran, Daten auf andere rechtmäßige Weise zu erlangen.

(37) Angesichts des derzeitigen Stands der Technik ist es übermäßig aufwendig, weitere Konzeptionspflichten für Produkte und verbundene Dienste aufzuerlegen, die von Kleinst- und Kleinunternehmen hergestellt oder konzipiert werden. Dies ist jedoch nicht der Fall, wenn ein Kleinst- oder Kleinunternehmen mit der Herstellung oder Konzeption eines Produkts beauftragt wird. In solchen Fällen ist das Unternehmen, das dem Kleinst- oder Kleinunternehmen den Auftrag erteilt hat, in der Lage, dem Auftragnehmer einen angemessenen Ausgleich zu verschaffen. Ein Kleinst- oder Kleinunternehmen kann jedoch als Dateninhaber den Anforderungen dieser Verordnung unterliegen, wenn es nicht der Hersteller des Produkts oder ein Erbringer verbundener Dienste ist.

(38) Diese Verordnung enthält allgemeine Zugangsvorschriften für alle Fälle, in denen ein Dateninhaber gesetzlich verpflichtet ist, einem Datenempfänger Daten bereitzustellen. Ein solcher Zugang sollte auf fairen, angemessenen, nichtdiskriminierenden und transparenten Bedingungen beruhen, um die Kohärenz der Verfahren für die gemeinsame Datennutzung im Binnenmarkt, auch sektorübergreifend, zu gewährleisten und eine faire gemeinsame Datennutzung auch in Bereichen zu unterstützen und zu fördern, in denen kein solches Datenzugangsrecht besteht. Diese allgemeinen Zugangsvorschriften gelten nicht für Datenbereitstellungspflichten gemäß

der Verordnung (EU) 2016/679. Die freiwillige gemeinsame Datennutzung bleibt von diesen Vorschriften unberührt.

(39) Auf der Grundlage des Grundsatzes der Vertragsfreiheit sollte es den Parteien freistehen, die genauen Bedingungen für die Bereitstellung von Daten in ihren Verträgen im Rahmen der allgemeinen Zugangsvorschriften für die Bereitstellung von Daten auszuhandeln.

(40) Um sicherzustellen, dass die Bedingungen für einen obligatorischen Datenzugang für beide Parteien fair sind, sollten die allgemeinen Vorschriften über Datenzugangsrechte auf die Vorschrift zur Vermeidung missbräuchlicher Vertragsklauseln Bezug nehmen.

(41) Zum Ausgleich des Mangels an Informationen über die Bedingungen verschiedener Verträge, der es dem Datenempfänger erschwert, zu beurteilen, ob die Bedingungen für die Bereitstellung der Daten nicht diskriminierend sind, sollte es Sache des Dateninhabers sein, nachzuweisen, dass eine Vertragsbedingung nicht diskriminierend ist. Es ist keine rechtswidrige Diskriminierung, wenn der Dateninhaber für die Bereitstellung von Daten unterschiedliche Vertragsbedingungen oder andere Gegenleistungen vorsieht, wenn diese Unterschiede aus objektiven Gründen gerechtfertigt sind. Diese Pflichten gelten unbeschadet der Verordnung (EU) 2016/679.

(42) Um Anreize für weitere Investitionen in die Erzeugung wertvoller Daten zu schaffen, einschließlich Investitionen in einschlägige technische Instrumente, enthält diese Verordnung den Grundsatz, dass der Dateninhaber eine angemessene Gegenleistung verlangen kann, wenn er rechtlich verpflichtet ist, dem Datenempfänger Daten bereitzustellen. Diese Bestimmungen sollten nicht als Bezahlung für die Daten selbst verstanden werden, sondern im Falle von Kleinstunternehmen, kleinen und mittleren Unternehmen als Ausgleich für die Kosten und Investitionen, die für die Bereitstellung der Daten erforderlich sind.

(43) In begründeten Fällen, einschließlich der Notwendigkeit, die Beteiligung der Verbraucher und den Wettbewerb zu gewährleisten oder Innovationen auf bestimmten Märkten zu fördern, können Rechtsvorschriften der Union oder nationale Rechtsvorschriften zur Umsetzung des Unionsrechts eine regulierte Gegenleistung für die Bereitstellung bestimmter Arten von Daten vorschreiben.

(44) Um Kleinstunternehmen sowie kleine und mittlere Unternehmen vor übermäßigen wirtschaftlichen Belastungen zu schützen, die es ihnen wirtschaftlich zu schwer machen, innovative Geschäftsmodelle zu entwickeln und zu betreiben, sollte die von ihnen zu tragende Gegenleistung für die Bereitstellung von Daten die unmittelbaren Kosten der Bereitstellung der Daten nicht übersteigen und nicht diskriminierend sein.

(45) Unmittelbare Kosten für die Bereitstellung von Daten sind die Kosten, die für die Reproduktion, die elektronische Verbreitung und Speicherung von Daten erforderlich sind, nicht aber die Kosten der Datensammlung oder -produktion. Unmittelbare Kosten für die Bereitstellung von Daten sollten auf den Anteil begrenzt werden, der den einzelnen Datenzugangsverlangen zuzurechnen ist, wobei zu berücksichtigen ist, dass der Dateninhaber die erforderlichen technischen Schnittstellen oder die erforderliche Software und Netzanbindung dauerhaft einrichten muss. Langfristige Vereinbarungen zwischen Dateninhabern und Datenempfängern, z. B. über ein Abonnementmodell, könnten die Kosten im Zusammenhang mit der Bereitstellung der Daten im Rahmen regelmäßiger oder wiederholter Transaktionen in einer Geschäftsbeziehung senken.

(46) Ein Eingreifen ist nicht erforderlich, wenn Daten zwischen großen Unternehmen ausgetauscht werden oder wenn es sich beim Dateninhaber um ein kleines oder mittleres Unternehmen und beim Datenempfänger um ein großes Unternehmen handelt. In solchen Fällen wird davon ausgegangen, dass die Unternehmen in der Lage sind, eine Gegenleistung auszuhandeln, wenn dies angemessen ist, wobei Faktoren wie Menge, Format, Art, Angebot und Nachfrage sowie die Kosten für die Sammlung und Bereitstellung der Daten für den Datenempfänger zu berücksichtigen sind.

(47) Transparenz ist ein wichtiger Grundsatz, um sicherzustellen, dass die vom Dateninhaber verlangte Gegenleistung angemessen ist oder, falls es sich bei dem Datenempfänger um ein Kleinstunternehmen, ein kleines oder mittleres Unternehmen handelt, dass die Gegenleistung die Kosten, die unmittelbar mit der Bereitstellung der Daten für den Datenempfänger zusammenhängen und dem einzelnen Verlangen zuzurechnen sind, nicht übersteigt. Damit der Datenempfänger beurteilen und überprüfen kann, ob die Gegenleistung den Anforderungen dieser Verordnung entspricht, sollte der Dateninhaber dem Datenempfänger ausreichend detaillierte Informationen für die Berechnung der Gegenleistung zur Verfügung stellen.

(48) Alternative Möglichkeiten zur Beilegung innerstaatlicher und grenzüberschreitender Streitigkeiten im Zusammenhang mit der Bereitstellung von Daten sollten Dateninhabern und Datenempfängern gleichermaßen zur Verfügung stehen, sodass das Vertrauen in die gemeinsame Datennutzung gestärkt wird. In Fällen, in denen sich die Parteien nicht auf faire, angemessene und nichtdiskriminierende Bedingungen für die Bereitstellung von Daten einigen können, sollten die Streitbeilegungsstellen den Parteien eine einfache, schnelle und kostengünstige Lösung anbieten.

(49) Um zu vermeiden, dass zwei oder mehr Streitbeilegungsstellen für dieselbe Streitigkeit, insbesondere in grenzüberschreitenden Fällen, angerufen werden, sollte eine Streitbeilegungsstelle ein Ersuchen zur Streitbeilegung ablehnen können, das bereits bei einer anderen Streitbeilegungsstelle oder einem Gericht eines Mitgliedstaats eingereicht wurde.

(50) Die Parteien eines Streitbeilegungsverfahrens sollten nicht daran gehindert werden, ihre Grundrechte auf einen wirksamen Rechtsbehelf und ein faires Verfahren auszuüben. Daher sollte die Entscheidung, in einer Streitigkeit eine Streitbeilegungsstelle anzurufen, diesen Parteien nicht das Recht nehmen, bei einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen.

(51) Wenn sich eine Partei in einer stärkeren Verhandlungsposition befindet, besteht die Gefahr, dass sie diese Position bei Verhandlungen über den Zugang zu Daten zum Nachteil der anderen Vertragspartei ausnutzen und so den Zugang zu Daten wirtschaftlich weniger tragfähig und bisweilen untragbar machen könnte. Solche vertraglichen Ungleichgewichte schaden insbesondere Kleinstunternehmen sowie kleinen und mittleren Unternehmen, die nicht in der Lage sind, die Bedingungen für den Zugang zu Daten auszuhandeln, und die keine andere Wahl haben, als nicht verhandelbare Vertragsbedingungen zu akzeptieren. Daher sollten missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten für Kleinstunternehmen sowie kleine und mittlere Unternehmen nicht bindend sein, wenn sie ihnen einseitig auferlegt wurden.

(52) Bei den Vorschriften über Vertragsbedingungen sollte der Grundsatz der Vertragsfreiheit als wesentliches Konzept in den Geschäftsbeziehungen zwischen Unternehmen berücksichtigt werden. Daher sollten nicht alle Vertragsbedingungen

einer Missbräuchlichkeitsprüfung unterzogen werden, sondern nur die Klauseln, die Kleinstunternehmen sowie kleinen und mittleren Unternehmen einseitig auferlegt werden. Dies betrifft Situationen ohne Verhandlungsspielraum, in denen eine Partei eine bestimmte Vertragsklausel einbringt und das Kleinstunternehmen bzw. das kleine oder mittlere Unternehmen den Inhalt dieser Klausel trotz Verhandlungsversuchs nicht beeinflussen kann. Eine Vertragsklausel, die lediglich von einer Partei eingebracht und von dem Kleinstunternehmen bzw. dem kleinen oder mittleren Unternehmen akzeptiert wird, oder eine Klausel, die zwischen den Vertragsparteien ausgehandelt und anschließend in geänderter Weise vereinbart wird, sollte nicht als einseitig auferlegt gelten.

(53) Darüber hinaus sollten die Vorschriften über missbräuchliche Vertragsklauseln nur für diejenigen Bestandteile eines Vertrags gelten, die sich auf die Bereitstellung von Daten beziehen, d. h. Vertragsklauseln über den Datenzugang und die Datennutzung sowie die Haftung oder Rechtsbehelfe bei Verletzung und Beendigung datenbezogener Pflichten. Andere Teile desselben Vertrags, die nicht mit der Bereitstellung von Daten zusammenhängen, sollten nicht der in dieser Verordnung festgelegten Missbräuchlichkeitsprüfung unterliegen.

(54) Kriterien für die Ermittlung missbräuchlicher Vertragsklauseln sollten nur auf überzogene Vertragsbedingungen angewandt werden, bei denen eine stärkere Verhandlungsposition missbraucht wird. Die überwiegende Mehrheit der Vertragsbedingungen, die für eine Partei wirtschaftlich günstiger sind als für die andere, einschließlich derjenigen, die in Verträgen zwischen Unternehmen üblich sind, sind ein normaler Ausdruck des Grundsatzes der Vertragsfreiheit und gelten weiterhin.

(55) Ist eine Vertragsbedingung nicht in der Liste der Klauseln aufgeführt, die stets als missbräuchlich gelten oder bei denen davon ausgegangen wird, dass sie missbräuchlich sind, so findet die allgemeine Missbräuchlichkeitsbestimmung Anwendung. In diesem Zusammenhang sollten die als missbräuchlich aufgeführten Klauseln als Maßstab für die Auslegung der allgemeinen Missbräuchlichkeitsbestimmung dienen. Schließlich können von der Kommission erstellte und empfohlene Mustervertragsbedingungen für Verträge über die gemeinsame Datennutzung zwischen Unternehmen für Wirtschaftsunternehmen auch bei der Aushandlung von Verträgen hilfreich sein.

(56) Im Falle außergewöhnlicher Notwendigkeit kann es erforderlich sein, dass öffentliche Stellen oder Organe, Einrichtungen und sonstige Stellen der Union Daten nutzen, die im Besitz eines Unternehmens sind, um auf öffentliche Notlagen oder andere Ausnahmesituationen zu reagieren. Forschungseinrichtungen und Forschungsförderungseinrichtungen könnten auch als öffentliche Stellen oder Einrichtungen des öffentlichen Rechts eingerichtet sein. Um die Belastung der Unternehmen zu begrenzen, sollten Kleinst- und Kleinunternehmen von der Pflicht befreit werden, öffentlichen Stellen und Organen, Einrichtungen und sonstigen Stellen der Union im Fall außergewöhnlicher Notwendigkeit Daten bereitzustellen.

(57) Bei öffentlichen Notständen wie Notlagen im Bereich der öffentlichen Gesundheit, Notlagen aufgrund von Umweltschäden und großen Naturkatastrophen, einschließlich solcher, die durch den Klimawandel verschärft werden, sowie von Menschen verursachten schweren Katastrophen, wie großen Cybersicherheitsvorfällen, wird das öffentliche Interesse an der Verwendung der Daten schwerer wiegen als das Interesse der Dateninhaber, frei über die Daten in ihrem Besitz zu verfügen. In einem solchen Fall sollten die Dateninhaber verpflichtet werden, die Daten öffentlichen Stellen oder

Organen, Einrichtungen oder sonstigen Stellen der Union auf deren Verlangen bereitzustellen. Das Vorliegen eines öffentlichen Notstands wird nach den jeweiligen Verfahren in den Mitgliedstaaten oder von einschlägigen internationalen Organisationen festgestellt.

(58) Eine außergewöhnliche Notwendigkeit kann auch entstehen, wenn eine öffentliche Stelle nachweisen kann, dass die Daten entweder zur Verhütung eines öffentlichen Notstands oder zur Unterstützung der Erholung nach einem öffentlichen Notstand unter Umständen erforderlich sind, die hinreichend eng mit dem betreffenden öffentlichen Notstand in Verbindung stehen. Ist die außergewöhnliche Notwendigkeit nicht dadurch gerechtfertigt, dass ein öffentlicher Notstand bewältigt oder verhindert oder die Erholung davon unterstützt werden muss, so sollte die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union nachweisen, dass sie mangels eines zeitnahen Zugangs zu den verlangten Daten und deren Nutzung daran gehindert wäre, eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse wirksam zu erfüllen. Eine solche außergewöhnliche Notwendigkeit kann auch in anderen Situationen auftreten, z. B. im Zusammenhang mit der rechtzeitigen Erstellung amtlicher Statistiken, wenn anderweitig keine Daten verfügbar sind oder wenn der Aufwand für die Auskunftgebenden in der Statistik erheblich verringert wird. Gleichzeitig sollte die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union, wenn es nicht um die Bewältigung oder Verhinderung eines öffentlichen Notstands oder die Unterstützung der Erholung davon geht, nachweisen, dass es keine alternativen Mittel gibt, um die verlangten Daten zu erlangen, und dass die Daten nicht rechtzeitig erlangt werden können, indem die erforderlichen Datenbereitstellungspflichten in neuen Rechtsvorschriften festgelegt werden.

(59) Diese Verordnung sollte weder für freiwillige Vereinbarungen über den Datenaustausch zwischen privaten und öffentlichen Stellen gelten noch ihnen vorgreifen. Die den Dateninhabern auferlegten Pflichten zur Bereitstellung von Daten, die nicht auf einer außergewöhnlichen Notwendigkeit beruhen, insbesondere wenn die Datengrundlage und die Dateninhaber bekannt sind und die Daten regelmäßig genutzt werden können, wie im Falle von Berichtspflichten und sich aus dem Binnenmarkt ergebenden Pflichten, sollten von dieser Verordnung nicht berührt werden. Datenzugangsanforderungen, die dazu dienen, die Einhaltung der geltenden Vorschriften zu überprüfen, sollten von dieser Verordnung ebenfalls nicht berührt werden, auch in Fällen, in denen öffentliche Stellen die Aufgabe der Überprüfung der Einhaltung der Vorschriften anderen als öffentlichen Stellen übertragen.

(60) Bei der Wahrnehmung ihrer Aufgaben in den Bereichen Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten, der Vollstreckung strafrechtlicher und verwaltungsrechtlicher Sanktionen sowie der Erhebung von Daten für Steuer- oder Zollzwecke sollten sich öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union auf ihre Befugnisse im Rahmen der sektorspezifischen Rechtsvorschriften stützen. Diese Verordnung berührt daher nicht die Instrumente für die Datenweitergabe, den Datenzugang und die Datenverwendung in diesen Bereichen.

(61) Ein verhältnismäßiger, begrenzter und vorhersehbarer Rahmen auf Unionsebene ist für die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen und Organe, Einrichtungen oder sonstige Stellen der Union im Fall außergewöhnlicher Notwendigkeit erforderlich, um sowohl Rechtssicherheit zu gewährleisten als auch den Verwaltungsaufwand für Unternehmen so gering wie möglich zu halten. Zu

diesem Zweck sollten Datenverlangen öffentlicher Stellen sowie von Organen, Einrichtungen und sonstigen Stellen der Union an Dateninhaber hinsichtlich ihres Umfangs und ihrer Granularität transparent und verhältnismäßig sein. Der Zweck des Verlangens und die beabsichtigte Nutzung der verlangten Daten sollten konkret und eindeutig erläutert werden, wobei der verlangenden Stelle eine angemessene Flexibilität bei der Wahrnehmung ihrer Aufgaben im öffentlichen Interesse einzuräumen ist. Das Verlangen sollte auch den berechtigten Interessen der Unternehmen, an die es gerichtet wird, Rechnung tragen. Der Aufwand für die Dateninhaber sollte so gering wie möglich gehalten werden, indem die verlangenden Stellen verpflichtet werden, den Einmaligkeitsgrundsatz einzuhalten, der verhindert, dass dieselben Daten mehrmals oder von mehreren öffentlichen Stellen oder Organen, Einrichtungen oder sonstigen Stellen der Union verlangt werden, wenn diese Daten zur Bewältigung eines öffentlichen Notstands benötigt werden. Zur Gewährleistung der Transparenz sollten Datenverlangen, die von öffentlichen Stellen und von Organen, Einrichtungen oder sonstigen Stellen der Union gestellt werden, unverzüglich von der die Daten verlangenden Stelle veröffentlicht werden, und es sollte sichergestellt werden, dass alle Verlangen, die durch einen öffentlichen Notstand gerechtfertigt sind, online öffentlich zugänglich sind.

(62) Mit der Datenbereitstellungspflicht soll sichergestellt werden, dass öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union über das erforderliche Wissen zur Bewältigung oder Verhinderung öffentlicher Notstände oder zur Erholung danach oder zur Aufrechterhaltung der Kapazitäten zur Erfüllung bestimmter, gesetzlich ausdrücklich vorgesehener Aufgaben verfügen. Bei den von diesen Stellen erlangten Daten kann es sich um Geschäftsgeheimnisse handeln. Daher sollte die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates[65] nicht für Daten gelten, die im Rahmen dieser Verordnung bereitgestellt werden, und diese sollten nicht als offene Daten betrachtet werden, die Dritten zur Weiterverwendung zur Verfügung stehen. Dies sollte jedoch die Anwendbarkeit der Richtlinie (EU) 2019/1024 auf die Weiterverwendung amtlicher Statistiken, für deren Erstellung gemäß dieser Verordnung erlangte Daten verwendet wurden, unberührt lassen, sofern sich die Weiterverwendung nicht auf die zugrunde liegenden Daten erstreckt. Darüber hinaus sollte dies die Möglichkeit der gemeinsamen Nutzung der Daten für Forschungszwecke oder für die Erstellung amtlicher Statistiken unberührt lassen, sofern die in dieser Verordnung festgelegten Bedingungen erfüllt sind. Öffentliche Stellen sollten auch Daten, die sie gemäß dieser Verordnung erlangt haben, mit anderen öffentlichen Stellen austauschen dürfen, um die außergewöhnliche Notwendigkeit auszuräumen, wegen der sie verlangt wurden.

(63) Dateninhaber sollten die Möglichkeit haben, je nach Art der in dem Verlangen geltend gemachten außergewöhnlichen Notwendigkeit innerhalb von 5 oder 15 Arbeitstagen entweder eine Änderung des Verlangens einer öffentlichen Stelle oder eines Organs, einer Einrichtung oder sonstigen Stelle der Union oder dessen Rücknahme zu beantragen. Bei einem Verlangen aufgrund eines öffentlichen Notstands sollte sich die Nichtbereitstellung der Daten begründen lassen, wenn nachgewiesen werden kann, dass das Verlangen einem zuvor von einer anderen öffentlichen Stelle oder einem anderen Organ, einer anderen Einrichtung oder sonstigen Stelle der Union zu demselben Zweck eingereichten Verlangen ähnlich oder gleich ist. Ein Dateninhaber,

[65] 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).

der das Verlangen ablehnt oder dessen Änderung beantragt, sollte der öffentlichen Stelle oder dem Organ, der Einrichtung oder sonstigen Stelle der Union, die/das das Verlangen eingereicht hat, die Begründung für die Ablehnung des Verlangens mitteilen. Sollten die Datenbankrechte sui generis gemäß der Richtlinie 96/6/EG des Europäischen Parlaments und des Rates[66] in Bezug auf die verlangten Datensätze Anwendung finden, so sollten die Dateninhaber ihre Rechte in einer Weise ausüben, die die öffentliche Stelle und die Organe, Einrichtungen oder sonstigen Stellen der Union nicht daran hindert, die Daten im Einklang mit dieser Verordnung zu erlangen oder weiterzugeben.

(64) Ist es unbedingt erforderlich, mit den Daten für eine öffentliche Stelle oder ein Organ, eine Einrichtung oder sonstige Stelle der Union auch personenbezogene Daten bereitzustellen, sollten die geltenden Vorschriften über den Schutz personenbezogener Daten eingehalten werden, und die Bereitstellung der Daten und ihre anschließende Nutzung sollten mit Schutzvorkehrungen für die Rechte und Interessen der von diesen Daten betroffenen Personen einhergehen. Die Stelle, die die Daten verlangt, sollte die strikte Notwendigkeit und die besonderen und begrenzten Zwecke der Verarbeitung nachweisen. Der Dateninhaber sollte angemessene Anstrengungen unternehmen, um die Daten zu anonymisieren, oder, wenn sich eine solche Anonymisierung als unmöglich erweist, vor der Bereitstellung der Daten technische Mittel wie Pseudonymisierung und Aggregation anwenden.

(65) Daten, die öffentlichen Stellen und Organen, Einrichtungen oder sonstigen Stellen der Union wegen außergewöhnlicher Notwendigkeit bereitgestellt werden, sollten nur für den Zweck verwendet werden, für den sie verlangt wurden, es sei denn, der Dateninhaber, der die Daten bereitgestellt hat, hat ausdrücklich zugestimmt, dass die Daten für andere Zwecke verwendet werden. Die Daten sollten vernichtet werden, sobald sie für den im Verlangen genannten Zweck nicht mehr erforderlich sind, sofern nichts anderes vereinbart wurde, und der Dateninhaber sollte davon in Kenntnis gesetzt werden.

(66) Bei der Weiterverwendung von Daten, die von Dateninhabern bereitgestellt werden, sollten öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union sowohl die geltenden Rechtsvorschriften als auch die vertraglichen Pflichten des Dateninhabers einhalten. Ist die Offenlegung von Geschäftsgeheimnissen des Dateninhabers gegenüber öffentlichen Stellen oder Organen, Einrichtungen oder sonstigen Stellen der Union unbedingt erforderlich, um den Zweck zu erfüllen, für den die Daten verlangt wurden, so sollte dem Dateninhaber die Vertraulichkeit dieser Informationen zugesichert werden.

(67) Wenn es um den Schutz eines bedeutenden öffentlichen Guts geht, wie etwa zur Bewältigung öffentliche Notstände, sollte von der öffentlichen Stelle oder dem Organ, der Einrichtung oder sonstigen Stelle der Union nicht erwartet werden, dass sie den Unternehmen für die erlangten Daten einen Ausgleich gewähren. Öffentliche Notstände sind seltene Ereignisse, und nicht alle derartigen Notstände erfordern die Nutzung von Daten, die im Besitz von Unternehmen sind. Es ist daher nicht wahrscheinlich, dass die Geschäftstätigkeit der Dateninhaber durch die Inanspruchnahme dieser Verordnung durch öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellern der Union beeinträchtigt wird. Da jedoch Fälle einer außergewöhnlichen Notwendigkeit, bei denen es sich nicht um die Bewältigung

[66] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken (ABl. L 77 vom 27.3.1996, S. 20).

eines öffentlichen Notstands handelt, häufiger auftreten könnten, darunter Fälle der Verhinderung eines öffentlichen Notstands oder der Erholung davon, sollten Dateninhaber in solchen Fällen Anspruch auf einen angemessenen Ausgleich haben, der die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, und eine angemessene Marge für die Bereitstellung der Daten für die öffentliche Stelle oder das Organ, die Einrichtung oder sonstige Stelle der Union nicht übersteigen sollte. Der Ausgleich sollte nicht als Bezahlung für die Daten selbst und nicht als obligatorisch verstanden werden.

(68) Die öffentliche Stelle oder das Organ, die Einrichtung oder sonstige Stelle der Union kann die Daten, die sie aufgrund des Verlangens erlangt hat, an andere Stellen oder Personen weitergeben, wenn dies zur Durchführung wissenschaftlicher oder analytischer Tätigkeiten erforderlich ist, die sie/es nicht selbst durchführen kann. Diese Daten können unter den gleichen Umständen auch für die Erstellung amtlicher Statistiken an die nationalen statistischen Ämter und Eurostat weitergegeben werden. Solche Forschungstätigkeiten sollten jedoch mit dem Zweck vereinbar sein, für den die Daten verlangt wurden, und der Dateninhaber sollte über die Weitergabe der von ihm bereitgestellten Daten informiert werden. Einzelpersonen, die Forschung betreiben, oder Forschungsorganisationen, an die diese Daten weitergegeben werden können, sollten entweder gemeinnützig sein oder in staatlich anerkanntem Auftrag im öffentlichen Interesse handeln. Für die Zwecke dieser Verordnung sollten Organisationen nicht als Forschungsorganisationen gelten, wenn solche Organisationen dem bestimmenden Einfluss gewerblicher Unternehmen unterliegen, die aufgrund der strukturellen Gegebenheiten Kontrolle ausüben können und dadurch einen bevorzugten Zugang zu den Forschungsergebnissen erhalten könnten.

(69) Die Fähigkeit der Kunden von Datenverarbeitungsdiensten, einschließlich Cloud- und Edge-Diensten, von einem Datenverarbeitungsdienst zu einem anderen zu wechseln, ist eine wesentliche Voraussetzung für einen vom Wettbewerb geprägten Markt mit geringeren Marktzutrittsschranken für neue Diensteanbieter.

(70) Mit der Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates werden Diensteanbieter angehalten, Verhaltensregeln für die Selbstregulierung zu entwickeln und umzusetzen, die bewährte Verfahren umfassen, unter anderem zur Erleichterung des Wechsels des Anbieters von Datenverarbeitungsdiensten und der Übertragung von Daten. Angesichts der begrenzten Wirksamkeit der daraufhin entwickelten Selbstregulierungsrahmen und des allgemeinen Fehlens offener Standards und Schnittstellen ist es erforderlich, eine Reihe von regulatorischen Mindestverpflichtungen für die Anbieter von Datenverarbeitungsdiensten festzulegen, um vertragliche, wirtschaftliche und technische Hindernisse für einen wirksamen Wechsel zwischen Datenverarbeitungsdiensten zu beseitigen.

(71) Datenverarbeitungsdienste sollten Dienste umfassen, die einen breiten Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer und verteilter Rechenressourcen auf Abruf ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige virtuelle oder physische Infrastrukturen, Betriebssysteme, Software, einschließlich Werkzeuge zur Entwicklung von Software, Speicher, Anwendungen und Dienste. Dass sich der Nutzer von Datenverarbeitungsdiensten selbst ohne Interaktion mit dem Diensteanbieter Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden. Der Begriff „breiter Fernzugang“ wird verwendet, um zu beschreiben, dass die Rechenkapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener

Thin- oder Thick-Client-Plattformen (von Webbrowsern bis hin zu mobilen Geräten und Arbeitsplatzrechnern) fördern. Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Datenverarbeitungsdienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool“ wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. Der Begriff „gemeinsam nutzbar“ wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird. Der Begriff „verteilt“ wird verwendet, um die Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und sich koordinieren. Der Begriff „hochgradig verteilt“ wird verwendet, um Datenverarbeitungsdienste zu beschreiben, bei denen Daten näher an dem Ort verarbeitet werden, an dem sie erzeugt oder gesammelt werden, z. B. in einem vernetzten Datenverarbeitungsgerät. Edge-Computing, eine Form dieser hochgradig verteilten Datenverarbeitung, dürfte neue Geschäftsmodelle und Cloud-Dienste hervorbringen, die von Anfang an offen und interoperabel sein sollten.

(72) Ziel dieser Verordnung ist es, den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, wozu alle Bedingungen und Maßnahmen gehören, damit ein Kunde in der Lage ist, einen Vertrag mit einem Datenverarbeitungsdienst zu kündigen, einen oder mehrere neue Verträge mit verschiedenen Anbietern von Datenverarbeitungsdiensten zu schließen, alle seine digitalen Vermögenswerte, einschließlich Daten, zu den betreffenden anderen Anbietern zu übertragen und deren Nutzung in der neuen Umgebung unter Aufrechterhaltung der Funktionsäquivalenz fortzusetzen. Digitale Vermögenswerte beziehen sich auf Elemente in digitalem Format, für die der Kunde das Nutzungsrecht hat, darunter Daten, Anwendungen, virtuelle Maschinen und andere Erscheinungsformen von Virtualisierungstechnik wie Container. Funktionsäquivalenz bedeutet die Aufrechterhaltung eines Mindestfunktionsumfangs eines Dienstes nach dem Wechsel und sollte als technisch machbar angesehen werden, wenn sowohl der vorherige Dienst als auch der übernehmende Dienst (teilweise oder vollständig) dieselbe Dienstart abdeckt. Auch Metadaten, die bei der Nutzung eines Dienstes durch den Kunden erzeugt werden, sollten nach den Bestimmungen dieser Verordnung zum Anbieterwechsel übertragbar sein.

(73) Wenn Anbieter von Datenverarbeitungsdiensten wiederum Kunden von Datenverarbeitungsdiensten sind, die von einem Dritten erbracht werden, werden sie selbst von einem wirksameren Wechsel profitieren, wobei sie gleichzeitig an die Pflichten nach dieser Verordnung in Bezug auf ihre eigenen Dienstangebote gebunden sind.

(74) Die Anbieter von Datenverarbeitungsdiensten sollten verpflichtet sein, jede erforderliche Hilfe und Unterstützung zu leisten, um den Wechselvorgang erfolgreich und wirksam zu gestalten, ohne dass diese Anbieter von Datenverarbeitungsdiensten neue Kategorien von Diensten innerhalb der IT-Infrastruktur verschiedener Anbieter von Datenverarbeitungsdiensten oder auf deren Grundlage entwickeln müssen, um die Funktionsäquivalenz in einer anderen Umgebung als ihren eigenen Systemen zu gewährleisten. Die Diensteanbieter sind jedoch verpflichtet, jede erforderliche Hilfe

und Unterstützung anzubieten, um den Wechselvorgang wirksam zu gestalten. Bestehende Rechte im Zusammenhang mit der Kündigung von Verträgen, einschließlich derjenigen, die mit der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates[67] eingeführt wurden, sollten davon unberührt bleiben.

(75) Um den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, sollten die Anbieter von Datenverarbeitungsdiensten die Verwendung von Instrumenten für die Umsetzung und/oder für die Einhaltung der Vorschriften in Erwägung ziehen, insbesondere derjenigen, die von der Kommission in Form eines Cloud-Regelwerks veröffentlicht wurden. Insbesondere Standardvertragsklauseln sind von Vorteil, um das Vertrauen in Datenverarbeitungsdienste zu stärken, ein ausgewogeneres Verhältnis zwischen Nutzern und Diensteanbietern zu schaffen und die Rechtssicherheit in Bezug auf die Bedingungen für den Wechsel zu anderen Datenverarbeitungsdiensten zu erhöhen. Vor diesem Hintergrund sollten Nutzer und Diensteanbieter die Verwendung von Standardvertragsklauseln in Erwägung ziehen, die von einschlägigen Gremien oder Sachverständigengruppen, die nach Unionsrecht eingerichtet wurden, ausgearbeitet wurden.

(76) Offene Interoperabilitätsspezifikationen und -normen, die gemäß Anhang II Nummern 3 und 4 der Verordnung (EU) Nr. 1025/2021 im Bereich der Interoperabilität und Übertragbarkeit entwickelt wurden, ermöglichen eine nahtlose Cloud-Umgebung mit mehreren Anbietern, was eine wesentliche Voraussetzung für offene Innovation in der europäischen Datenwirtschaft ist. Da nicht nachgewiesen wurde, dass technische Spezifikationen oder Normen, die eine wirksame Cloud-Interoperabilität auf den Ebenen der Verarbeitung von Daten auf Plattformen (*Platform-as-a-Service*, PaaS) oder in Anwendungen (*Software-as-a-Service*, SaaS) erleichtern, mit marktgesteuerten Verfahren festgelegt werden können, sollte die Kommission auf der Grundlage dieser Verordnung und im Einklang mit der Verordnung (EU) Nr. 1025/2012 europäische Normungsgremien mit der Entwicklung solcher Normen beauftragen können, insbesondere für Dienstarten, für die solche Normen noch nicht existieren. Darüber hinaus wird die Kommission die Marktteilnehmer anhalten, einschlägige offene Interoperabilitätsspezifikationen zu entwickeln. Die Kommission kann im Wege delegierter Rechtsakte durch einen Verweis in einem Zentralspeicher der Union für Normen für die Interoperabilität von Datenverarbeitungsdiensten die Verwendung europäischer Normen für die Interoperabilität oder offener Interoperabilitätsspezifikationen für bestimmte Dienstarten vorschreiben. Auf europäische Normen und offene Interoperabilitätsspezifikationen wird nur verwiesen, wenn sie den in dieser Verordnung festgelegten Kriterien entsprechen, die dieselbe Bedeutung haben wie die Anforderungen in Anhang II Nummern 3 und 4 der Verordnung (EU) Nr. 1025/2021 und die in der Norm ISO/IEC 19941:2017 definierten Interoperabilitätsaspekte.

(77) Drittländer können Gesetze, Verordnungen und sonstige Rechtsakte erlassen, die auf die unmittelbare Übertragung nicht personenbezogener Daten oder den unmittelbaren Zugang staatlicher Stellen zu solchen außerhalb ihrer Grenzen – auch in der Union – gespeicherten Daten abzielen. In Drittländern ergangene Gerichtsurteile oder Entscheidungen anderer Justiz- oder Verwaltungsbehörden, einschließlich Strafverfolgungsbehörden, mit denen eine solche Übertragung nicht

[67] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (ABl. L 136 vom 22.5.2019, S. 1).

personenbezogener Daten gefordert wird, sollten vollstreckbar sein, wenn sie sich auf eine internationale Vereinbarung, etwa ein Rechtshilfeabkommen, stützen, dass zwischen dem betreffenden Drittland und der Union oder einem Mitgliedstaat besteht. Mitunter kann es dazu kommen, dass die sich aus einem Gesetz eines Drittlands ergebende Verpflichtung zur Übertragung nicht personenbezogener Daten oder zur Gewährung des Zugangs zu diesen Daten mit der Verpflichtung zum Schutz dieser Daten nach Unionsrecht oder nationalem Recht kollidiert, insbesondere im Hinblick auf den Schutz der Grundrechte des Einzelnen, wie das Recht auf Sicherheit und das Recht auf einen wirksamen Rechtsbehelf, oder im Hinblick auf die grundlegenden Interessen eines Mitgliedstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung sowie auf den Schutz sensibler Geschäftsdaten, einschließlich des Schutzes des Geschäftsgeheimnisses, und Rechte des geistigen Eigentums, darunter auch vertragliche Vertraulichkeitspflichten nach einem solchen Gesetz. Besteht keine internationale Vereinbarung zur Regelung dieser Fragen sollte die Übertragung oder der Zugang nur erlaubt werden, wenn überprüft wurde, dass das Rechtssystem des betreffenden Drittlands die Begründung und Verhältnismäßigkeit sowie die hinreichende Bestimmtheit der gerichtlichen Anordnung oder Entscheidung vorschreibt und dem Adressaten die Möglichkeit einräumt, seinen begründeten Einwand dem zuständigen Gericht des Drittlands, das befugt ist, die einschlägigen rechtlichen Interessen des Bereitstellers der Daten gebührend zu berücksichtigen, zur Überprüfung vorzulegen. Nach Möglichkeit sollte der Anbieter von Datenverarbeitungsdiensten im Rahmen des Datenzugangsverlangens der Behörde des Drittlands den Kunden, dessen Daten verlangt werden, informieren können, um zu prüfen, ob ein solcher Zugang möglicherweise gegen Unionsvorschriften oder nationalen Vorschriften verstößt, wie etwa Vorschriften über den Schutz sensibler Geschäftsdaten, einschließlich des Schutzes des Geschäftsgeheimnisses, und Rechte des geistigen Eigentums, darunter auch vertragliche Vertraulichkeitspflichten.

(78) Um das Vertrauen in die Daten weiter zu stärken, ist es wichtig, dass Schutzvorkehrungen in Bezug auf die Unionsbürger, den öffentlichen Sektor und die Unternehmen so weit wie möglich umgesetzt werden, um die Kontrolle über ihre Daten zu gewährleisten. Darüber hinaus sollten die Rechtsvorschriften, Werte und Standards der Union u. a. in Bezug auf Sicherheit, Datenschutz und Privatsphäre sowie Verbraucherschutz gewahrt werden. Um einen unrechtmäßigen Zugang zu nicht personenbezogenen Daten zu verhindern, sollten Anbieter von Datenverarbeitungsdiensten, die diesem Instrument unterliegen, wie Cloud- und Edge-Dienste, alle zumutbaren Maßnahmen ergreifen, um den Zugang zu den Systemen zu verhindern, in denen nicht personenbezogene Daten gespeichert werden, gegebenenfalls auch durch die Verschlüsselung von Daten, häufige Audits, die überprüfte Einhaltung der einschlägigen Systeme für die Sicherheitszertifizierung und die Änderung der Unternehmenspolitik.

(79) Normung und semantische Interoperabilität sollten eine wichtige Rolle bei der Bereitstellung technischer Lösungen zur Gewährleistung der Interoperabilität spielen. Um die Bewertung der Konformität mit den geltenden Interoperabilitätsanforderungen zu erleichtern, sollte bei jenen Interoperabilitätslösungen, die den harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates oder Teilen davon entsprechen, von einer Konformitätsvermutung ausgegangen werden. Die Kommission sollte gemeinsame Spezifikationen in Bereichen annehmen, in denen es keine harmonisierten Normen gibt oder diese unzureichend sind, um die Interoperabilität in Bezug auf gemeinsame europäische Datenräume, Anwendungsprogrammierschnittstellen, Cloud-Wechsel sowie

intelligente Verträge weiter zu verbessern. Darüber hinaus könnten in den verschiedenen Sektoren auch gemeinsame Spezifikationen im Einklang mit den sektorspezifischen Rechtsvorschriften der Union oder der Mitgliedstaaten auf der Grundlage der besonderen Bedürfnisse dieser Sektoren angenommen werden. Weiterverwendbare Datenstrukturen und -modelle (in Form von Kernvokabularen), Ontologien, Metadaten-Anwendungsprofile, Referenzdaten in Form eines Kernvokabulars, Taxonomien, Codelisten, Befugnislisten und Lexika sollten ebenfalls Teil der technischen Spezifikationen für die semantische Interoperabilität sein. Darüber hinaus sollte die Kommission in die Lage versetzt werden, die Entwicklung harmonisierter Normen für die Interoperabilität von Datenverarbeitungsdiensten in Auftrag zu geben.

(80) Um die Interoperabilität intelligenter Verträge in Anwendungen für die gemeinsame Datennutzung zu fördern, müssen wesentliche Anforderungen an intelligente Verträge für Fachkräfte festgelegt werden, die intelligente Verträge für andere erstellen oder solche intelligenten Verträge in Anwendungen integrieren, die die Umsetzung von Vereinbarungen über die gemeinsame Nutzung von Daten unterstützen. Um die Bewertung der Konformität solcher intelligenter Verträge mit diesen wesentlichen Anforderungen zu erleichtern, sollte bei jenen intelligenten Verträgen, die den harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates oder Teilen davon entsprechen, von einer Konformitätsvermutung ausgegangen werden.

(81) Um die effiziente Durchführung dieser Verordnung zu gewährleisten, sollten die Mitgliedstaaten eine oder mehrere zuständige Behörden benennen. Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so sollte er auch eine koordinierende zuständige Behörde benennen. Die zuständigen Behörden sollten miteinander zusammenarbeiten. Die für die Überwachung der Einhaltung des Datenschutzes zuständigen Behörden und die nach sektorspezifischen Rechtsvorschriften benannten zuständigen Behörden sollten in ihren Zuständigkeitsbereichen für die Anwendung dieser Verordnung verantwortlich sein.

(82) Zur Durchsetzung ihrer Rechte gemäß dieser Verordnung sollten natürliche und juristische Personen das Recht haben, bei Verletzung ihrer Rechte aus dieser Verordnung durch Beschwerde bei den zuständigen Behörden Rechtsmittel einzulegen. Diese Behörden sollten zur Zusammenarbeit verpflichtet sein, damit die Beschwerde angemessen bearbeitet und gelöst wird. Um den Mechanismus des Netzwerks für die Zusammenarbeit im Verbraucherschutz zu nutzen und Verbandsklagen zu ermöglichen, werden mit dieser Verordnung die Anhänge der Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates[68] und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates[69] geändert.

(83) Die zuständigen Behörden der Mitgliedstaaten sollten sicherstellen, dass Verstöße gegen die in dieser Verordnung festgelegten Pflichten mit Sanktionen geahndet werden. Dabei sollten sie Art, Schwere, wiederholtes Auftreten und Dauer der Pflichtverletzung im Hinblick auf das betreffende öffentliche Interesse, Umfang und

[68] Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden und zur Aufhebung der Verordnung (EG) Nr. 2006/2004 (ABl. L 345 vom 27.12.2017, S. 1).

[69] Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409 vom 4.12.2020, S. 1).

Art der ausgeübten Tätigkeiten sowie die wirtschaftliche Leistungsfähigkeit des Rechtsverletzers berücksichtigen. Sie sollten berücksichtigen, ob der Rechtsverletzer seinen Pflichten aus dieser Verordnung systematisch oder wiederholt nicht nachkommt. Um Unternehmen bei der Ausarbeitung und Aushandlung von Verträgen zu unterstützen, sollte die Kommission unverbindliche Mustervertragsbedingungen für Verträge über die gemeinsame Datennutzung zwischen Unternehmen erstellen und empfehlen, erforderlichenfalls unter Berücksichtigung der Bedingungen in bestimmten Sektoren und der bestehenden Verfahren mit freiwilligen Mechanismen für die gemeinsame Datennutzung. Diese Mustervertragsbedingungen sollten in erster Linie ein praktisches Werkzeug sein, um insbesondere kleineren Unternehmen den Abschluss eines Vertrags zu erleichtern. Werden diese Mustervertragsbestimmungen umfassend und durchgehend verwendet, so sollten sie sich auch auf die Gestaltung von Verträgen über den Datenzugang und die Datennutzung positiv auswirken und somit insgesamt zu faireren Vertragsbeziehungen beim Datenzugang und bei der gemeinsamen Datennutzung führen.

(84) Um das Risiko auszuschließen, dass die Inhaber von Daten in Datenbanken, die durch physische Komponenten wie Sensoren eines vernetzten Produkts und verbundenen Dienstes gewonnen oder erzeugt wurden, das Schutzrecht sui generis gemäß Artikel 7 der Richtlinie 96/9/EG geltend machen, obwohl das Schutzrecht sui generis auf solche Datenbanken keine Anwendung findet, und dadurch die wirksame Ausübung des Rechts der Nutzer auf Datenzugang und Datennutzung sowie des Rechts auf die Weitergabe von Daten an Dritte gemäß dieser Verordnung behindern, sollte in dieser Verordnung klargestellt werden, dass das Schutzrecht sui generis nicht für solche Datenbanken gilt, da die Schutzanforderungen nicht erfüllt wären.

(85) Damit den technischen Aspekten von Datenverarbeitungsdiensten Rechnung getragen wird, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um einen Mechanismus zur Überwachung der von den Anbietern von Datenverarbeitungsdiensten auf dem Markt verlangten Wechselentgelte einzuführen, um die wesentlichen Anforderungen an Betreiber von Datenräumen und Anbieter von Datenverarbeitungsdiensten im Hinblick auf die Interoperabilität zu präzisieren und die Fundstellen offener Interoperabilitätsspezifikationen und europäischer Normen für die Interoperabilität von Datenverarbeitungsdiensten zu veröffentlichen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Experten, durchführt und dass diese Konsultationen mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[70] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(86) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse in Bezug auf die Ergänzung dieser Verordnung übertragen werden, damit sie gemeinsame Spezifikationen zur Sicherstellung der Interoperabilität gemeinsamer europäischer

[70] ABl. L 123 vom 12.5.2016, S. 1.

Datenräume und Vorschriften über die gemeinsame Datennutzung, den Wechsel zwischen Datenverarbeitungsdiensten, die Interoperabilität intelligenter Verträge sowie technische Mittel wie Anwendungsprogrammierschnittstellen zur Ermöglichung der Datenübertragung zwischen Parteien, auch kontinuierlich oder in Echtzeit, und über Kernvokabulare für die semantische Interoperabilität sowie gemeinsame Spezifikationen für intelligente Verträge festlegen kann. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[71] ausgeübt werden.

(87) Diese Verordnung sollte besondere Vorschriften in Rechtsakten der Union für die Datenweitergabe zwischen Unternehmen, zwischen Unternehmen und Verbrauchern sowie zwischen Unternehmen und öffentlichen Stellen, die vor dem Zeitpunkt der Annahme dieser Verordnung erlassen wurden, unberührt lassen. Zur Gewährleistung der Kohärenz und des reibungslosen Funktionierens des Binnenmarkts sollte die Kommission gegebenenfalls die Situation in Bezug auf das Verhältnis zwischen dieser Verordnung und den vor Erlass dieser Verordnung zur Regelung der gemeinsamen Datennutzung erlassenen Rechtsakten prüfen, um zu beurteilen, ob diese besonderen Bestimmungen an diese Verordnung angepasst werden müssen. Diese Verordnung sollte Vorschriften unberührt lassen, die besonderen Bedürfnissen einzelner Sektoren oder Bereichen von öffentlichem Interesse Rechnung tragen. Solche Vorschriften können zusätzliche Anforderungen an technische Aspekte des Datenzugangs wie Schnittstellen für den Datenzugang oder die Art und Weise umfassen, wie der Datenzugang gewährt werden könnte, z. B. direkt über das Produkt oder über Datenvermittlungsdienste. Ebenso können solche Vorschriften Beschränkungen der Rechte der Dateninhaber auf Zugang zu oder Nutzung von Nutzerdaten oder andere Aspekte betreffen, die über den Datenzugang und die Datennutzung hinausgehen, wie z. B. Governance-Aspekte. Diese Verordnung sollte auch spezifischere Vorschriften im Zusammenhang mit der Entwicklung gemeinsamer europäischer Datenräume unberührt lassen.

(88) Diese Verordnung sollte die Anwendung der Wettbewerbsvorschriften, insbesondere der Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unberührt lassen. Die in dieser Verordnung vorgesehenen Maßnahmen sollten nicht dazu verwendet werden, den Wettbewerb in einer gegen den AEUV verstoßenden Weise einzuschränken.

(89) Damit sich die Wirtschaftsteilnehmer an die neuen Vorschriften dieser Verordnung anpassen können, sollten sie erst ein Jahr nach Inkrafttreten der Verordnung anwendbar werden.

(90) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 der Verordnung (EU) 2018/1725 angehört und haben am [XX. XX 2022] eine gemeinsame Stellungnahme abgegeben —

[71] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand und Anwendungsbereich

(1) Diese Verordnung enthält harmonisierte Vorschriften über die Bereitstellung von Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, für den Nutzer dieses Produktes oder Dienstes, über die Bereitstellung von Daten durch Dateninhaber für Datenempfänger und über die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen oder Organe, Einrichtungen und sonstige Stellen der Union, soweit diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse benötigt werden.

(2) Diese Verordnung gilt für

a) Hersteller von Produkten und Erbringer verbundener Dienste, die in der Union in Verkehr gebracht werden, und die Nutzer solcher Produkte oder Dienste;

b) Dateninhaber, die Datenempfängern in der Union Daten bereitstellen;

c) Datenempfänger in der Union, denen Daten bereitgestellt werden;

d) öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union, die von Dateninhabern verlangen, Daten bereitzustellen, sofern diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer Aufgabe von öffentlichem Interesse benötigt werden, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;

e) Anbieter von Datenverarbeitungsdiensten, die Kunden in der Union solche Dienste anbieten.

(3) Die Rechtsvorschriften der Union über den Schutz personenbezogener Daten, die Privatsphäre, die Vertraulichkeit der Kommunikation und die Integrität von Endgeräten gelten für personenbezogene Daten, die im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten verarbeitet werden. Diese Verordnung berührt nicht die Anwendbarkeit der Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, sowie die Befugnisse und Zuständigkeiten der Aufsichtsbehörden. Soweit die in Kapitel II dieser Verordnung festgelegten Rechte betroffen sind und es sich bei den Nutzern um von der Verarbeitung personenbezogener Daten betroffene Personen handelt, die den Rechten und Pflichten des genannten Kapitels unterliegen, ergänzen die Bestimmungen dieser Verordnung das Recht auf Datenübertragbarkeit nach Artikel 20 der Verordnung (EU) 2016/679.

(4) Diese Verordnung berührt nicht Rechtsvorschriften der Union und die nationalen Rechtsvorschriften über die Datenweitergabe, den Datenzugang und die Datennutzung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich der Verordnung

(EU) 2021/784 des Europäischen Parlaments und des Rates[72] und der [Vorschläge über elektronische Beweismittel COM(2018) 225 und COM(2018) 226], sobald diese angenommen sind, sowie die internationale Zusammenarbeit in diesem Bereich. Diese Verordnung berührt nicht die Datenerhebung, den Datenaustausch, den Datenzugang und die Datennutzung gemäß der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates über die Übermittlung von Angaben bei Geldtransfers. Im Einklang mit dem Unionsrecht berührt diese Verordnung nicht die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, Verteidigung, nationale Sicherheit, Zoll- und Steuerverwaltung sowie Gesundheit und Sicherheit der Bürger.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Daten“ jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material;
2. „Produkt“ einen körperlichen beweglichen Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist;
3. „verbundener Dienst“ einen digitalen Dienst, einschließlich Software, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine seiner Funktionen nicht ausführen könnte;
4. „virtuelle Assistenten“ Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton- und Schriftform, Gesten oder Bewegungen, und auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu eigenen Diensten und Diensten Dritter gewährt oder eigene Geräte und Geräte Dritter steuert;
5. „Nutzer“ eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt;
6. „Dateninhaber“ eine juristische oder natürliche Person, die nach dieser Verordnung, nach anwendbarem Unionsrecht oder nach den anwendbaren nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet bzw. im Falle nicht personenbezogener Daten und durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen;
7. „Datenempfänger“ eine juristische oder natürliche Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines Produktes oder verbundenen Dienstes zu sein, und der vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der

[72] Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (ABl. L 172 vom 17.5.2021, S. 79).

Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer Rechtspflicht aus anderen Rechtsvorschriften der Union oder aus nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts Daten bereitstellt;

8. „Unternehmen“ eine natürliche oder juristische Person, die in Bezug auf von dieser Verordnung erfasste Verträge und Praktiken zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt;

9. „öffentliche Stelle“ die nationalen, regionalen und lokalen Behörden, Körperschaften und Einrichtungen des öffentlichen Rechts der Mitgliedstaaten oder Verbände, die aus einer oder mehreren dieser Behörden, Körperschaften oder Einrichtungen bestehen;

10. „öffentlicher Notstand“ eine außergewöhnliche Situation, die sich negativ auf die Bevölkerung der Union, eines Mitgliedstaats oder eines Teils davon auswirkt und das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen oder die wirtschaftliche Stabilität oder die Gefahr einer erheblichen Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem bzw. den betroffenen Mitgliedstaaten birgt;

11. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Daten in elektronischer Form wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

12. „Datenverarbeitungsdienst“ eine digitale Dienstleistung, bei der es sich um keinen Online-Inhaltedienst im Sinne des Artikels 2 Absatz 5 der Verordnung (EU) 2017/1128 handelt, die einem Kunden bereitgestellt wird und eine Verwaltung auf Abruf und einen breiten Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer, zentralisierter, verteilter oder hochgradig verteilter Rechenressourcen ermöglicht;

13. „Dienstart“ eine Reihe von Datenverarbeitungsdiensten, die dasselbe Hauptziel haben und dasselbe grundlegende Dienstmodell für die Datenverarbeitung aufweisen;

14. „Funktionsäquivalenz“ die Aufrechterhaltung eines Mindestfunktionsumfangs in der Umgebung eines neuen Datenverarbeitungsdienstes nach dem Wechselvorgang, sodass der Nutzer bei einer Eingabe zu Kernelementen des Dienstes vom übernehmenden Dienst das gleiche Ergebnis mit der gleichen Leistung und dem gleichen Niveau der Sicherheit, Betriebsstabilität und Dienstqualität erhält wie vom vorherigen Dienst zum Zeitpunkt der Vertragskündigung;

15. „offene Interoperabilitätsspezifikationen“ technische IKT-Spezifikationen im Sinne der Verordnung (EU) Nr. 1025/2012, die leistungsbezogen darauf ausgerichtet sind, die Interoperabilität zwischen Datenverarbeitungsdiensten herzustellen;

16. „intelligenter Vertrag“ ein in einem elektronischen Vorgangsregistersystem gespeichertes Computerprogramm, bei dem das Ergebnis der Programmausführung in dem elektronischen Vorgangsregister aufgezeichnet wird;

17. „elektronisches Vorgangsregister“ ein elektronisches Vorgangsregister im Sinne des Artikels 3 Nummer 53 der Verordnung (EU) Nr. 910/2014;

18. „gemeinsame Spezifikationen“ ein Dokument, bei dem es sich nicht um eine Norm handelt und das technische Lösungen enthält, die es ermöglichen, bestimmte Anforderungen und Pflichten, die im Rahmen dieser Verordnung festgelegt worden sind, zu erfüllen;

19. „Interoperabilität“ die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, Produkten, Anwendungen oder Komponenten, Daten auszutauschen und zu verwenden, um ihre Funktionen auszuführen;

20. „harmonisierte Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012.

KAPITEL II
DATENWEITERGABE VON UNTERNEHMEN AN VERBRAUCHER UND ZWISCHEN UNTERNEHMEN

Artikel 3
Pflicht der Zugänglichmachung von bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten

(1) Produkte werden so konzipiert und hergestellt und verbundene Dienste so erbracht, dass die bei ihrer Nutzung erzeugten Daten standardmäßig für den Nutzer einfach, sicher und – soweit relevant und angemessen – direkt zugänglich sind.

(2) Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein Produkt oder verbundenen Dienst werden dem Nutzer mindestens folgende Informationen in einem klaren und verständlichen Format bereitgestellt:

a) Art und Umfang der Daten, die voraussichtlich bei der Nutzung des Produktes oder verbundenen Dienstes erzeugt werden;

b) ob die Daten voraussichtlich kontinuierlich und in Echtzeit erzeugt werden;

c) wie der Nutzer auf diese Daten zugreifen kann;

d) ob der Hersteller, der das Produkt liefert, oder der Dienstleister, der den verbundenen Dienst erbringt, beabsichtigt, die Daten selbst zu nutzen oder einem Dritten die Nutzung der Daten zu gestatten, und falls ja, für welche Zwecke diese Daten genutzt werden sollen;

e) ob der Verkäufer, Mieter oder Leasinggeber der Dateninhaber ist und, falls nicht, die Identität des Dateninhabers, z. B. sein Handelsname und die Anschrift des Ortes, an dem er niedergelassen ist;

f) die Kommunikationsmittel, mit denen der Nutzer den Dateninhaber schnell kontaktieren und effizient mit diesem kommunizieren kann;

g) wie der Nutzer veranlassen kann, dass die Daten an einen Dritten weitergegeben werden;

h) das Recht des Nutzers, bei der in Artikel 31 genannten zuständigen Behörde Beschwerde wegen eines Verstoßes gegen die Bestimmungen dieses Kapitels einzulegen.

Artikel 4

Recht der Nutzer auf Zugang zu den bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten und auf deren Nutzung

(1) Soweit der Nutzer nicht direkt vom Produkt aus auf die Daten zugreifen kann, stellt der Dateninhaber dem Nutzer die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit zur Verfügung. Dies geschieht auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch machbar ist.

(2) Der Dateninhaber verlangt vom Nutzer keine Informationen, die über das hinausgehen, was erforderlich ist, um dessen Eigenschaft als Nutzer gemäß Absatz 1 zu überprüfen. Der Dateninhaber bewahrt keine Informationen über den Zugang des Nutzers zu den verlangten Daten auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Nutzers und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist.

(3) Geschäftsgeheimnisse werden nur offengelegt, wenn alle besonderen Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Dateninhaber und der Nutzer können Maßnahmen vereinbaren, um die Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten, zu wahren.

(4) Der Nutzer darf die aufgrund eines Verlangens nach Absatz 1 erlangten Daten nicht zur Entwicklung eines Produktes nutzen, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht.

(5) Ist der Nutzer keine von der Datenverarbeitung betroffene Person, so darf der Dateninhaber personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, dem Nutzer nur dann zur Verfügung stellen, wenn es dafür eine gültige Rechtsgrundlage gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 der Verordnung (EU) 2016/679 erfüllt sind.

(6) Der Dateninhaber darf nicht personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen. Der Dateninhaber darf solche Daten, die bei der Nutzung des Produktes oder verbundenen Dienstes erzeugt werden, nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer zu erlangen, wenn dies die gewerbliche Position des Nutzers auf den Märkten, auf denen dieser tätig ist, untergraben könnte.

Artikel 5

Recht auf Weitergabe von Daten an Dritte

(1) Auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei stellt der Dateninhaber die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugten Daten einem Dritten unverzüglich, für den Nutzer kostenlos, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, und gegebenenfalls kontinuierlich und in Echtzeit bereit.

(2) Ein Unternehmen, das zentrale Plattformdienste erbringt und für mindestens einen dieser Dienste nach Artikel [...] der [Verordnung XXX über bestreitbare und faire

Märkte im digitalen Sektor (Gesetz über digitale Märkte)[73]] als Gatekeeper benannt wurde, kommt nicht als zulässiger Dritter im Sinne dieses Artikels in Betracht und darf daher nicht

a) einen Nutzer in irgendeiner Weise auffordern oder geschäftlich anreizen, auch nicht durch eine finanzielle oder sonstige Gegenleistung, Daten, die vom Nutzer aufgrund eines Verlangens nach Artikel 4 Absatz 1 erlangt wurden, für einen seiner Dienste bereitzustellen;

b) einen Nutzer auffordern oder geschäftlich anreizen, vom Dateninhaber zu verlangen, gemäß Absatz 1 dieses Artikels Daten für einen seiner Dienste bereitzustellen;

c) von einem Nutzer Daten erhalten, die der Nutzer aufgrund eines Verlangens nach Artikel 4 Absatz 1 erlangt hat.

(3) Der Nutzer oder der Dritte braucht keine Informationen herauszugeben, die über das hinausgehen, was erforderlich ist, um dessen Eigenschaft als Nutzer oder Dritter gemäß Absatz 1 zu überprüfen. Der Dateninhaber bewahrt keine Informationen über den Zugang des Dritten zu den verlangten Daten auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Dritten und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist.

(4) Der Dritte darf keine Zwangsmittel einsetzen oder offensichtliche Lücken in der technischen Infrastruktur des Dateninhabers, mit der die Daten geschützt werden sollen, ausnutzen, um Zugang zu Daten zu erlangen.

(5) Der Dateninhaber darf nicht personenbezogene Daten, die bei der Nutzung des Produktes oder verbundenen Dienstes erzeugt werden, nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Dritten oder in die Nutzung durch den Dritten zu erlangen, wenn dies die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte, es sei denn, der Dritte hat einer solchen Nutzung zugestimmt und hat die technische Möglichkeit, diese Zustimmung jederzeit zu widerrufen.

(6) Ist der Nutzer keine von der Datenverarbeitung betroffene Person, so dürfen personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, nur dann bereitgestellt werden, wenn es dafür eine gültige Rechtsgrundlage gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 der Verordnung (EU) 2016/679 erfüllt sind.

(7) Die Ausübung der Rechte der betroffenen Person gemäß der Verordnung (EU) 2016/679 und insbesondere des Rechts auf Datenübertragbarkeit gemäß Artikel 20 der genannten Verordnung darf durch Versäumnisse seitens des Dateninhabers oder des Dritten, Vorkehrungen für die Übermittlung der Daten zu treffen, nicht behindert, verhindert oder beeinträchtigt werden.

(8) Geschäftsgeheimnisse werden Dritten gegenüber nur insoweit offengelegt, als dies für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck unbedingt erforderlich ist und der Dritte alle zwischen ihm und dem Dateninhaber vereinbarten besonderen Maßnahmen getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren. In diesem Fall werden die Eigenschaft der Daten als Geschäftsgeheimnisse und die Maßnahmen zur Wahrung der

[73] ABl. […].

Vertraulichkeit in der Vereinbarung zwischen dem Dateninhaber und dem Dritten festgelegt.

(9) Das Recht gemäß Absatz 1 darf die Datenschutzrechte anderer Personen nicht beeinträchtigen.

Artikel 6
Pflichten Dritter, die Daten auf Verlangen des Nutzers erhalten

(1) Ein Dritter verarbeitet die ihm nach Artikel 5 bereitgestellten Daten nur für die Zwecke und unter den Bedingungen, die er mit dem Nutzer vereinbart hat, und – soweit personenbezogene Daten betroffen sind – vorbehaltlich der Rechte der betroffenen Person, und löscht die Daten, sobald sie für den vereinbarten Zweck nicht mehr benötigt werden.

(2) Der Dritte darf nicht

a) den Nutzer in irgendeiner Weise zwingen, täuschen oder manipulieren, indem er – auch mittels einer digitalen Schnittstelle mit dem Nutzer – die Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten des Nutzers untergräbt oder beeinträchtigt;

b) die erhaltenen Daten für das Profiling natürlicher Personen im Sinne des Artikels 4 Nummer 4 der Verordnung (EU) 2016/679 nutzen, es sei denn, dies ist erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen;

c) die erhaltenen Daten einem anderen Dritten in roher, aggregierter oder abgeleiteter Form bereitstellen, es sei denn, dies ist erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen;

d) die erhaltenen Daten einem Unternehmen, das zentrale Plattformdienste erbringt und für mindestens einen dieser Dienste gemäß Artikel […] der [Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte)] als Gatekeeper benannt wurde, bereitstellen;

e) die erhaltenen Daten nutzen, um ein Produkt zu entwickeln, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht, oder die Daten zu diesem Zweck an einen anderen Dritten weitergeben;

f) den Nutzer – auch nicht durch vertragliche Pflichten – daran hindern, die erhaltenen Daten anderen Parteien bereitzustellen.

Artikel 7
Umfang der Pflichten zur Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

(1) Die Pflichten dieses Kapitels gelten nicht für Daten, die bei der Nutzung von Produkten oder verbundenen Diensten erzeugt werden, die von Unternehmen hergestellt bzw. erbracht werden, die als Kleinst- oder Kleinunternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG gelten, sofern diese Unternehmen keine Partnerunternehmen oder verbundenen Unternehmen im Sinne des Artikels 3 des Anhangs der Empfehlung 2003/361/EG haben, die nicht als Kleinst- oder Kleinunternehmen gelten.

(2) Wird in dieser Verordnung auf Produkte und verbundene Dienste Bezug genommen, so schließt diese Bezugnahme auch virtuelle Assistenten ein, soweit diese für den

Zugang zu einem Produkt oder verbundenen Dienst oder dessen Steuerung benutzt werden.

KAPITEL III
PFLICHTEN DER DATENINHABER, DIE RECHTLICH VERPFLICHTET SIND, DATEN BEREITZUSTELLEN

Artikel 8
Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen

(1) Ist ein Dateninhaber nach Artikel 5 oder nach anderen Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts verpflichtet, einem Datenempfänger Daten bereitzustellen, so geschieht dies zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise im Einklang mit den Bestimmungen dieses Kapitels und des Kapitels IV.

(2) Der Dateninhaber vereinbart mit dem Datenempfänger die Bedingungen für die Bereitstellung der Daten. Eine Vertragsklausel in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten ist nicht bindend, wenn sie die Bedingungen des Artikels 13 erfüllt oder wenn sie die Ausübung der Rechte des Nutzers nach Kapitel II ausschließt, davon abweicht oder deren Wirkung abändert.

(3) Bei der Bereitstellung von Daten darf ein Dateninhaber nicht zwischen vergleichbaren Kategorien von Datenempfängern, einschließlich seiner Partnerunternehmen oder verbundenen Unternehmen im Sinne des Artikels 3 des Anhangs der Empfehlung 2003/361/EG, diskriminieren. Ist ein Datenempfänger der Ansicht, dass die Bedingungen, unter denen ihm Daten bereitgestellt werden, diskriminierend sind, so obliegt dem Dateninhaber der Nachweis, dass keine Diskriminierung vorliegt.

(4) Ein Dateninhaber darf einem Datenempfänger Daten nur dann exklusiv zur Verfügung stellen, wenn der Nutzer dies gemäß Kapitel II verlangt hat.

(5) Dateninhaber und Datenempfänger brauchen keine Informationen herauszugeben, die über das hinausgehen, was erforderlich ist, um die Einhaltung der für die Datenbereitstellung vereinbarten Vertragsbedingungen oder die Erfüllung ihrer Pflichten aus dieser Verordnung oder aus anderen anwendbaren Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts zu überprüfen.

(6) Eine Pflicht, einem Datenempfänger Daten bereitzustellen, verpflichtet nicht zur Offenlegung von Geschäftsgeheimnissen im Sinne der Richtlinie (EU) 2016/943, es sei denn, im Unionsrecht, einschließlich des Artikels 6 dieser Verordnung, oder in nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts ist etwas anderes vorgesehen.

Artikel 9
Gegenleistung für die Bereitstellung von Daten

(1) Jede Gegenleistung, die zwischen einem Dateninhaber und einem Datenempfänger für die Bereitstellung von Daten vereinbart wird, muss angemessen sein.

(2) Ist der Datenempfänger ein Kleinstunternehmen oder ein kleines oder mittleres Unternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG, so darf die vereinbarte Gegenleistung nicht höher sein als die Kosten, die mit der Bereitstellung der Daten für den Datenempfänger unmittelbar zusammenhängen und dem Verlangen zuzurechnen sind. Artikel 8 Absatz 3 gilt entsprechend.

(3) Dieser Artikel steht dem nicht entgegen, dass andere Rechtsvorschriften der Union oder nationale Rechtsvorschriften zur Umsetzung des Unionsrechts eine Gegenleistung für die Bereitstellung von Daten ausschließen oder eine geringere Gegenleistung vorsehen.

(4) Der Dateninhaber stellt dem Datenempfänger Informationen zur Verfügung, denen die Grundlage für die Berechnung der Gegenleistung so detailliert zu entnehmen ist, dass der Datenempfänger überprüfen kann, ob die Anforderungen des Absatzes 1 und gegebenenfalls des Absatzes 2 erfüllt sind.

Artikel 10
Streitbeilegung

(1) Dateninhaber und Datenempfänger haben Zugang zu Streitbeilegungsstellen, die nach Absatz 2 dieses Artikels zugelassen sind, um Streitigkeiten in Bezug auf die Festlegung fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten und die transparente Art und Weise der Bereitstellung von Daten gemäß den Artikeln 8 und 9 beizulegen.

(2) Der Mitgliedstaat, in dem die Streitbeilegungsstelle niedergelassen ist, lässt diese Stelle auf deren Antrag hin zu, nachdem die Stelle nachgewiesen hat, dass sie alle folgenden Bedingungen erfüllt:

a) sie ist unparteiisch und unabhängig und wird ihre Entscheidungen nach klaren und fairen Verfahrensregeln treffen;

b) sie verfügt über das erforderliche Fachwissen in Bezug auf die Festlegung fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten und die transparente Art und Weise ihrer Bereitstellung, das es der Stelle ermöglicht, solche Bedingungen wirksam festzulegen;

c) sie ist über elektronische Kommunikationsmittel leicht erreichbar;

d) sie ist in der Lage, ihre Entscheidungen rasch, effizient und kostengünstig in mindestens einer Amtssprache der Union zu treffen.

Ist in einem Mitgliedstaat bis zum [Datum des Geltungsbeginns der Verordnung] keine Streitbeilegungsstelle zugelassen worden, so richtet dieser Mitgliedstaat eine Streitbeilegungsstelle ein, die die in den Buchstaben a bis d dieses Absatzes genannten Bedingungen erfüllt, und lässt diese zu.

(3) Die Mitgliedstaaten teilen der Kommission die nach Absatz 2 zugelassenen Streitbeilegungsstellen mit. Die Kommission veröffentlicht auf einer eigens hierfür eingerichteten Website eine Liste dieser Stellen und hält diese auf dem neuesten Stand.

(4) Die Streitbeilegungsstellen machen den betroffenen Parteien die Entgelte oder die zur Festsetzung der Entgelte verwendeten Methoden bekannt, bevor diese Parteien eine Entscheidung beantragen.

(5) Die Streitbeilegungsstellen verweigern die Bearbeitung eines Streitbeilegungsantrags, der bereits bei einer anderen Streitbeilegungsstelle oder einem Gericht eines Mitgliedstaats eingereicht wurde.

(6) Die Streitbeilegungsstellen räumen den Parteien die Möglichkeit ein, sich innerhalb einer angemessenen Frist zu den Angelegenheiten zu äußern, in denen sich die Parteien an diese Stellen gewandt haben. In diesem Zusammenhang stellen die Streitbeilegungsstellen diesen Parteien die Schriftsätze der anderen Partei und etwaige Erklärungen von Sachverständigen zur Verfügung. Die Streitbeilegungsstellen geben den Parteien die Möglichkeit, zu diesen Schriftsätzen und Erklärungen Stellung zu nehmen.

(7) Die Streitbeilegungsstellen entscheiden in Angelegenheiten, die ihnen vorgelegt werden, spätestens 90 Tage nach der Beantragung. Diese Entscheidungen werden schriftlich oder auf einem dauerhaften Datenträger niedergelegt und mit einer Begründung versehen.

(8) Die Entscheidung der Streitbeilegungsstelle ist für die Parteien nur dann bindend, wenn die Parteien vor Beginn des Streitbeilegungsverfahrens dem bindenden Charakter ausdrücklich zugestimmt haben.

(9) Dieser Artikel berührt nicht das Recht der Parteien, wirksame Rechtsmittel bei einem Gericht eines Mitgliedstaats einzulegen.

Artikel 11

Technische Schutzmaßnahmen und Bestimmungen über die unbefugte Nutzung oder Offenlegung von Daten

(1) Der Dateninhaber kann geeignete technische Schutzmaßnahmen, einschließlich intelligenter Verträge, anwenden, um einen unbefugten Zugang zu den Daten zu verhindern und die Einhaltung der Artikel 5, 6, 9 und 10 sowie der für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen. Solche technischen Schutzmaßnahmen dürfen nicht als Mittel eingesetzt werden, um zu verhindern, dass ein Nutzer sein Recht, Dritten nach Artikel 5 wirksam Daten bereitzustellen, ausübt oder dass ein Dritter ein Recht nach den Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts gemäß Artikel 8 Absatz 1 in Anspruch nimmt.

(2) Ein Datenempfänger, der dem Dateninhaber zwecks Erlangung der Daten ungenaue oder falsche Informationen gegeben, Täuschungen und Zwangsmittels eingesetzt oder offensichtliche Lücken in der dem Schutz der Daten dienenden technischen Infrastruktur des Dateninhabers missbraucht, die bereitgestellten Daten für nicht genehmigte Zwecke genutzt oder ohne Zustimmung des Dateninhabers an eine andere Partei weitergegeben hat, muss – sofern der Dateninhaber oder der Nutzer nichts anderes anweist – unverzüglich

a) die vom Dateninhaber bereitgestellten Daten und alle etwaigen Kopien davon vernichten;

b) das Herstellen, Anbieten, Inverkehrbringen oder Verwenden von Waren, abgeleiteten Daten oder Dienstleistungen, die auf den mit den Daten erlangten Kenntnissen beruhen, oder das Einführen, Ausführen oder Lagern von in diesem Sinne rechtsverletzenden Waren beenden und alle rechtsverletzenden Waren vernichten.

(3) Absatz 2 Buchstabe b gilt nicht in folgenden Fällen:

a) dem Dateninhaber ist durch die Nutzung der Daten kein erheblicher Schaden entstanden;

b) dies wäre im Hinblick auf die Interessen des Dateninhabers unverhältnismäßig.

Artikel 12

Umfang der Pflichten der Dateninhaber, die rechtlich verpflichtet sind, Daten bereitzustellen

(1) Dieses Kapitel gilt, wenn ein Dateninhaber nach Artikel 5 oder nach Unionsrecht oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts verpflichtet ist, einem Datenempfänger Daten bereitzustellen.

(2) Eine Vertragsklausel in einer Datenweitergabevereinbarung, die zum Nachteil einer Partei oder gegebenenfalls zum Nachteil des Nutzers die Anwendung dieses Kapitels ausschließt, davon abweicht oder seine Wirkung abändert, ist für diese Partei nicht bindend.

(3) Dieses Kapitel gilt nur in Bezug auf Datenbereitstellungspflichten nach Unionsrecht oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts, die nach dem [Datum des Geltungsbeginns der Verordnung] in Kraft treten.

KAPITEL IV
MISSBRÄUCHLICHE KLAUSELN IN BEZUG AUF DEN DATENZUGANG UND DIE DATENNUTZUNG ZWISCHEN UNTERNEHMEN

Artikel 13

Missbräuchliche Vertragsklauseln, die einem Kleinstunternehmen, kleinen oder mittleren Unternehmen einseitig auferlegt werden

(1) Eine Vertragsklausel in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, die ein Unternehmen einem Kleinstunternehmen oder einem kleinen oder mittleren Unternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG einseitig auferlegt hat, ist für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich ist.

(2) Eine Vertragsklausel ist missbräuchlich, wenn ihre Verwendung gröblich von der guten Geschäftspraxis beim Datenzugang und der Datennutzung abweicht und gegen das Gebot von Treu und Glauben und des redlichen Geschäftsverkehrs verstößt.

(3) Eine Vertragsklausel ist missbräuchlich im Sinne dieses Artikels, wenn sie Folgendes bezweckt oder bewirkt:

a) den Ausschluss oder die Beschränkung der Haftung der Partei, die die Klausel einseitig auferlegt hat, für vorsätzliche oder grob fahrlässige Handlungen;

b) den Ausschluss der Rechtsbehelfe, die der Partei, der die Klausel einseitig auferlegt wurde, bei Nichterfüllung von Vertragspflichten zur Verfügung stehen, oder den Ausschluss der Haftung der Partei, die die Klausel einseitig auferlegt hat, bei einer Verletzung solcher Pflichten;

c) das ausschließliche Recht der Partei, die die Klausel einseitig auferlegt hat, zu bestimmen, ob die gelieferten Daten vertragsgemäß sind, oder eine Vertragsklausel auszulegen.

(4) Eine Vertragsklausel gilt als missbräuchlich im Sinne dieses Artikels, wenn sie Folgendes bezweckt oder bewirkt:

a) eine unangemessene Beschränkung der Rechtsmittel bei Nichterfüllung von Vertragspflichten oder der Haftung bei einer Verletzung solcher Pflichten;

b) ein Recht der Partei, die die Klausel einseitig auferlegt hat, auf Zugang zu Daten der anderen Vertragspartei und deren Nutzung in einer Weise, die den berechtigten Interessen der anderen Vertragspartei erheblich schadet;

c) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, die von ihr während der Vertragslaufzeit bereitgestellten oder erzeugten Daten zu nutzen, oder eine Beschränkung der Nutzung solcher Daten insofern, als diese Partei nicht berechtigt ist, diese Daten in verhältnismäßiger Weise zu nutzen, zu erfassen, darauf zuzugreifen oder sie zu kontrollieren oder zu verwerten;

d) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, eine Kopie der von ihr bereitgestellten oder erzeugten Daten während der Vertragslaufzeit oder innerhalb einer angemessenen Frist nach Kündigung des Vertrags zu erhalten;

e) die Möglichkeit, dass die Partei, die die Klausel einseitig auferlegt hat, den Vertrag mit unangemessen kurzer Frist kündigen darf, und zwar unter Berücksichtigung der realistischen Möglichkeiten der anderen Vertragspartei, zu einem alternativen und vergleichbaren Dienst zu wechseln, und des durch die Kündigung verursachten finanziellen Nachteils, außer bei Vorliegen schwerwiegender Gründe.

(5) Eine Vertragsklausel gilt im Sinne dieses Artikels als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht wird und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann. Die Vertragspartei, die eine Vertragsklausel eingebracht hat, trägt die Beweislast dafür, dass diese Klausel nicht einseitig auferlegt wurde.

(6) Ist die missbräuchliche Vertragsklausel von den übrigen Bedingungen des Vertrags abtrennbar, so bleiben die übrigen Vertragsbedingungen bindend.

(7) Dieser Artikel gilt weder für Vertragsklauseln, in denen der Hauptgegenstand des Vertrags festgelegt wird, noch für Vertragsklauseln, in denen der zu zahlende Preis festgelegt wird.

(8) Die Parteien eines unter Absatz 1 fallenden Vertrags können die Anwendung dieses Artikels nicht ausschließen, davon abweichen oder dessen Wirkungen abändern.

KAPITEL V
BEREITSTELLUNG VON DATEN FÜR ÖFFENTLICHE STELLEN UND ORGANE, EINRICHTUNGEN UND SONSTIGE STELLEN DER UNION WEGEN AUßERGEWÖHNLICHER NOTWENDIGKEIT

Artikel 14

Pflicht zur Bereitstellung von Daten wegen außergewöhnlicher Notwendigkeit

(1) Auf Verlangen stellt der Dateninhaber einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union, die eine außergewöhnliche Notwendigkeit der Nutzung der verlangten Daten nachweist, Daten bereit.

(2) Dieses Kapitel gilt nicht für kleine Unternehmen und Kleinstunternehmen im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG der Kommission.

Artikel 15

Außergewöhnliche Notwendigkeit der Datennutzung

Eine außergewöhnliche Notwendigkeit der Datennutzung im Sinne dieses Kapitels liegt unter einem der folgenden Umstände vor:

a) die verlangten Daten sind zur Bewältigung eines öffentlichen Notstands erforderlich,

b) das Datenverlangen ist zeitlich befristet, im Umfang begrenzt und erforderlich, um einen öffentlichen Notstand zu verhindern oder die Erholung von einem öffentlichen Notstand zu unterstützen;

c) aufgrund des Fehlens verfügbarer Daten ist die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union daran gehindert, eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen, und

   1. die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union kann diese Daten nicht auf andere Weise erlangen, auch nicht durch Datenerwerb auf dem Markt zu Marktpreisen oder aufgrund bestehender Datenbereitstellungspflichten, und durch den Erlass neuer Rechtsvorschriften kann die rechtzeitige Verfügbarkeit der Daten nicht gewährleistet werden, oder

   2. die Erlangung der Daten nach dem in diesem Kapitel festgelegten Verfahren würde den Verwaltungsaufwand der Dateninhaber oder anderer Unternehmen erheblich verringern.

Artikel 16

Verhältnis zu anderen Pflichten zur Übermittlung von Daten an öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union

(1) Dieses Kapitel berührt nicht die im Unionsrecht oder im nationalen Recht festgelegten Pflichten in Bezug auf die Berichterstattung, das Beantworten von Auskunftsersuchen oder den Nachweis und die Überprüfung der Einhaltung rechtlicher Pflichten.

(2) Öffentliche Stellen sowie Organe, Einrichtungen und sonstige Stelle der Union dürfen die Rechte aus diesem Kapitel nicht ausüben, um Tätigkeiten der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung oder der Zoll- oder Steuerverwaltung durchzuführen. Dieses Kapitel berührt nicht das anwendbare Unionsrecht und die anwendbaren nationalen Rechtsvorschriften über die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder über die Vollstreckung von Strafen oder verwaltungsrechtlichen Sanktionen oder über die Zoll- oder Steuerverwaltung.

Artikel 17
Datenbereitstellungsverlangen

(1) Öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellen der Union müssen in ihren Datenverlangen nach Artikel 14 Absatz 1

a) angeben, welche Daten benötigt werden;

b) die außergewöhnliche Notwendigkeit nachweisen, für die die Daten verlangt werden;

c) den Zweck des Verlangens, die beabsichtigte Nutzung der verlangten Daten und die Dauer dieser Nutzung erläutern;

d) die Rechtsgrundlage für das Datenverlangen angeben;

e) die Frist angeben, innerhalb deren die Daten bereitzustellen sind oder innerhalb deren der Dateninhaber die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union ersuchen kann, das Verlangen zu ändern oder zurückzuziehen.

(2) Ein Datenverlangen nach Absatz 1 muss

a) in klarer, prägnanter, einfacher und für den Dateninhaber verständlicher Sprache abgefasst sein;

b) im Hinblick auf die Granularität und den Umfang der verlangten Daten sowie die Häufigkeit des Zugangs zu den verlangten Daten in einem angemessenen Verhältnis zu der außergewöhnlichen Notwendigkeit stehen;

c) die rechtmäßigen Ziele des Dateninhabers unter Berücksichtigung des Schutzes von Geschäftsgeheimnissen und der Kosten und des nötigen Aufwands der Datenbereitstellung achten;

d) soweit wie möglich nur nicht personenbezogene Daten betreffen;

e) dem Dateninhaber Aufschluss über die Sanktionen geben, die nach Artikel 33 von einer nach Artikel 31 zuständigen Behörde verhängt werden, wenn er dem Verlangen nicht nachkommt;

f) ohne ungebührliche Verzögerung online veröffentlicht werden.

(3) Öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellen der Union dürfen nach diesem Kapitel erlangte Daten nicht zur Weiterverwendung im Sinne der Richtlinie (EU) 2019/1024 zur Verfügung stellen. Die Richtlinie (EU) 2019/1024 findet keine Anwendung auf nach diesem Kapitel erlangte Daten im Besitz öffentlicher Stellen.

(4) Absatz 3 hindert eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union nicht daran, nach diesem Kapitel erlangte Daten mit anderen öffentlichen Stellen und mit Organen, Einrichtungen oder sonstigen Stellen der Union zur Wahrnehmung der in Artikel 15 genannten Aufgaben auszutauschen oder die Daten einem Dritten bereitzustellen, den sie im Rahmen einer öffentlich zugänglichen Vereinbarung mit technischen Inspektionen oder anderen Aufgaben betraut hat. Dabei gelten die in Artikel 19 genannten Pflichten der öffentlichen Stellen und der Organe, Einrichtungen und sonstigen Stellen der Union.

Wenn eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union Daten nach diesem Absatz übermittelt oder bereitstellt, teilt sie dies dem Dateninhaber, von dem sie die Daten erhalten hat, mit.

Artikel 18
Erfüllung von Datenzugangsverlangen

(1) Ein Dateninhaber, der ein Datenzugangsverlangen nach diesem Kapitel erhält, stellt der anfragenden öffentlichen Stelle oder dem Organ, der Einrichtung oder der sonstigen Stelle der Union die Daten unverzüglich bereit.

(2) Unbeschadet besonderer Erfordernisse bezüglich der Verfügbarkeit von Daten, die in sektorspezifischen Rechtsvorschriften festgelegt sind, kann der Dateninhaber im Falle von Daten, die zur Bewältigung eines öffentlichen Notstands erforderlich sind, innerhalb von fünf Arbeitstagen und in anderen Fällen einer außergewöhnlichen Notwendigkeit innerhalb von 15 Arbeitstagen nach Eingang das Verlangen aus einem der folgenden Gründe ablehnen oder dessen Änderung beantragen:

a) die Daten sind nicht verfügbar;

b) das Verlangen erfüllt nicht die Voraussetzungen in Artikel 17 Absätze 1 und 2.

(3) Im Falle eines Verlangens nach Daten, die zur Bewältigung eines öffentlichen Notstands erforderlich sind, kann der Dateninhaber das Verlangen auch dann ablehnen oder dessen Änderung beantragen, wenn er die verlangten Daten bereits auf ein vorheriges Verlangen einer anderen öffentlichen Stelle oder eines Organs, einer Einrichtung oder einer sonstigen Stelle der Union zu demselben Zweck übermittelt hat und ihm nicht gemäß Artikel 19 Absatz 1 Buchstabe c die Vernichtung der Daten mitgeteilt wurde.

(4) Wenn der Dateninhaber das Verlangen gemäß Absatz 3 ablehnt oder dessen Änderung beantragt, nennt er die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union, die zuvor zu demselben Zweck Daten verlangt hatte.

(5) Ist zur Erfüllung eines Verlangens, einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union Daten bereitzustellen, die Offenlegung personenbezogener Daten erforderlich, so unternimmt der Dateninhaber angemessene Anstrengungen, um die Daten zu pseudonymisieren, sofern das Verlangen mit pseudonymisierten Daten erfüllt werden kann.

(6) Möchte die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union der Ablehnung eines Dateninhabers, die verlangten Daten bereitzustellen, oder der von ihm beantragten Änderung des Verlangens widersprechen oder möchte der Dateninhaber Einspruch gegen das Verlangen einlegen, so wird die in Artikel 31 genannte zuständige Behörde mit der Angelegenheit befasst.

Artikel 19

Pflichten öffentlicher Stellen und der Organe, Einrichtungen und sonstigen Stellen der Union

(1) Eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union, die Daten aufgrund eines Verlangens nach Artikel 14 erhalten hat,

a) darf die Daten nicht in einer Weise nutzen, die mit dem Zweck, zu dem sie verlangt wurden, unvereinbar ist;

b) trifft – soweit die Verarbeitung personenbezogener Daten erforderlich ist – technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen;

c) vernichtet die Daten, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und teilt dem Dateninhaber die Vernichtung der Daten mit.

(2) Eine Offenlegung von Geschäftsgeheimnissen oder mutmaßlichen Geschäftsgeheimnissen gegenüber einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union ist nur insoweit erforderlich, wie dies für den Zweck des Verlangens unerlässlich ist. In diesem Falle trifft die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union geeignete Maßnahmen, um die Vertraulichkeit dieser Geschäftsgeheimnisse zu wahren.

Artikel 20

Ausgleich im Falle der außergewöhnlichen Notwendigkeit

(1) Werden Daten zur Bewältigung eines öffentlichen Notstands nach Artikel 15 Buchstabe a bereitgestellt, so geschieht dies kostenlos.

(2) Beantragt der Dateninhaber für die Bereitstellung von Daten nach einem Verlangen gemäß Artikel 15 Buchstaben b oder c einen Ausgleich, so darf dieser Ausgleich die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, erforderlichenfalls einschließlich der Kosten einer Anonymisierung und technischen Anpassung, zuzüglich einer angemessenen Marge, nicht übersteigen. Auf Anfrage der öffentlichen Stelle oder des Organs, der Einrichtung oder der sonstigen Stelle der Union, die bzw. das die Daten verlangt hat, übermittelt der Dateninhaber Informationen über die Grundlage für die Berechnung der Kosten und der angemessenen Marge.

Artikel 21

Beitrag von Forschungsorganisationen oder statistischen Ämtern im Zusammenhang mit außergewöhnlichen Notwendigkeiten

(1) Eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union ist berechtigt, die nach diesem Kapitel erhaltenen Daten an Personen oder Organisationen zur Durchführung wissenschaftlicher Forschungstätigkeiten oder Analysen, die mit dem Zweck, für den die Daten verlangt wurden, vereinbar sind, oder an nationale statistische Ämter und an Eurostat zur Erstellung amtlicher Statistiken weiterzugeben.

(2) Personen oder Organisationen, die Daten nach Absatz 1 erhalten, müssen gemeinnützig oder im Rahmen einer im Unionsrecht oder im Recht der Mitgliedstaaten anerkannten Aufgabe von öffentlichem Interesse handeln. Dies umfasst keine Organisationen, die dem bestimmenden Einfluss gewerblicher

Unternehmen unterliegen, wodurch diese Unternehmen einen bevorzugten Zugang zu den Forschungsergebnissen erhalten könnten.

(3) Personen oder Organisationen, die Daten nach Absatz 1 erhalten, müssen die Bestimmungen des Artikels 17 Absatz 3 und des Artikels 19 einhalten.

(4) Wenn eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union Daten nach Absatz 1 übermittelt oder bereitstellt, teilt sie dies dem Dateninhaber, von dem sie die Daten erhalten hat, mit.

Artikel 22
Amtshilfe und grenzüberschreitende Zusammenarbeit

(1) Öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union arbeiten zusammen und unterstützen sich gegenseitig bei der einheitlichen Umsetzung dieses Kapitels.

(2) Daten, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe nach Absatz 1 ausgetauscht worden sind, dürfen nicht in einer Weise genutzt werden, die mit dem Zweck, zu dem sie verlangt wurden, unvereinbar ist.

(3) Beabsichtigt eine öffentliche Stelle, von einem Dateninhaber, der in einem anderen Mitgliedstaat niedergelassen ist, die Bereitstellung von Daten zu verlangen, so teilt sie diese Absicht zunächst der in Artikel 31 genannten zuständigen Behörde des betreffenden Mitgliedstaats mit. Dies gilt auch für Zugangsverlangen von Organen, Einrichtungen und sonstigen Stellen der Union.

(4) Nach Eingang der Mitteilung nach Absatz 3 berät die betreffende zuständige Behörde die anfragende öffentliche Stelle hinsichtlich einer etwaigen Notwendigkeit der Zusammenarbeit mit öffentlichen Stellen des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, um den Verwaltungsaufwand des Dateninhabers bei der Erfüllung des Verlangens zu verringern. Die anfragende öffentliche Stelle trägt den Ratschlägen der betreffenden zuständigen Behörde Rechnung.

KAPITEL VI
WECHSEL ZWISCHEN DATENVERARBEITUNGSDIENSTEN

Artikel 23
Beseitigung von Hindernissen für einen wirksamen Wechsel zwischen Anbietern von Datenverarbeitungsdiensten

(1) Anbieter von Datenverarbeitungsdiensten treffen die in den Artikeln 24, 25 und 26 vorgesehenen Maßnahmen, damit die Kunden ihres Dienstes zu einem anderen Datenverarbeitungsdienst wechseln können, der dieselbe Dienstart abdeckt und von einem anderen Diensteanbieter erbracht wird. Anbieter von Datenverarbeitungsdiensten beseitigen insbesondere gewerbliche, technische, vertragliche und organisatorische Hindernisse, die Kunden daran hindern,

a) den Vertrag über den Dienst nach einer Kündigungsfrist von höchstens 30 Kalendertagen zu kündigen;

b) neue Verträge mit einem anderen Anbieter von Datenverarbeitungsdiensten für dieselbe Dienstart zu schließen;

c) ihre Daten, Anwendungen und anderen digitalen Vermögenswerte zu einem anderen Anbieter von Datenverarbeitungsdiensten zu übertragen;

d) die Funktionsäquivalenz des Dienstes im IT-Umfeld des bzw. der anderen Anbieter von Datenverarbeitungsdiensten, die dieselbe Dienstart abdecken, gemäß Artikel 26 aufrechtzuerhalten.

(2) Absatz 1 gilt nur für Hindernisse im Zusammenhang mit den Dienstleistungen, Verträgen oder Geschäftspraktiken des ursprünglichen Anbieters.

Artikel 24

Vertragsbedingungen für den Wechsel zwischen Anbietern von Datenverarbeitungsdiensten

(1) Die Rechte des Kunden und die Pflichten des Anbieters eines Datenverarbeitungsdienstes in Bezug auf den Wechsel zwischen Anbietern solcher Dienste werden in einem schriftlichen Vertrag eindeutig festgelegt. Unbeschadet der Richtlinie (EU) 2019/770 enthält dieser Vertrag mindestens Folgendes:

a) Klauseln, die es dem Kunden ermöglichen, auf Verlangen zu einem Datenverarbeitungsdienst zu wechseln, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, oder alle direkt oder indirekt vom Kunden erzeugten Daten, Anwendungen und digitalen Vermögenswerte auf ein System in eigenen Räumlichkeiten zu übertragen, und die insbesondere die Festlegung einer verbindlichen Übergangsfrist von höchstens 30 Kalendertagen vorsehen, in der der Datenverarbeitungsdienstleister

1. den Wechselvorgang unterstützt und – soweit technisch machbar – abschließt;

2. die uneingeschränkte Kontinuität bei der Erbringung der jeweiligen Funktionen oder Dienste sicherstellt;

b) eine vollständige Spezifizierung aller Kategorien von Daten und Anwendungen, die während des Wechsels exportierbar sind, einschließlich mindestens aller Daten, die der Kunde zu Beginn der Dienstleistungsvereinbarung importiert hat, und aller Daten und Metadaten, die vom Kunden erstellt und durch die Nutzung des Dienstes während der Diensterbringung erzeugt wurden, einschließlich mindestens der Konfigurationsparameter, Sicherheitseinstellungen, Zugangsrechte und Zugangsprotokolle des Dienstes;

c) eine Mindestfrist für den Datenabruf von mindestens 30 Kalendertagen, der nach dem Ablauf des zwischen dem Kunden und dem Diensteanbieter gemäß Absatz 1 Buchstabe a und Absatz 2 vereinbarten Übergangszeitraums beginnt.

(2) Ist der in Absatz 1 Buchstaben a und c vorgesehene verbindliche Übergangszeitraum technisch nicht machbar, so teilt der Anbieter von Datenverarbeitungsdiensten dies dem Kunden innerhalb von sieben Arbeitstagen nach der Veranlassung des Anbieterwechsels mit, wobei er die technische Undurchführbarkeit mit einem ausführlichen Bericht ordnungsgemäß begründet und einen alternativen Übergangszeitraum angibt, der sechs Monate nicht überschreiten darf. Im Einklang mit Absatz 1 wird während des in Artikel 25 Absatz 2 genannten alternativen Übergangszeitraums gegen ermäßigtes Entgelt eine uneingeschränkte Betriebskontinuität sichergestellt.

Artikel 25
Schrittweise Abschaffung der Wechselentgelte

(1) Ab dem [Datum X+ 3 Jahre] verlangen die Anbieter von Datenverarbeitungsdiensten von den Kunden für den Wechsel keine Entgelte mehr.

(2) Vom [Datum X, Tag des Inkrafttretens des Datengesetzes] bis zum [Datum X+ 3 Jahre] dürfen die Anbieter von Datenverarbeitungsdiensten von den Kunden für den Wechsel ermäßigte Entgelte verlangen.

(3) Die in Absatz 2 genannten Entgelte dürfen die dem Anbieter von Datenverarbeitungsdiensten im unmittelbaren Zusammenhang mit dem betreffenden Wechselvorgang entstehenden Kosten nicht übersteigen.

(4) Der Kommission wird die Befugnis übertragen, gemäß Artikel 38 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um einen Überwachungsmechanismus einzuführen, mit dem die Kommission die von den Anbietern von Datenverarbeitungsdiensten auf dem Markt verlangten Wechselentgelte überwachen kann, um sicherzustellen, dass die in Absatz 1 vorgesehene Abschaffung der Wechselentgelte innerhalb der in demselben Absatz festgelegten Frist erreicht wird.

Artikel 26
Technische Aspekte des Wechsels

(1) Anbieter von Datenverarbeitungsdiensten, die skalierbare und elastische Rechenressourcen betreffen, die auf Infrastrukturelemente wie Server, Netze und die für den Betrieb der Infrastruktur erforderlichen virtuellen Ressourcen beschränkt sind, die aber keinen Zugang zu den Betriebsdiensten, zur Software und zu den Anwendungen gewähren, die dort gespeichert, anderweitig verarbeitet oder auf diesen Infrastrukturelementen eingesetzt werden, stellen sicher, dass der Kunde nach dem Wechsel zu einem Dienst, der dieselbe Dienstart abdeckt und von einem anderen Anbieter von Datenverarbeitungsdiensten erbracht wird, Funktionsäquivalenz bei der Nutzung des neuen Dienstes genießt.

(2) Bei anderen als den unter Absatz 1 fallenden Datenverarbeitungsdiensten stellen die Anbieter von Datenverarbeitungsdiensten offene Schnittstellen öffentlich und kostenlos bereit.

(3) Bei anderen als den unter Absatz 1 fallenden Datenverarbeitungsdiensten gewährleisten die Anbieter von Datenverarbeitungsdiensten die Kompatibilität mit offenen Interoperabilitätsspezifikationen oder europäischen Interoperabilitätsnormen, die gemäß Artikel 29 Absatz 5 dieser Verordnung benannt werden.

(4) Bestehen für die betreffende Dienstart keine offenen Interoperabilitätsspezifikationen oder europäischen Normen nach Absatz 3, so exportiert der Anbieter von Datenverarbeitungsdiensten auf Verlangen des Kunden alle erzeugten oder gemeinsam erzeugten Daten, einschließlich der relevanten Datenformate und Datenstrukturen, in einem strukturierten, gängigen und maschinenlesbaren Format.

KAPITEL VII
SCHUTZVORKEHRUNGEN FÜR NICHT PERSONENBEZOGENE DATEN IM INTERNATIONALEN UMFELD

Artikel 27
Internationaler Zugang und internationale Übermittlung

(1) Unbeschadet des Absatzes 2 oder 3 treffen die Anbieter von Datenverarbeitungsdiensten alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen, um eine internationale Übermittlung oder einen internationalen staatlichen Zugriff zu in der Union gespeicherten nicht personenbezogenen Daten zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde.

(2) Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Anbieter von Datenverarbeitungsdiensten die Übermittlung von oder die Zugangsgewährung zu im Rahmen dieser Verordnung in der Union gespeicherten nicht personenbezogenen Daten verlangt wird, dürfen jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder eine solche Übereinkunft zwischen dem ersuchenden Drittland und einem Mitgliedstaat gestützt sind.

(3) Besteht keine solche internationale Übereinkunft und ergeht an einen Anbieter von Datenverarbeitungsdiensten ein Urteil eines Gerichts eines Drittlands oder eine Entscheidung einer Verwaltungsbehörde eines Drittlands, im Rahmen dieser Verordnung in der Union gespeicherte nicht personenbezogene Daten zu übermitteln oder Zugang dazu zu gewähren, und würde die Befolgung eines solchen Urteils oder einer solchen Entscheidung den Adressaten in Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats bringen, so erfolgt die Übermittlung dieser Daten an diese Behörde oder die Zugangsgewährung nur dann,

a) wenn das Rechtssystem des Drittlands vorschreibt, dass die Entscheidung oder das Urteil zu begründen ist und verhältnismäßig sein muss, und weiter vorsieht, dass die Entscheidung oder das Urteil eine hinreichende Bestimmtheit aufweisen muss, indem z. B. darin eine hinreichende Bezugnahme auf bestimmte verdächtige Personen oder Rechtsverletzungen erfolgt,

b) wenn der begründete Einwand des Adressaten von einem zuständigen Gericht in dem Drittland überprüft wird und

c) wenn das zuständige Gericht, das die Entscheidung oder das Urteil erlässt oder die Entscheidung einer Verwaltungsbehörde überprüft, nach dem Recht dieses Landes befugt ist, die einschlägigen rechtlichen Interessen des Bereitstellers der durch das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats geschützten Daten gebührend zu berücksichtigen.

Der Adressat der Entscheidung kann die Stellungnahme der nach dieser Verordnung zuständigen Stellen oder Behörden einholen, um festzustellen, ob diese Bedingungen erfüllt sind, insbesondere wenn er der Auffassung ist, dass die Entscheidung sensible

Geschäftsdaten betreffen oder die nationalen Sicherheits- oder Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten beeinträchtigen könnte.

Der durch die Verordnung [xxx – Daten-Governance-Gesetz] eingesetzte Europäische Dateninnovationsrat berät und unterstützt die Kommission bei der Ausarbeitung von Leitlinien für die Bewertung, ob diese Bedingungen erfüllt sind.

(4) Falls die Voraussetzungen des Absatzes 2 oder 3 erfüllt sind, stellt der Anbieter von Datenverarbeitungsdiensten aufgrund einer angemessenen Auslegung des Verlangens die zulässige Mindestmenge der darin verlangten Daten bereit.

(5) Der Anbieter von Datenverarbeitungsdiensten teilt dem Dateninhaber mit, dass ein Verlangen einer Verwaltungsbehörde eines Drittlands nach Zugang zu seinen Daten vorliegt, bevor er dem Verlangen nachkommt, außer wenn das Verlangen Strafverfolgungszwecken dient und solange dies zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahmen erforderlich ist.

KAPITEL VIII
INTEROPERABILITÄT

Artikel 28
Wesentliche Anforderungen an die Interoperabilität

(1) Betreiber von Datenräumen müssen die folgenden wesentlichen Anforderungen zur Erleichterung der Interoperabilität der Daten und der Mechanismen und Dienste für die gemeinsame Datennutzung erfüllen:

a) die Datensatzinhalte, Nutzungsbeschränkungen, Lizenzen, Datenerhebungsmethoden, Datenqualität und Unsicherheiten sind hinreichend beschrieben, um dem Empfänger das Auffinden der Daten, den Datenzugang und die Datennutzung zu ermöglichen;

b) die Datenstrukturen, Datenformate, Vokabulare, Klassifizierungssysteme, Taxonomien und Codelisten werden in einer öffentlich zugänglichen und einheitlichen Weise beschrieben;

c) die technischen Mittel für den Datenzugang, wie z. B. Anwendungsprogrammierschnittstellen, sowie ihre Nutzungsbedingungen und die Dienstqualität sind ausreichend beschrieben, um den automatischen Datenzugang und die automatische Datenübermittlung zwischen den Parteien, auch kontinuierlich oder in Echtzeit in einem maschinenlesbaren Format, zu ermöglichen;

d) es werden die Mittel bereitgestellt, mit denen die Interoperabilität intelligenter Verträge innerhalb ihrer Dienste und Tätigkeiten ermöglicht wird.

Diese Anforderungen können allgemeiner Art sein oder ganz bestimmte Sektoren betreffen, müssen aber das Zusammenspiel mit Anforderungen anderer sektorspezifischer Rechtsvorschriften der Union oder der Mitgliedstaaten in vollem Umfang berücksichtigen.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 38 delegierte Rechtsakte zur Ergänzung dieser Verordnung durch eine nähere Bestimmung der in Absatz 1 genannten wesentlichen Anforderungen zu erlassen.

(3) Bei Betreibern von Datenräumen, die den harmonisierten Normen oder Teilen davon entsprechen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, wird eine Konformität mit den in Absatz 1 genannten wesentlichen Anforderungen vermutet, soweit sich diese Normen auf diese Anforderungen erstrecken.

(4) Die Kommission kann gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen, Entwürfe für harmonisierte Normen auszuarbeiten, die den in Absatz 1 genannten wesentlichen Anforderungen genügen.

(5) Die Kommission erlässt in Bezug auf eine oder alle der in Absatz 1 festgelegten Anforderungen nötigenfalls im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen, wenn es keine harmonisierten Normen nach Absatz 4 gibt oder wenn sie der Auffassung ist, dass die einschlägigen harmonisierten Normen nicht ausreichen, um die Erfüllung der wesentlichen Anforderungen in Absatz 1 zu gewährleisten. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 39 Absatz 2 erlassen.

(6) Die Kommission kann Leitlinien mit Interoperabilitätsspezifikationen für die Funktionsweise gemeinsamer europäischer Datenräume annehmen, beispielsweise Architekturmodelle und technische Normen für die Umsetzung von Rechtsvorschriften und Vereinbarungen zwischen den Parteien, die eine gemeinsame Datennutzung fördern, z. B. im Hinblick auf Zugangsrechte und die technische Übertragung von Einwilligungen oder Genehmigungen.

Artikel 29
Interoperabilität von Datenverarbeitungsdiensten

(1) Offene Interoperabilitätsspezifikationen und europäische Normen für die Interoperabilität von Datenverarbeitungsdiensten müssen

a) leistungsbezogen darauf ausgerichtet sein, die Interoperabilität zwischen verschiedenen Datenverarbeitungsdiensten, die dieselbe Dienstart abdecken, herzustellen;

b) die Übertragbarkeit digitaler Vermögenswerte zwischen verschiedenen Datenverarbeitungsdiensten, die dieselbe Dienstart abdecken, verbessern;

c) soweit dies technisch machbar ist, die Funktionsäquivalenz zwischen verschiedenen Datenverarbeitungsdiensten, die dieselbe Dienstart abdecken, gewährleisten.

(2) Offene Interoperabilitätsspezifikationen und europäische Normen für die Interoperabilität von Datenverarbeitungsdiensten müssen Folgendes regeln:

a) die Aspekte der Cloud-Interoperabilität in Bezug auf die Transportinteroperabilität, die syntaktische Interoperabilität, die semantische Dateninteroperabilität, die verhaltensbezogene Interoperabilität und die Interoperabilität der Regeln und Vorgaben;

b) die Aspekte der Cloud-Datenübertragbarkeit in Bezug auf die syntaktische Datenübertragbarkeit, die semantische Datenübertragbarkeit und die Übertragbarkeit der Datenregeln;

c) die Aspekte der Cloud-Anwendungen in Bezug auf die syntaktische Übertragbarkeit von Anwendungen, die Übertragbarkeit von Anwendungsbefehlen, die Übertragbarkeit von Anwendungsmetadaten, die Übertragbarkeit des Anwendungsverhaltens und die Übertragbarkeit der Anwendungsregeln.

(3) Offene Interoperabilitätsspezifikationen müssen mit Anhang II Nummern 3 und 4 der Verordnung (EU) Nr. 1025/2012 übereinstimmen.

(4) Die Kommission kann gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen, Entwürfe für europäische Normen für bestimmte Dienstarten von Datenverarbeitungsdiensten auszuarbeiten.

(5) Für die Zwecke des Artikels 26 Absatz 3 dieser Verordnung wird der Kommission die Befugnis übertragen, gemäß Artikel 38 delegierte Rechtsakte zu erlassen, um die Fundstellen offener Interoperabilitätsspezifikationen und europäischer Normen für die Interoperabilität von Datenverarbeitungsdiensten im Zentralspeicher der Union für Normen für die Interoperabilität von Datenverarbeitungsdiensten zu veröffentlichen, sofern diese den Kriterien der Absätze 1 und 2 des vorliegenden Artikels genügen.

Artikel 30

Wesentliche Anforderungen an intelligente Verträge für die gemeinsame Datennutzung

(1) Der Anbieter einer Anwendung, in der intelligente Verträge verwendet werden, oder – in Ermangelung dessen – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit einer Datenbereitstellungsvereinbarung beinhaltet, muss die folgenden wesentlichen Anforderungen erfüllen:

a) Robustheit: Gewährleistung, dass der intelligente Vertrag so konzipiert wurde, dass er ein sehr hohes Maß an Robustheit bietet, um Funktionsfehler zu vermeiden und Manipulationen durch Dritte standzuhalten;

b) sichere Beendigung und Unterbrechung: Gewährleistung, dass es einen Mechanismus gibt, mit dem die weitere Ausführung von Transaktionen beendet werden kann: der intelligente Vertrag enthält interne Funktionen, mit denen der Vertrag zurückgesetzt oder angewiesen werden kann, den Betrieb zu beenden oder zu unterbrechen, um eine künftige (unbeabsichtigte) Ausführung zu vermeiden;

c) Datenarchivierung und Datenkontinuität: für den Fall, dass ein intelligenter Vertrag beendet oder deaktiviert werden muss, ist die Möglichkeit der Archivierung der Transaktionsdaten, der Logik und des Programmcodes des intelligenten Vertrags zur Aufzeichnung der in der Vergangenheit mit den Daten durchgeführten Vorgänge (Prüfbarkeit) vorzusehen; und

d) Zugriffskontrolle: ein intelligenter Vertrag muss durch strenge Zugriffskontrollmechanismen auf der Governance-Ebene und der Ebene des intelligenten Vertrags geschützt sein.

(2) Der Anbieter eines intelligenten Vertrags oder – in Ermangelung dessen – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit einer

Datenbereitstellungsvereinbarung beinhaltet, führt im Hinblick auf die Erfüllung der wesentlichen Anforderungen nach Absatz 1 eine Konformitätsbewertung durch und stellt bei Erfüllung der Anforderungen eine EU-Konformitätserklärung aus.

(3) Mit der Ausstellung der EU-Konformitätserklärung übernimmt der Anbieter einer Anwendung, in der intelligente Verträge verwendet werden, oder – in Ermangelung dessen – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit einer Datenbereitstellungsvereinbarung beinhaltet, die Verantwortung dafür, dass die Anforderungen nach Absatz 1 erfüllt sind.

(4) Bei einem intelligenten Vertrag, der den harmonisierten Normen oder Teilen davon entspricht, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, wird eine Konformität mit den in Absatz 1 genannten wesentlichen Anforderungen vermutet, soweit sich diese Normen auf diese Anforderungen erstrecken.

(5) Die Kommission kann gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen, Entwürfe für harmonisierte Normen auszuarbeiten, die den in Absatz 1 genannten wesentlichen Anforderungen genügen.

(6) Wenn es keine harmonisierten Normen nach Absatz 4 gibt oder die Kommission der Auffassung ist, dass die einschlägigen harmonisierten Normen nicht ausreichen, um die Erfüllung der wesentlichen Anforderungen in Absatz 1 in einem grenzüberschreitenden Zusammenhang zu gewährleisten, kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für die in Absatz 1 genannten wesentlichen Anforderungen erlassen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 39 Absatz 2 erlassen.

KAPITEL IX
ANWENDUNG UND DURCHSETZUNG

Artikel 31
Zuständige Behörden

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für die Anwendung und Durchsetzung dieser Verordnung verantwortlich sind. Die Mitgliedstaaten können eine oder mehrere neue Behörden einrichten oder sich auf bestehende Behörden stützen.

(2) Unbeschadet des Absatzes 1 gilt Folgendes:

a) die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständige unabhängige Aufsichtsbehörde ist bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung der vorliegenden Verordnung zuständig. Die Kapitel VI und VII der Verordnung (EU) 2016/679 finden sinngemäß Anwendung. Die Aufgaben und Befugnisse der Aufsichtsbehörden werden in Bezug auf die Verarbeitung personenbezogener Daten wahrgenommen;

b) bei besonderen sektoralen Problemen des Datenaustauschs im Zusammenhang mit der Anwendung dieser Verordnung bleibt die Zuständigkeit der Fachbehörden gewahrt;

c) die für die Anwendung und Durchsetzung des Kapitels VI dieser Verordnung zuständige nationale Behörde muss über Erfahrungen auf dem Gebiet der Daten und der elektronischen Kommunikationsdienste verfügen.

(3) Die Mitgliedstaaten sorgen dafür, dass die jeweiligen Aufgaben und Befugnisse der nach Absatz 1 benannten zuständigen Behörden eindeutig festgelegt werden und Folgendes umfassen:

a) Sensibilisierung von Nutzern und Rechtsträgern, die in den Anwendungsbereich dieser Verordnung fallen, für die Rechte und Pflichten aus dieser Verordnung;

b) Bearbeitung von Beschwerden über mutmaßliche Verstöße gegen diese Verordnung, angemessene Untersuchung des Beschwerdegegenstands und Unterrichtung des Beschwerdeführers innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung, insbesondere, wenn eine weitere Untersuchung oder eine Koordinierung mit einer anderen zuständigen Behörde notwendig ist;

c) Durchführung von Untersuchungen über Fragen der Anwendung dieser Verordnung, auch auf der Grundlage von Informationen einer anderen zuständigen Behörde oder einer sonstigen Behörde;

d) Verhängung abschreckender finanzieller Sanktionen, die auch Zwangsgelder und Geldstrafen mit Rückwirkung umfassen können, im Verwaltungsverfahren oder Einleitung von Gerichtsverfahren zur Verhängung von Geldbußen;

e) Beobachtung technischer Entwicklungen, die für die Bereitstellung und Nutzung von Daten von Bedeutung sind;

f) Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten, um die einheitliche Anwendung dieser Verordnung zu gewährleisten, einschließlich des unverzüglichen Austauschs aller relevanten Informationen auf elektronischem Wege;

g) Gewährleistung der Online-Veröffentlichung der von öffentlichen Stellen bei Notständen nach Kapitel V gestellten Datenzugangsverlangen;

h) Zusammenarbeit mit allen einschlägigen zuständigen Behörden zur Gewährleistung der Durchsetzung der Pflichten des Kapitels VI im Einklang mit anderen Rechtsvorschriften der Union und mit der Selbstregulierung, die für Anbieter von Datenverarbeitungsdiensten gelten;

i) Gewährleistung der Abschaffung von Entgelten für den Wechsel zwischen Anbietern von Datenverarbeitungsdiensten gemäß Artikel 25.

(4) Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so arbeiten die zuständigen Behörden bei der Wahrnehmung der ihnen nach Absatz 3 übertragenen Aufgaben und Befugnisse untereinander sowie gegebenenfalls auch mit der für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörde zusammen, um die einheitliche Anwendung der vorliegenden Verordnung zu gewährleisten. In solchen Fällen benennen die betreffenden Mitgliedstaaten eine koordinierende zuständige Behörde.

(5) Die Mitgliedstaaten teilen der Kommission die Namen der benannten zuständigen Behörden und ihre jeweiligen Aufgaben und Befugnisse sowie gegebenenfalls den

Namen der koordinierenden zuständigen Behörde mit. Die Kommission führt ein öffentliches Register dieser Behörden.

(6) Bei der Wahrnehmung ihrer Aufgaben und Befugnisse gemäß dieser Verordnung unterliegen die zuständigen Behörden keiner direkten oder indirekten Einflussnahme von außen und dürfen von anderen Behörden oder von privaten Stellen keine Weisungen einholen oder entgegennehmen.

(7) Die Mitgliedstaaten sorgen dafür, dass die benannten zuständigen Behörden mit den erforderlichen Mitteln ausgestattet werden, damit sie ihre Aufgaben gemäß dieser Verordnung angemessen wahrnehmen können.

Artikel 32
Recht auf Beschwerde bei einer zuständigen Behörde

(1) Unbeschadet eines anderen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs haben natürliche und juristische Personen das Recht, einzeln oder gegebenenfalls gemeinsam bei der jeweils zuständigen Behörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder ihrer Niederlassung Beschwerde einzulegen, wenn sie der Ansicht sind, dass ihre Rechte nach dieser Verordnung verletzt wurden.

(2) Die zuständige Behörde, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung.

(3) Die zuständigen Behörden arbeiten zusammen, um Beschwerden zu bearbeiten und zu lösen, und tauschen dazu unter anderem unverzüglich alle relevanten Informationen auf elektronischem Wege aus. Diese Zusammenarbeit berührt nicht das besondere Verfahren der Zusammenarbeit gemäß den Kapiteln VI und VII der Verordnung (EU) 2016/679.

Artikel 33
Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum [Datum des Geltungsbeginns der Verordnung] mit und melden ihr unverzüglich etwaige spätere Änderungen.

(3) Bei Verstößen gegen die Pflichten der Kapitel II, III und V dieser Verordnung können die in Artikel 51 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden innerhalb ihres Zuständigkeitsbereichs Geldbußen im Einklang mit Artikel 83 der Verordnung (EU) 2016/679 bis zu dem in Artikel 83 Absatz 5 der Verordnung genannten Betrag verhängen.

(4) Bei Verstößen gegen die Pflichten des Kapitels V dieser Verordnung kann die in Artikel 52 der Verordnung (EU) 2018/1725 genannte Aufsichtsbehörde innerhalb ihres Zuständigkeitsbereichs Geldbußen im Einklang mit Artikel 66 der Verordnung (EU) 2018/1725 bis zu dem in Artikel 66 Absatz 3 der Verordnung genannten Betrag verhängen.

Artikel 34
Mustervertragsbedingungen

Die Kommission erstellt und empfiehlt unverbindliche Mustervertragsbedingungen für den Datenzugang und die Datennutzung, um die Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit ausgewogenen vertraglichen Rechten und Pflichten zu unterstützen.

KAPITEL X
SUI-GENERIS-RECHT IM RAHMEN DER RICHTLINIE 1996/9/EG

Artikel 35
Datenbanken, die bestimmte Daten enthalten

Damit die Ausübung des Rechts der Nutzer auf Zugang zu solchen Daten und deren Nutzung nach Artikel 4 dieser Verordnung oder des Rechts auf Weitergabe solcher Daten an Dritte nach Artikel 5 dieser Verordnung nicht behindert wird, findet das in Artikel 7 der Richtlinie 96/9/EG festgelegte spezifische Schutzrecht sui generis keine Anwendung auf Datenbanken, die Daten enthalten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden.

KAPITEL XI
SCHLUSSBESTIMMUNGEN

Artikel 36
Änderung der Verordnung (EU) 2017/2394

Im Anhang der Verordnung (EU) 2017/2394 wird folgende Nummer angefügt:

„29. [Verordnung (EU) XXX des Europäischen Parlaments und des Rates [Datengesetz]].“

Artikel 37
Änderung der Richtlinie (EU) 2020/1828

Im Anhang der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates wird folgende Nummer angefügt:

„67. [Verordnung (EU) XXX des Europäischen Parlaments und des Rates [Datengesetz]].“

Artikel 38
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 25 Absatz 4, Artikel 28 Absatz 2 und Artikel 29 Absatz 5 wird der Kommission auf unbestimmte Zeit ab dem […] übertragen.

(3) Die Befugnisübertragung gemäß Artikel 25 Absatz 4, Artikel 28 Absatz 2 und Artikel 29 Absatz 5 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.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 25 Absatz 4, Artikel 28 Absatz 2 und Artikel 29 Absatz 5 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 Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

Artikel 39
Ausschussverfahren

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

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 40
Andere Rechtsakte der Union zur Regelung von Rechten und Pflichten in Bezug auf den Datenzugang und die Datennutzung

(1) Die besonderen Pflichten zur Bereitstellung von Daten zwischen Unternehmen, zwischen Unternehmen und Verbrauchern sowie ausnahmsweise zwischen Unternehmen und öffentlichen Stellen aus Rechtsvorschriften der Union, die bis zum [xx XXX xxx] in Kraft getreten sind, und aus darauf beruhenden delegierten Rechtsakten oder Durchführungsrechtsakten bleiben unberührt.

(2) Diese Verordnung berührt nicht die Rechtsvorschriften der Union, in denen hinsichtlich der Bedürfnisse eines Sektors, eines gemeinsamen europäischen Datenraums oder eines Gebietes von öffentlichem Interesse weitere Anforderungen festgelegt werden, insbesondere in Bezug auf

a) technische Aspekte des Datenzugangs,

b) Beschränkungen der Rechte des Dateninhabers auf Zugang zu bestimmten von Nutzern bereitgestellten Daten und auf deren Nutzung,

c) Aspekte, die über den Datenzugang und die Datennutzung hinausgehen.

Artikel 41
Bewertung und Überprüfung

Bis zum [*zwei Jahre nach dem Geltungsbeginn dieser Verordnung*] führt die Kommission eine Bewertung dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über deren wichtigste Ergebnisse. Darin wird insbesondere Folgendes bewertet:

a) andere Kategorien oder Arten von Daten, die zugänglich gemacht werden sollten,

b) der Ausschluss bestimmter Kategorien von Unternehmen als Begünstigte nach Artikel 5,

c) sonstige Situationen, die für die Zwecke des Artikels 15 eine außergewöhnliche Notwendigkeit begründen;

d) Änderungen in der Vertragspraxis der Anbieter von Datenverarbeitungsdiensten und die Frage, ob dies zu einer hinreichenden Einhaltung des Artikels 24 führt,

e) die Senkung der Entgelte, die Anbieter von Datenverarbeitungsdiensten für den Wechsel im Einklang mit der schrittweisen Abschaffung der Wechselentgelte nach Artikel 25 verlangen.

Artikel 42
Inkrafttreten und Geltungsbeginn

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

Sie gilt ab dem [12 Monate nach dem Datum des Inkrafttretens dieser Verordnung].

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident /// Die Präsidentin	*Der Präsident /// Die Präsidentin*