Europäisches Parlament
2019-2024

ANGENOMMENE TEXTE

P9_TA(2023)0069

Datengesetz

Abänderungen des Europäischen Parlaments vom 14. März 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))[1]

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

[1] Der Gegenstand wurde gemäß Artikel 59 Absatz 4 Unterabsatz 4 der Geschäftsordnung zu interinstitutionellen Verhandlungen an den zuständigen Ausschuss zurücküberwiesen (A9-0031/2023).

Abänderung 1

ABÄNDERUNGEN DES EUROPÄISCHEN PARLAMENTS*

am Vorschlag der Kommission

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[1],

nach Stellungnahme des Ausschusses der Regionen[2],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

---

* Textänderungen: Der neue bzw. geänderte Text wird durch Fett- und Kursivdruck gekennzeichnet; Streichungen werden durch das Symbol ▌ gekennzeichnet.

1 ABl. C 365 vom 23.9.2022, S. 18.

2 ABl. C 375 vom 30.9.2022, S. 112.

(1) In den letzten Jahren haben datengetriebene Technologien transformative Wirkung auf alle Wirtschaftssektoren gehabt. Insbesondere die rasche Verbreitung von Produkten, die mit dem Internet ▌ 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) ***In einem Kontext, in dem die Europäische Union eine herausragende globale Wettbewerbsposition im verarbeitenden Gewerbe innehat und ein führender Akteur in industrieller Software und Robotik ist,*** verhindern Hindernisse bei der gemeinsamen Datennutzung 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, ***der wirtschaftliche Wert von Datensätzen, die*** 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 ***(KMU)*** mangelt es häufig an digitalen Kapazitäten und Kompetenzen für die 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***, die Fragmentierung des Binnenmarktes, die durch einzelstaatliche Rechtsvorschriften entstehen könnte, zu verhindern*** und Hindernisse für einen gut funktionierenden Binnenmarkt für Daten zu beseitigen, muss ein harmonisierter Rahmen geschaffen werden, in dem festgelegt wird, wer ▌ unter welchen Bedingungen und auf welcher Grundlage berechtigt ist, ***die zugänglichen Daten zu nutzen,*** die durch ***vernetzte*** Produkte oder damit verbundene

Dienste ***erhoben, erlangt oder anderweitig*** 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 Hersteller vernetzter Produkte und die Anbieter verbundener Dienste die Produkte bzw. Dienste so gestalten müssen, dass*** die Nutzer eines ***vernetzten*** Produktes oder verbundenen Dienstes in der Union zeitnah auf die Daten zugreifen können, ***auf*** die ***von diesem Produkt aus zugegriffen werden kann oder die*** bei der ***Erbringung eines*** verbundenen Dienstes erzeugt werden, und dass diese Nutzer die Daten verwenden und auch an Dritte ihrer Wahl weitergeben können. Sie verpflichtet ***die*** Dateninhaber, die Daten ▌den Nutzern und den von ihnen benannten ***Datenempfängern*** 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 ▌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 Daten bereitstellen, ***wenn eine*** außergewöhnliche Notwendigkeit ***besteht***. 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 ***die*** Dateninhaber anerkennt oder schafft, nach der ***sie*** Daten besitzen, auf sie zugreifen oder sie verarbeiten ***dürfen***, oder dass sie ***einem*** Dateninhaber ein neues Recht auf Nutzung von Daten verleiht, ***auf die von einem vernetzten Produkt zugegriffen wird oder die bei der Erbringung eines*** verbundenen Dienstes erzeugt werden. ***Vielmehr wird mit der Verordnung anerkannt, dass Nutzer einwilligen können, den Dateninhabern die Genehmigung zum Zugriff und zur***

Nutzung von Daten zu erteilen, auf die von vernetzten Produkten zugegriffen wird oder die bei der Erbringung verbundener Dienste erzeugt werden, wobei es sich bei den Dateninhabern häufig um Hersteller handelt und die Dateninhaber mit dem Nutzer vertraglich vereinbaren können, einen oder mehrere verbundene Dienste ***zu erbringen.***

(6) Die Datenerzeugung ist ***eine Funktion der Konzeption eines vernetzten Produkts seitens des Herstellers, insbesondere des Einbaus von Sensoren und Verarbeitungssoftware in das Gerät,*** der Handlungen ***des Nutzers und – je nach den Betriebsmodalitäten – der Erbringung eines oder mehrerer verbundener Dienste. Viele vernetzte Produkte, z. B. im Bereich der zivilen Infrastruktur oder der Energieerzeugung oder im Verkehrssektor, erfassen Daten über ihre Umgebung oder ihre Interaktion mit anderen Elementen dieser Infrastruktur, ohne dass der Nutzer oder Dritte tätig werden. Solche Daten sind häufig möglicherweise nicht personenbezogen und für den Nutzer oder Dritte wertvoll, die sie nutzen können, um ihren Betrieb oder das Funktionieren eines Netzes oder Systems insgesamt zu verbessern oder sie anderen zugänglich zu machen. Dadurch*** stellen sich Fragen der Fairness in der digitalen Wirtschaft, da die ▌ Daten***, auf die von vernetzten Produkten zugegriffen wird oder die bei der Erbringung verbundener Dienste erzeugt werden,*** ein wichtiges Gut für Anschluss-, Neben- und sonstige Dienste sind. Um die wichtigen wirtschaftlichen Vorteile von Daten ▌ 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. ***Es ist jedoch auch wichtig, dass die gemeinsame Nutzung von Daten auf der Grundlage freiwilliger Vereinbarungen weiter ausgebaut wird, um die Entwicklung eines datengetriebenen Wertschöpfungswachstums europäischer Unternehmen zu fördern.***

(7) Das Grundrecht auf Schutz personenbezogener Daten wird insbesondere durch die ***Verordnungen*** (EU) 2016/679[1] und ▌ (EU) 2018/1725[2] ***des Europäischen Parlaments***

---

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

[2] ***Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen***

und des Rates gewahrt. Die Richtlinie 2002/58/EG ***des Europäischen Parlaments und des Rates***[1] 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. ***Mit dieser Verordnung sollte keine neue Rechtsgrundlage für die Verarbeitung personenbezogener Daten für irgendeine der regulierten Tätigkeiten geschaffen werden bzw. keine Änderung der Informationsanforderungen gemäß der Verordnung (EU) 2016/679 bewirkt werden. Im Fall eines Konflikts zwischen dieser Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem gemäß diesem Unionsrecht erlassenen nationalen Recht sollte das einschlägige Unionsrecht bzw. das nationale Recht über den Schutz personenbezogener Daten Vorrang haben.***

(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,

---

der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

[1] ***Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), (ABl. L 201 vom 31.7.2002, S. 37).***

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[1], die Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates[2] und die Richtlinie 93/13/EWG des Europäischen Parlaments und des Rates[3], 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 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

---

1 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).

2 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.

3 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.

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***, mit Ausnahme der Pflichten nach Artikel 3 Absatz 1,*** unberührt bleiben.

(12) Diese Verordnung ergänzt das Unionsrecht zur Festlegung von Barrierefreiheitsanforderungen für bestimmte Produkte und Dienstleistungen, insbesondere die Richtlinie (EU)2019/882[1], 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.

(13a) Mit dieser Verordnung sollen auch die Position und die Geschäftsmodelle Dritter, z. B. von Lieferanten, durch einen horizontalen Ansatz gestärkt werden. Um der besonderen Situation und Komplexität des jeweiligen Sektors Rechnung zu tragen, sollten im Anschluss an diese Verordnung sektorspezifische Rechtsvorschriften erlassen werden, z. B. für den Mobilitätsdatenraum. In diesen Rechtsvorschriften könnten weitere Regeln für das Recht der Lieferanten auf einen verbesserten oder direkten Zugang von ihren eigenen intelligenten Komponenten aus zu Daten in Bezug auf Fragen wie Qualitätsüberwachung, Produktentwicklung oder Verbesserung der Sicherheit festgelegt und die Rolle der Anbieter von Komponenten in Bezug auf vernetzte Produkte präzisiert werden.

---

[1] 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).

(13b) Diese Verordnung berührt nicht die Rechtsakte der Union und der Mitgliedstaaten zum Schutz der Rechte des geistigen Eigentums, einschließlich der Richtlinien 2001/29/EG[1], 2004/48/EG[2] und (EU) 2019/790[3] des Europäischen Parlaments und des Rates.

(14) Physische Produkte, die mittels ihrer Komponenten Daten über ihre Leistung, Nutzung oder Umgebung erlangen, erzeugen oder sammeln und die diese Daten über einen ▌elektronischen Kommunikationsdienst***, eine physische Verbindung oder ein Gerät*** übermitteln können (häufig als Internet der Dinge bezeichnet), sollten unter diese Verordnung fallen***, ausgenommen Prototypen***. Zu den elektronischen Kommunikationsdiensten gehören terrestrische Telefonnetze, Fernsehkabelnetze, Satellitennetze und Nahfeldkommunikationsnetze. Solche ***vernetzten*** Produkte ***kommen in allen Bereichen der Wirtschaft und Gesellschaft vor, darunter private, zivile oder gewerbliche Infrastrukturen,*** Fahrzeuge, ***Schiffe, Luftfahrzeuge,*** Haushaltsgeräte und Konsumgüter, Medizin- und Gesundheitsprodukte, landwirtschaftliche und industrielle Maschinen ***oder Anlagen zur Energieerzeugung und -übertragung***. Daten***, die von einem vernetzten Produkt erlangt, erzeugt oder gesammelt werden und für Dateninhaber oder Datenempfänger zugänglich sind,*** sollten ▌für den ***Eigentümer des Produkts oder einen Dritten, dem der Eigentümer des Produkts auf der Grundlage eines Miet- oder Leasingvertrags bestimmte Rechte an dem Produkt übertragen hat, stets*** zugänglich sein***. Der Eigentümer bzw. ein solcher Dritter sollte für die Zwecke*** dieser Verordnung ***als Nutzer bezeichnet werden. Diese Zugangsrechte sollten in keiner Weise die Grundrechte der betroffenen Personen, die möglicherweise mit dem vernetzten Produkt interagieren, in Bezug auf die von dem Produkt erzeugten personenbezogenen Daten ändern oder beeinträchtigen. Die Entscheidungen der Hersteller bei der Konzeption, die Anforderungen der Nutzer und gegebenenfalls die sektorspezifischen***

---

[1] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.6.2001, S. 10).

[2] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. L 157 vom 30.4.2004, S. 45).

[3] Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (ABl. L 130 vom 17.5.2019, S. 92).

Rechtsvorschriften zur Berücksichtigung sektorspezifischer Bedürfnisse und Ziele bzw. kartellrechtliche Entscheidungen sollten bestimmen, welche Daten ein vernetztes Produkt Dateninhabern oder Datenempfängern an der Verkaufsstelle zugänglich machen kann. Diese Verordnung gilt für in der Union in Verkehr gebrachte Produkte; sie gilt somit nicht für Produkte, die sich in der Entwicklungsphase befinden, wie etwa Prototypen.

(15) Dagegen sollten ***Inhalte oder Daten, die von dem vernetzten Produkt erlangt oder erzeugt werden oder auf die von dem vernetzten Produkt zugegriffen wird oder die zum Zweck der Speicherung oder Verarbeitung im Auftrag Dritter an das vernetzte Produkt übermittelt werden – wie etwa im Fall von Servern oder Cloud-Infrastrukturen, unter anderem für die Nutzung durch einen Online-Dienst –, nicht unter diese Verordnung fallen.***

(16) ***Ferner*** müssen Vorschriften für ***verbundene Dienste*** festgelegt werden, ▌die ▌so ***in ein vernetztes Produkt*** integriert oder ▌so mit ihm verbunden sind, dass das Produkt ohne ***den jeweiligen Dienst eine oder mehrere seiner*** Funktionen nicht ausführen könnte ***und die die Übermittlung von Daten zwischen dem vernetzten Produkt und dem Anbieter des verbundenen Dienstes umfassen. Wenn ein Anbieter eines verbundenen Dienstes von einem vernetzten Produkt auf Daten zugreift oder Zugang zu Daten hat, die bei der Erbringung des verbundenen Dienstes erzeugt werden, und das Recht hat, nicht personenbezogene Daten gemäß Artikel 4 Absatz 6 zu nutzen, sollte er für die Daten, auf die er von dem Produkt zugegriffen hat oder die während der Erbringung des verbundenen Dienstes erzeugt werden, als Dateninhaber gelten. Derartige verbundene Dienste können Teil des Verkaufs sein***. Diese verbundenen Dienste können selbst, unabhängig von den Datenerhebungsmöglichkeiten des ***vernetzten*** Produkts, mit dem sie verbunden sind, Daten erzeugen, die für den Nutzer von Wert sind. ***Solche Daten stellen digitalisierte Nutzerhandlungen und -vorgänge dar und sollten daher für den Nutzer zugänglich sein. Solche Daten sind potenziell wertvoll für den 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 oder die Entwicklung von Produkten oder Diensten erleichtern. Informationen, die ein Dateninhaber oder ein Datenempfänger aus nicht personenbezogenen Daten ableitet oder folgert, nachdem von dem vernetzten Produkt***

darauf zugegriffen wurde, und die nicht in den Daten enthalten sind, die bei der Erbringung eines verbundenen Dienstes erzeugt werden, sollten nicht in den Anwendungsbereich dieser Verordnung fallen. 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 eines verbundenen Dienstes notwendig ist, um den funktionalen Betrieb des vernetzten Produkts aufrechtzuerhalten, oder ob*** die Erbringung des Dienstes Teil des Kauf-, Miet- oder Leasingvertrags ist, sollte diese Verordnung Anwendung finden. ***Weder die Stromversorgung noch die Bereitstellung der Konnektivität sind nach dieser Verordnung als verbundene Dienste auszulegen.***

(17) Daten, ***auf die von einem vernetzten Produkt zugegriffen wird oder die bei der Erbringung eines*** 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, wie z. B. ***Daten über die Umgebung oder die Interaktionen des vernetzten Produkts, u. a.,*** 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 ▌vom Produkt ***auf sie zugegriffen wird, und in einem verständlichen, strukturierten, gängigen und maschinenlesbaren Format unter Berücksichtigung einschlägiger Metadaten zusammengestellt werden***; sie sollten jedoch keine Daten umfassen, die sich aus ***einer Wertschöpfung durch einen*** Softwareprozess ergeben, mit dem abgeleitete Daten ▌berechnet werden, ***wenn*** ein solcher Softwareprozess ***Geschäftsgeheimnissen und*** Rechten des geistigen Eigentums ***unterliegt***. ***Beim Zugriff auf Daten in einem verschlüsselten Format sollten dem Nutzer alle erforderlichen Mittel zur Verfügung gestellt werden, um diese Daten zu entschlüsseln und zugänglich zu machen.***

(17a) Es müssen weitere Anstrengungen unternommen werden, um die Datenwirtschaft und die Daten-Governance zu konsolidieren. Insbesondere die Verbesserung und Unterstützung der Datenkompetenz ist von entscheidender Bedeutung, damit sich Nutzer und Unternehmen der Möglichkeit bewusst und motiviert sind, im Einklang mit den einschlägigen Rechtsvorschriften Zugang zu ihren Daten anzubieten und zu

gewähren. Dies ist die Grundlage einer nachhaltigen Datengesellschaft. Die Verbreitung von Maßnahmen zur Datenkompetenz würde den Abbau digitaler Ungleichheiten mit sich bringen, dazu beitragen, die Arbeitsbedingungen zu verbessern, und letztlich die Konsolidierung und den Innovationspfad der Datenwirtschaft in der Union unterstützen. Um hochwertige Beschäftigungsmöglichkeiten zu schaffen, sollte für den Erwerb und die Entwicklung von Datenkompetenz gesorgt werden, damit Bürger und Arbeitnehmer, insbesondere Beschäftigte von Start-ups und KMU, digitale Kompetenzen erwerben können.

(18) Als Nutzer eines vernetzten Produkts sollte die juristische oder natürliche Person, z. B. ein Unternehmen***,*** ein Verbraucher ***oder eine öffentliche Stelle***, verstanden werden, die das ***vernetzte*** Produkt gekauft ▌ hat ***oder verbundene Dienste in Anspruch nimmt oder vom Eigentümer des vernetzten Produkts auf der Grundlage eines Miet- oder Leasingvertrags eine vorübergehende Genehmigung erteilt bekommen hat, das vernetzte Produkt zu nutzen oder verbundene Dienste in Anspruch zu nehmen.*** Ein solcher Nutzer trägt die Risiken und genießt die Vorteile der Nutzung des vernetzten Produkts und sollte ▌ daher berechtigt sein, aus den ***Daten, auf die von dem vernetzten Produkt zugegriffen wird und die bei der Erbringung von verbundenen Diensten erzeugt werden,*** Nutzen zu ziehen.

(18a) Der Begriff „Datenkompetenz“ bezeichnet Fähigkeiten, Kenntnisse und Verständnis, die es Nutzern, Verbrauchern und Unternehmen, insbesondere Kleinstunternehmen sowie kleinen und mittleren Unternehmen, ermöglichen, sich des potenziellen Werts der von ihnen erzeugten, produzierten und weitergegebenen Daten im Zusammenhang mit ihren in dieser Verordnung und anderen datenbezogenen EU-Verordnungen festgelegten Rechten und Pflichten bewusst zu werden. Datenkompetenz sollte über das Erlernen von Instrumenten und Technologien hinausgehen und darauf abzielen, Bürger und Unternehmen in die Lage zu versetzen, aus einem fairen Datenmarkt Nutzen zu ziehen. Es ist daher notwendig, dass die Kommission und die Mitgliedstaaten in Zusammenarbeit mit allen einschlägigen Interessenträgern die Entwicklung von Datenkompetenz in allen Bereichen der Gesellschaft und für Bürger aller Altersgruppen, einschließlich Frauen und Mädchen, fördern. Daher sollten die Union und ihre Mitgliedstaaten mehr in die allgemeine und berufliche Bildung investieren, um die Datenkompetenz zu verbreiten und dafür zu sorgen, dass die in diesem Bereich erzielten Fortschritte aufmerksam

verfolgt werden. Dementsprechend sollten die Unternehmen auch Instrumente fördern und Maßnahmen zur Sicherstellung der Datenkompetenz ihrer Beschäftigten, die mit Datenzugang, Datennutzung und Datenübermittlung zu tun haben, sowie, falls zutreffend, der Datenkompetenz anderer Personen, die in ihrem Auftrag Daten verarbeiten, treffen, wobei sie deren technisches Wissen, Erfahrung sowie allgemeine und berufliche Bildung berücksichtigen und den Nutzern oder Nutzergruppen, von denen die Daten produziert oder erzeugt werden, Rechnung tragen.

(19) In der Praxis sind nicht alle Daten, die durch ***vernetzte*** 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 ▌ vernetzte Produkte erzeugt werden. Die Nutzer sind daher nicht in der Lage, die Daten zu erlangen, die erforderlich sind, um Reparaturdienste 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 ***vernetzte*** 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***, und zwar kostenlos, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und auch zum Zwecke der Abfrage, der Nutzung oder der Weitergabe der Daten. Sofern im Unionsrecht oder in den Rechtsvorschriften der Mitgliedstaaten oder in den einschlägigen kartellrechtlichen Entscheidungen nichts anderes bestimmt ist, sollten diese Daten auf der Verarbeitungsebene zugänglich sein, und zwar auch mithilfe der in dem vernetzten Produkt enthaltenen Software, die einer Entscheidung des Herstellers bei der Konzeption vor dem Verkauf an den Nutzer unterliegt. Die Daten sollten in der Form verfügbar sein, in der sie von dem Produkt abgerufen werden können, wobei nur geringfügige Anpassungen vorgenommen werden, die erforderlich sind, um sie für Dritte nutzbar zu machen, einschließlich der zugehörigen Metadaten, die für die Interpretation und Nutzung der Daten benötigt werden. Dies macht es erforderlich, dass – wenn dies technisch möglich ist – technische Hindernisse beseitigt werden,***

damit die Nutzer ohne umfangreiche individuelle Prüfverfahren in Echtzeit auf ihre Daten zugreifen können. Um den Zugriff Dritter auf die erforderlichen Daten zu erleichtern, ist außerdem ein kostengünstiger Zugang zu Software-Tools erforderlich. Führen spätere Aktualisierungen oder Änderungen des vernetzten Produkts durch den Hersteller oder eine andere Partei zu zusätzlichen zugänglichen Daten oder zu einer Einschränkung der ursprünglich zugänglichen Daten, so sollten diese Änderungen dem Nutzer im Rahmen der Aktualisierung oder Änderung mitgeteilt werden. Mit dieser Verordnung wird keine Verpflichtung zur Speicherung zusätzlicher Daten auf der zentralen Rechnereinheit eines Produkts festgelegt, wenn dies in Bezug auf die erwartete Nutzung unverhältnismäßig wäre. Hersteller oder Dateninhaber werden dadurch nicht daran gehindert, solche Anpassungen mit dem Nutzer freiwillig zu vereinbaren.

(20) ***In Fällen eines gemeinschaftlichen Eigentums an dem vernetzten Produkt und den erbrachten verbundenen Diensten,*** wenn mehrere Personen oder Einrichtungen Eigentümer eines Produkts oder Beteiligte eines Leasing- oder Mietvertrags sind ▌, ***sollte es die*** Konzeption des ***vernetzten*** Produkts oder verbundenen Dienstes oder der entsprechenden Schnittstelle ***ermöglichen, dass*** alle Personen Zugang zu den erzeugten Daten haben. Nutzer von ***vernetzten*** Produkten, die Daten erzeugen, müssen in der Regel ein Nutzerkonto einrichten. Dies ermöglicht die Identifizierung des Nutzers durch ***einen Dateninhaber, bei dem es sich um*** den Hersteller ***handeln kann,*** sowie die Kommunikation zur Ausführung und Bearbeitung von Datenzugangsverlangen. ***Zu Zwecken der Identifizierung und Authentifizierung sollten Hersteller und Erbringer von verbundenen Diensten Nutzern die Verwendung von gemäß der Verordnung (EU) Nr. 910/2014[1] ausgestellten EUid-Brieftaschen ermöglichen.*** 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 ***einen*** Hersteller oder Dateninhaber erfordern. Dies bedeutet, dass

---

[1] ***Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).***

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. ***Nutzerkonten sollten es Nutzern ermöglichen, ihre Einwilligung in die Verarbeitung und den Austausch von Daten zurückzunehmen und die Löschung der Daten zu beantragen, die im Rahmen der Nutzung des vernetzten Produkts erzeugt werden, insbesondere, wenn der Nutzer beabsichtigt, das Eigentum an dem Produkt auf eine andere Person zu übertragen.***

(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 ***einer Cloud*** handeln ▌. ***Von Auftragsverarbeitern gemäß der Verordnung (EU) 2016/679 wird standardmäßig nicht erwartet, dass sie als Dateninhaber agieren, es sei denn, sie wurden vom Datenverantwortlichen speziell damit beauftragt.*** Die Server können 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 des beruflichen Umfelds*** und dienen als benutzerfreundliche Schnittstelle für das Abspielen von Inhalten, den Abruf von Informationen oder die Aktivierung materieller Gegenstände, die mit dem Internet ▌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 ▌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, der von einer anderen Stelle als dem Hersteller des ***vernetzten*** Produkts bereitgestellt wird, mit einem ***vernetzten*** Produkt interagiert. ▌

(23) Vor Abschluss eines ***Kaufvertrags*** für ein ***vernetztes*** Produkt ***sollte der Hersteller oder gegebenenfalls der Verkäufer dem Nutzer klare und ausreichende Informationen über die Daten bereitstellen, auf die von dem vernetzten Produkt zugegriffen werden kann, einschließlich Art, Format, Erhebungsfrequenz und der geschätzten Menge zugänglicher Daten. Dies sollte auch Informationen über Datenstrukturen, Datenformate, Vokabulare, Klassifikationssysteme, Taxonomien und Codelisten, soweit verfügbar, sowie*** Informationen darüber ***umfassen***, wie ▌die ▌Daten ***gespeichert oder abgerufen werden können bzw. wie auf sie*** zugegriffen werden kann***, einschließlich der Bereitstellung von Software Development Kits oder Anwendungsprogrammierschnittstellen, zusammen mit Beschreibungen ihrer Nutzungsbedingungen und ihrer Dienstqualität***. Diese Pflicht sorgt für Transparenz in Bezug auf die erzeugten ***zugänglichen*** Daten und verbessert den einfachen Zugang für den Nutzer. ***Die Transparenzverpflichtung könnte vom Dateninhaber beispielsweise erfüllt werden, indem er eine dauerhafte URL-Adresse im Internet unterhält, die als Weblink oder QR-Code verbreitet werden kann und unter der die relevanten Informationen eingesehen werden können. Eine solche URL-Adresse könnte dem Nutzer vom Hersteller oder gegebenenfalls vom Verkäufer bereitgestellt werden, bevor der Kaufvertrag für ein vernetztes Produkt geschlossen wird. Der Nutzer muss die Informationen in jedem Fall so speichern können, dass sie in der Folge eingesehen werden können und die unveränderte Wiedergabe der gespeicherten Informationen möglich ist.*** 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.

(23a) Verbundene Dienste sollten so erbracht werden, dass die dabei erzeugten Daten, die die digitalisierten Nutzerhandlungen und -vorgänge darstellen, standardmäßig einfach, sicher und – soweit relevant und technisch machbar – für den Nutzer kostenlos in einem strukturierten, gängigen und maschinenlesbaren Format zusammen mit den einschlägigen Metadaten, die für die Interpretation und Nutzung erforderlich sind, direkt zugänglich sind. Informationen, die durch komplexe

proprietäre Algorithmen aus diesen Daten abgeleitet oder gefolgert werden, insbesondere wenn sie die Ausgabe mehrerer Sensoren in dem vernetzten Produkt kombinieren, sollten nicht unter die Verpflichtung des Dateninhabers zur Weitergabe von Daten an Nutzer oder Datenempfänger fallen, es sei denn, es wurde eine andere Vereinbarung getroffen. Vor Abschluss einer Vereinbarung mit einem Nutzer über die Erbringung eines verbundenen Dienstes, die den Zugang des Anbieters zu Daten von dem vernetzten Produkt aus im Einklang mit Artikel 4 Absatz 6 dieser Verordnung beinhaltet, sollte der Anbieter mit dem Nutzer die Art, das Volumen, die Erhebungsfrequenz und das Format der Daten, auf die der Anbieter verbundener Dienste von dem vernetzten Produkt aus zugreift, sowie die Art und das geschätzte Volumen der bei der Erbringung des verbundenen Dienstes erzeugten Daten und gegebenenfalls die Modalitäten für den Zugang zu diesen Daten oder den Abruf derselben durch den Nutzer, einschließlich des Zeitraums, in dem diese gespeichert werden sollten, vereinbaren.

(24) Mit dieser Verordnung wird den Dateninhabern die Pflicht auferlegt, Daten unter bestimmten Umständen bereitzustellen. Soweit personenbezogene Daten verarbeitet werden, sollte ***ein*** 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 ***den Dateninhabern*** 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 ***den Dateninhabern*** ein neues Recht auf die Nutzung von Daten eingeräumt wird, ***auf*** die ***von dem vernetzten Produkt aus zugegriffen wurde oder die während der Erbringung eines*** verbundenen Dienstes erzeugt wurden. Dies gilt insbesondere dann, wenn der Hersteller ▌ 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 ***Kaufvertrags*** für das ***vernetzte*** Produkt sein. ***Der Nutzer sollte eine angemessene Gelegenheit erhalten, um diese Vereinbarung abzulehnen. Sollte ein Nutzer die Vertragsbedingungen ablehnen, so darf dies den Nutzer nicht***

daran hindern, das betreffende Produkt des Dienstes zu nutzen, es sei denn, das Produkt des Dienstes kann ohne die Annahme der Vertragsbedingungen durch den Nutzer nicht funktionieren. Jede Vertragsbedingung in der Vereinbarung, nach der ***ein*** 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 ***ein*** 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 ***einen*** 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 ***einen*** Dateninhaber aus genau festgelegten Gründen der öffentlichen Ordnung ausschließen oder einschränken würden.

(24a) Für Unternehmen ist es derzeit oft schwierig, die Personal- oder EDV-Kosten zu rechtfertigen, die für die Aufbereitung nicht personenbezogener Datensätze oder Datenprodukte und deren Angebot an potenzielle Gegenparteien über Datenmarktplätze, einschließlich Datenvermittlungsdiensten im Sinne der Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates[1], erforderlich sind. Ein wesentliches Hindernis für die Weitergabe nicht personenbezogener Daten durch Unternehmen ergibt sich daher aus der fehlenden Vorhersehbarkeit des wirtschaftlichen Ertrags von Investitionen in die Aufbereitung und Bereitstellung von Datensätzen oder Datenprodukten. Damit in der Union liquide, effiziente und faire Märkte für nicht personenbezogene Daten entstehen können, muss geklärt werden, welche Partei das Recht hat, solche Daten auf einem Marktplatz anzubieten. Nutzer sollten daher das Recht haben, nicht personenbezogene Daten zu kommerziellen und nicht kommerziellen Zwecken an Datenempfänger weiterzugeben. Eine solche Datenweitergabe könnte direkt durch den Nutzer, auf Anfrage des Nutzers über einen Dateninhaber oder durch Datenvermittlungsdienste erfolgen. Datenvermittlungsdienste im Sinne der Verordnung (EU) 2022/868 könnten eine Datenwirtschaft fördern, indem sie Geschäftsbeziehungen zwischen Nutzern, Datenempfängern und Dritten herstellen

---

[1] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) (ABl. L 152 vom 3.6.2022, S. 1).

und die Nutzer bei der Ausübung ihres Datennutzungsrechts unterstützen, z. B. indem sie die ordnungsgemäße Anonymisierung der Daten oder die Aggregation des Zugangs zu Daten von einer Vielzahl einzelner Nutzer sicherstellen. Um die Anreize für Nutzer zur Monetarisierung nicht personenbezogener Daten von vernetzten Produkten, deren Eigentümer sie sind, zu schützen, sollten Dateninhaber nur die aggregierten Datensätze von einer Vielzahl von Nutzern monetarisieren können und sie sollten Dritten nicht personenbezogene Daten, auf die sie von dem vernetzten Produkt aus zugreifen, nicht für andere kommerzielle oder nicht kommerzielle Zwecke als die Erfüllung ihrer vertraglichen Verpflichtungen gegenüber dem Nutzer zur Verfügung stellen. Gleichzeitig sollte es den Dateninhabern, wenn sie mit den Nutzern vertraglich das Recht zur Nutzung solcher Daten vereinbart haben, freistehen, diese für eine Vielzahl von Zwecken zu verwenden, einschließlich der Verbesserung der Funktionsweise des vernetzten Produkts oder der verbundenen Dienste, der Entwicklung neuer Produkte oder Dienste oder der Anreicherung, Manipulation oder Zusammenführung dieser Daten mit anderen Daten, auch mit dem Ziel, den sich daraus ergebenden Datensatz Dritten zur Verfügung zu stellen, solange der abgeleitete Datensatz es nicht ermöglicht, einzelne Datenelemente zu ermitteln, auf die der Dateninhaber von dem vernetzten Produkt aus zugreift, und es Dritten nicht ermöglicht, diese Datenelemente ohne erheblichen Aufwand aus dem Datensatz abzuleiten.

(24b) Erzeugen Produkte Daten, die durch komplexe proprietäre Algorithmen – einschließlich jener, die Bestandteil einer proprietären Software im Sinne der Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates[1] sind – aus anderen von dem vernetzten Produkt erzeugten Daten abgeleitet oder gefolgert werden, so sollten diese Daten nicht in den Anwendungsbereich dieser Verordnung fallen und daher auch nicht der Verpflichtung eines Dateninhabers unterliegen, sie einem Nutzer oder Datenempfänger zur Verfügung zu stellen, es sei denn, der Nutzer und der Dateninhaber haben etwas anderes vereinbart. Zu diesen Daten sollten insbesondere Informationen gehören, die durch Sensorfusion gewonnen werden, bei der Daten von mehreren Sensoren abgeleitet oder gefolgert werden, die in dem vernetzten Produkt unter Verwendung komplexer proprietärer Algorithmen

---

*[1] **Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen (ABl. L 111 vom 5.5.2009, S. 16).***

gesammelt werden. Daten, die aus der Verarbeitung von Rohdaten, die von einem einzelnen Sensor oder einer Gruppe von miteinander verbundenen Sensoren gesammelt wurden, abgeleitet oder gefolgert werden, um die gesammelten Daten für vielfältigere Anwendungsfälle verständlich zu machen, indem eine physikalische Größe oder Qualität oder die Veränderung einer physikalischen Größe wie Temperatur, Druck, Durchflussmenge, pH-Wert, Flüssigkeitsstand, Position, Beschleunigung oder Geschwindigkeit bestimmt wird, sollten hingegen in die Verpflichtung der Dateninhaber, den Nutzern und Datenempfängern Daten zur Verfügung zu stellen, aufgenommen werden. In sektorspezifischen Rechtsvorschriften sollten zugängliche Daten auf der Grundlage der Besonderheiten des betreffenden Sektors genauer definiert werden.

(24c) Um das Entstehen liquider, fairer und effizienter Märkte für nicht personenbezogene Daten zu fördern, sollten die Nutzer vernetzter Produkte Daten grundsätzlich mit minimalem rechtlichem und technischem Aufwand, auch für kommerzielle Zwecke, an andere weitergeben können. Vor der Weitergabe von Daten sollte ein Nutzer ein hohes Maß an Sicherheit dahingehend haben, dass er nicht mit nachteiligen rechtlichen Folgen rechnen muss, wenn er die Daten weitergegeben hat. Sind Daten von der Verpflichtung eines Dateninhabers, sie den Nutzern oder Datenempfängern zur Verfügung zu stellen, ausgenommen, so sollte der Umfang dieser Daten daher in der vertraglichen Vereinbarung zwischen dem Nutzer und dem Dateninhaber über die Erbringung eines verbundenen Dienstes in einem verständlichen und klaren Format so festgelegt werden, dass die Nutzer leicht feststellen können, welche Daten ihnen für die Weitergabe an Datenempfänger oder Dritte ohne weitere Verpflichtungen zum Schutz dieser Daten zur Verfügung stehen.

(24d) Es gibt viele Gründe dafür, dass bestimmte Daten, die durch die Verwendung eines Produkts erzeugt werden, für einen Dateninhaber unzugänglich bleiben und daher nicht den Pflichten zur Datenweitergabe nach Kapitel II unterliegen. Möglicherweise sind die Daten sehr volatil (mit hoher Frequenz aufgezeichnete Werte) und werden entweder sofort oder rasch überschrieben. Sie werden möglicherweise nur für die Aktivierung einer sehr spezifischen Funktion, wie z. B. der Aktivität von Scheibenwischern oder Scheinwerfern, erhoben, und es gibt derzeit keinen Anwendungsfall und das Produkt ist nicht dafür konzipiert, dass solche Daten in dem Produkt gespeichert werden, und zwar aufgrund der Kosten für die Speicherung

solcher Daten und die Verbindung des datenerfassenden Sensors mit einer zentralen Rechenkomponente, aus der Daten exportiert werden könnten, sowie aufgrund der Konnektivitätskosten für die Datenübertragung bei erheblichem Datenvolumen. In diesem Zusammenhang sollte in sektorspezifischen Vorschriften die Relevanz zugänglicher Daten entsprechend ihren Besonderheiten weiter präzisiert werden, um die Verfügbarkeit zumindest solcher Daten sicherzustellen, die für die Reparatur oder Wartung der vernetzten Produkte und verbundenen Dienste wesentlich sind.

(25) In konzentrierten Sektoren, in denen die Endnutzer durch eine kleine Zahl von Herstellern ***oder Anbietern verbundener Dienste*** versorgt werden, ***ist die Möglichkeit der Nutzer, über den Zugang zu Daten zu verhandeln, die von dem vernetzten Produkt übertragen oder bei der Erbringung verbundener Dienste erzeugt werden, aufgrund der Verhandlungsmacht des Herstellers oder des Anbieters verbundener Dienste begrenzt.*** Unter solchen Umständen reichen vertragliche Vereinbarungen möglicherweise nicht aus, um das Ziel der Stärkung der Handlungsfähigkeit der Nutzer zu erreichen. Die Daten verbleiben in der Regel unter der Kontrolle der Hersteller ***oder der Anbieter verbundener Dienste***, was es den Nutzern erschwert, aus den Daten, die sie mit den ***in ihrem Besitz befindlichen*** 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***, Sicherheitsbedenken*** und Zielen Rechnung zu tragen. Darüber hinaus ***sollten*** Dateninhaber ***Daten, auf die von dem vernetzten Produkt aus zugegriffen wurde oder die bei der Erbringung verbundener Dienste erzeugt wurden,*** 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 zu 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 ***vernetzter Produkte*** oder ***eines*** verbundenen Dienstes, ***die*** bzw. der Daten ***erzeugen bzw.*** erzeugt, ***gilt das EU-Verbraucherrecht, wie die Richtlinie 2005/29/EG, die gegen unfaire Geschäftspraktiken Anwendung findet, und*** die Richtlinie 93/13/EWG findet auf die Vertragsklauseln Anwendung, damit ein Verbraucher keinen missbräuchlichen Vertragsklauseln unterliegt. Bei missbräuchlichen Vertragsklauseln, die ▌einseitig auferlegt werden, sieht diese Verordnung vor, dass diese missbräuchlichen Klauseln für das betreffende Unternehmen unverbindlich sein sollten.

(27) ***Die*** Dateninhaber ***können*** 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, ***sollten die*** 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 ***Datenempfänger***, der einen anschließenden Dienst anbietet, der möglicherweise mit einem ***von einem*** Dateninhaber bereitgestellten Dienst im Wettbewerb steht, oder die Anweisung hierzu an den Dateninhaber. ***Das Verlangen sollte auch unabhängig davon gültig sein, ob es vom Nutzer oder von einem bevollmächtigten Dritten gestellt wird, der im Namen des Nutzers handelt, beispielsweise von einem bevollmächtigten Datenvermittlungsdienst im Sinne der Verordnung (EU) 2022/868. Die*** Dateninhaber ***sollten*** sicherstellen, dass die ***einem Datenempfänger*** bereitgestellten Daten so genau, vollständig, zuverlässig, relevant und aktuell sind wie die bei der Nutzung des ***vernetzten*** 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 ***in vollem Umfang*** 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 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. ***Weitere rechtmäßige Zwecke in diesem Zusammenhang sind das Reverse Engineering, sofern dies gemäß der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates[1] als rechtmäßiges Mittel zum unabhängigen Erwerb von Know-how oder Informationen zulässig ist und dies nicht zu unlauterem Wettbewerb führt sowie die Verpflichtung, kein konkurrierendes Produkt unter Verwendung der im Rahmen dieser Verordnung erhaltenen Daten zu entwickeln, unberührt lässt. Dies kann für die Zwecke der Reparatur oder der Verlängerung der Lebensdauer eines Produkts oder der Erbringung von Anschlussdiensten für vernetzte Produkte der Fall sein, wenn der Hersteller oder Anbieter verbundener Dienste die Produktion bzw. Erbringung eingestellt hat.***

(28a) Die vorliegende Verordnung sollte so ausgelegt werden, dass der Schutz von Geschäftsgeheimnissen gemäß der Richtlinie (EU) 2016/943 gewahrt bleibt. Zu diesem Zweck sollten Dateninhaber dem Nutzer oder vom Nutzer ausgewählten Dritten die Wahrung der Vertraulichkeit von Daten, die als Geschäftsgeheimnisse gelten, vorschreiben können. Geschäftsgeheimnisse sollten vor der Offenlegung bestimmt werden. Dateninhaber dürfen jedoch das Recht der Nutzer, Zugang zu den Daten und deren Verwendung gemäß dieser Verordnung anzufordern, nicht auf der Grundlage bestimmter Daten untergraben, die der Dateninhaber als Geschäftsgeheimnisse betrachtet. Der Dateninhaber oder, wenn es sich dabei nicht

---

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

um den Dateninhaber handelt, der Träger des Geschäftsgeheimnisses sollte die Möglichkeit haben, mit dem Nutzer oder vom Nutzer ausgewählten Dritten geeignete Maßnahmen zur Wahrung ihrer Vertraulichkeit zu vereinbaren, unter anderem durch die Verwendung von Mustervertragsbedingungen, Vertraulichkeitsvereinbarungen, strengen Zugangsprotokollen, technischen Standards und der Anwendung von Verhaltenskodizes. In Fällen, in denen der Nutzer bzw. die von ihm ausgewählten Dritten diese Maßnahmen nicht umsetzen oder die Vertraulichkeit von Geschäftsgeheimnissen untergraben, sollte der Dateninhaber die Weitergabe von als Geschäftsgeheimnisse eingestuften Daten bis zur Überprüfung durch den Datenkoordinator des jeweiligen Mitgliedstaats aussetzen können. In solchen Fällen sollte der Dateninhaber dem Datenkoordinator des Mitgliedstaats, in dem er gemäß Artikel 31 dieser Verordnung niedergelassen ist, unverzüglich mitteilen, dass er die Weitergabe der Daten ausgesetzt hat, und angeben, welche Maßnahmen nicht umgesetzt wurden oder bei welchen Geschäftsgeheimnissen gegen die Vertraulichkeit verstoßen wurde. Möchte der Nutzer oder ein von ihm ausgewählter Dritter die Entscheidung des Dateninhabers, die Weitergabe der Daten auszusetzen, anfechten, so sollte der Datenkoordinator innerhalb einer angemessenen Frist entscheiden, ob die Weitergabe der Daten wieder aufgenommen werden sollte, und gibt, falls dies der Fall ist, an, unter welchen Bedingungen sie wieder aufgenommen wird. Die Kommission sollte mit Unterstützung des Europäischen Dateninnovationsrats Mustervertragsbedingungen ausarbeiten und in der Lage sein, technische Normen auszuarbeiten. Die Kommission könnte mit Unterstützung des Europäischen Innovationsrats auch die Aufstellung von Verhaltenskodizes in Bezug auf den Schutz von Geschäftsgeheimnissen oder die Wahrung von Rechten des geistigen Eigentums beim Umgang mit Daten fördern, um zur Verwirklichung des Ziels dieser Verordnung beizutragen.

(29) Ein ***Datenempfänger***, dem Daten bereitgestellt werden, kann ***eine natürliche oder juristische Person,*** ein Unternehmen, eine Forschungseinrichtung***,*** eine gemeinnützige Organisation ***oder ein Vermittler*** sein***, einschließlich Datenvermittlungsdiensten oder datenaltruistischer Organisationen gemäß der Verordnung (EU) 2022/868***. Wenn ▌Dateninhaber ***einem Datenempfänger*** die Daten ***bereitstellen***, ***sollten sie ihre*** Position nicht missbrauchen, um einen Wettbewerbsvorteil auf Märkten zu erlangen, auf denen ***ein*** Dateninhaber und ***ein Datenempfänger*** möglicherweise in direktem

Wettbewerb stehen. ▌Dateninhaber ***sollten*** die ***Daten, auf die von dem vernetzten Produkt zugegriffen wurde oder die bei der Erbringung eines verbundenen Dienstes erzeugt wurden,*** 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. ***Der Nutzer sollte das Recht haben, nicht personenbezogene Daten zu kommerziellen Zwecken an Dritte weiterzugeben. Nach Zustimmung des Nutzers und vorbehaltlich der Bestimmungen dieser Verordnung sollten Datenempfänger die vom Nutzer eingeräumten Datenzugangsrechte auf Dritte übertragen können, auch gegen Entgelt. Datenvermittlungsdienste [im Sinne der Verordnung (EU) 2022/868] können Nutzer oder Datenempfänger beim Aufbau einer Geschäftsbeziehung für einen rechtmäßigen Zweck auf der Grundlage von Daten, die in den Anwendungsbereich dieser Verordnung fallen, unterstützen. Sie könnten eine entscheidende Rolle bei der Aggregation des Zugangs zu Daten einer großen Anzahl potenzieller einzelner Datennutzer spielen, sodass Big-Data-Analysen oder maschinelles Lernen erleichtert werden können, solange diese Nutzer die volle Kontrolle darüber behalten, ob sie ihre Daten zu einer solchen Aggregation beisteuern und unter welchen kommerziellen Bedingungen ihre Daten verwendet werden.***

(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[1]. 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

[1] ABl. L 303 vom 28.11.2018, S. 59.

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.

(31) Daten, ***auf die von einem vernetzten Produkt zugegriffen wird*** oder ***die bei der Erbringung eines damit*** 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. In diesem Artikel ist vorgesehen, 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 ***Datenempfänger*** alle Daten bereitzustellen, ***auf die von dem vernetzten Produkt aus zugegriffen wird oder die bei der Erbringung eines*** 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 sichergestellt. Außerdem ***können die 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 ***Datenempfängern***, nicht aber vom Nutzer zu tragen sind. 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 Dateninhaber oder ***Datenempfänger*** 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 ***Datenempfänger***, denen die Daten auf Verlangen des Nutzers bereitgestellt wurden, die Daten nur für die mit dem Nutzer vereinbarten Zwecke verarbeiten und sie ***nicht*** an andere Dritte weitergeben, ***ohne den Nutzer rechtzeitig unmissverständlich zu informieren und seine ausdrückliche Zustimmung zu einer solchen Weitergabe zu haben.***

(34) ***Datenempfänger sollten*** nur auf solche zusätzlichen Informationen zugreifen, die für die Erbringung des vom Nutzer gewünschten Dienstes erforderlich sind. Nachdem der ***Datenempfänger*** 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 des ***Datenempfängers*** zu den Daten zu verweigern oder zu beenden, wie es für ihn ist, den Zugang zu den Daten zu erlauben. ***Ein Datenempfänger oder Dateninhaber*** sollte ***die Ausübung der Rechte oder Wahlmöglichkeiten der Nutzer nicht unangemessen erschweren, auch nicht, indem er ihnen Wahlmöglichkeiten auf nicht neutrale Weise anbietet, oder*** den Nutzer in irgendeiner Weise zwingen, täuschen oder manipulieren, ***oder*** indem er – auch mittels einer digitalen Schnittstelle ***oder eines Teils davon, einschließlich ihrer Struktur, Gestaltung, Funktion oder Art der Bedienung*** – die Autonomie, Entscheidungsfähigkeit oder freie Wahlmöglichkeiten des Nutzers untergräbt und beeinträchtigt. In diesem Zusammenhang sollten Dritte ***oder Dateninhaber*** 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 ***und Dateninhaber*** sollten ihren Pflichten nach dem einschlägigen Unionsrecht nachkommen, ***einschließlich*** der Anforderungen der Richtlinie 2005/29/EG, der Richtlinie 2011/83/EU, der Richtlinie 2000/31/EG und der Richtlinie 98/6/EG.

(35) ***Dateninhaber und Datenempfänger*** 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, ***personenbezogene*** Daten zu löschen, wenn diese für den mit dem Nutzer vereinbarten Zweck nicht mehr erforderlich sind, ergänzt das Recht der betroffenen Person auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679. Wenn ***ein Datenempfänger*** ein Anbieter eines Datenvermittlungsdienstes im Sinne der ***Verordnung (EU) 2022/868*** 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, ***KMU*** 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 (EU) 2022/1925 des Europäischen Parlaments und des Rates***[1]

---

[1] ***Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (OJ L 265, 12.10.2022, p. 1).***

zielt darauf ab, diese Ineffizienzen und Ungleichgewichte zu beheben, indem die Kommission einen Anbieter als „Torwächter“ benennen kann und diesen benannten Torwächtern 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 (EU) 2022/1925*** 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 Torwächter-Unternehmen ein Datenzugangsrecht einzuräumen. Dies bedeutet, dass ein als Torwächter 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 ***der Verordnung (EU) 2022/1925*** als Torwächter 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 Torwächter bereitstellen. Beispielsweise darf der Dritte keinen Torwächter mit der Erbringung des Dienstes beauftragen. Dies hindert Dritte jedoch nicht daran, Datenverarbeitungsdienste in Anspruch zu nehmen, die von einem benannten Torwächter angeboten werden. Dieser Ausschluss benannter Torwächter vom Anwendungsbereich des Zugangsrechts nach dieser Verordnung hindert diese Unternehmen nicht daran, Daten auf andere rechtmäßige Weise zu erlangen.

(37) ***Kleinst- und Kleinunternehmen sollten von den*** Pflichten ***im Sinne des Kapitels II ausgenommen 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 ▌Vorschriften 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) ***In Vereinbarungen über die Bereitstellung von Daten sollte unabhängig davon, ob es sich um große Unternehmen oder Kleinstunternehmen, kleine oder mittlere Unternehmen handelt, nicht zwischen vergleichbaren Kategorien von Datenempfängern unterschieden werden.*** 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 ***in der Verantwortung des Dateninhabers liegen***, nachzuweisen, dass eine Vertragsbedingung nicht diskriminierend ist. ***Die Kommission sollte unter Einbeziehung aller betroffenen Interessenträger konkrete Leitlinien dafür festlegen, was unter nichtdiskriminierenden Bedingungen zu verstehen ist.*** Es ist keine rechtswidrige Diskriminierung, wenn der Dateninhaber für die Bereitstellung von Daten unterschiedliche Vertragsbedingungen 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 ***und Bereitstellung*** wertvoller Daten zu schaffen, einschließlich Investitionen in einschlägige technische Instrumente, enthält diese Verordnung den Grundsatz, dass ***Dateninhaber*** eine angemessene

Gegenleistung verlangen können, wenn sie rechtlich verpflichtet sind, dem Datenempfänger ***im Rahmen von Geschäftsbeziehungen zwischen Unternehmen*** Daten bereitzustellen. Diese Bestimmungen sollten nicht als Bezahlung für die Daten selbst verstanden werden, sondern ***dafür, dass den Dateninhabern eine angemessene Vergütung für die Bereitstellung der Daten gewährt wird, oder,*** im Falle von Kleinstunternehmen, kleinen und mittleren Unternehmen ***und Forschungseinrichtungen, die die Daten gemeinnützig nutzen,*** als Ausgleich für die ***unmittelbaren*** Kosten und die Investitionen, die für die Bereitstellung der Daten erforderlich sind. ***Die Kommission sollte Leitlinien ausarbeiten, in denen ausführlich dargelegt wird, was in der Datenwirtschaft als angemessene Gegenleistung gilt.***

(42a) Eine derartige angemessene Gegenleistung kann zum einen die Kosten und, außer bei Kleinst- und Kleinunternehmen, die Investitionen umfassen, die für die Bereitstellung der Daten erforderlich sind. Dazu können technische Kosten gehören, beispielsweise Kosten, die für die Reproduktion, die elektronische Verbreitung und die Speicherung von Daten erforderlich sind, nicht aber die Kosten der Datensammlung oder -produktion. Technische Kosten könnten auch die Kosten für die Verarbeitung, die für die Bereitstellung der Daten erforderlich ist, umfassen. Die Kosten im Zusammenhang mit der Bereitstellung der Daten können auch die Kosten für die Erleichterung konkreter Anfragen zur gemeinsamen Datennutzung umfassen. Sie können sich auch in Abhängigkeit von den für die Bereitstellung der Daten getroffenen Vereinbarungen unterscheiden. Langfristige Vereinbarungen zwischen Dateninhabern und Datenempfängern, z. B. über ein Abonnementmodell oder die Verwendung von intelligenten Verträgen, könnten die Kosten im Rahmen regelmäßiger oder wiederholter Transaktionen in einer Geschäftsbeziehung senken. Die Kosten im Zusammenhang mit der Bereitstellung von Daten sind entweder anfragespezifisch oder decken mehrere Anfragen ab. Im letzteren Fall sollte nicht ein einzelner Datenempfänger die Kosten für die Bereitstellung der Daten in voller Höhe tragen. Ein angemessener Ausgleich kann, außer bei Kleinst- und Kleinunternehmen, zweitens eine Marge umfassen. Diese Marge kann in Abhängigkeit von den Faktoren, die mit den Daten selbst im Zusammenhang stehen, z. B. mit der Menge, dem Format oder der Art der Daten, oder in Abhängigkeit von Angebot und Nachfrage nach den Daten unterschiedlich sein. In der Marge können die Kosten für die Erhebung der Daten berücksichtigt sein. Daher kann sich die

Marge verringern, wenn der Dateninhaber die Daten für sein eigenes Unternehmen erhoben hat, ohne wesentliche Investitionen zu tätigen, oder sie kann sich erhöhen, wenn die Investitionen in die Datenerhebung für die Zwecke des Unternehmens des Dateninhabers umfangreich sind. Die Marge kann auch von der Folgenutzung der Daten durch den Datenempfänger abhängig sein. In Fällen, in denen sich die Nutzung der Daten durch den Datenempfänger nicht auf die eigenen Tätigkeiten des Dateninhabers auswirkt, kann die Marge eingeschränkt oder sogar ausgeschlossen werden. Auch durch die Tatsache, dass die Daten von einem vernetzten Produkt im Besitz des Nutzers miterzeugt werden, könnte sich die Höhe der Gegenleistung im Vergleich zu anderen Fällen, in denen die Daten vom Dateninhaber erzeugt werden, zum Beispiel bei der Erbringung eines verbundenen Dienstes, verringern.

(43) In ***hinreichend*** 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. ***Dieselbe Regelung sollte für Forschungseinrichtungen gelten, die die Daten gemeinnützig nutzen.***

(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. ***Der***

Dateninhaber sollte, wenn er kein KMU ist, aktiv die Berechnung vorlegen, aus der hervorgeht, dass sein Preis kostenbasiert ist, wenn er weiß oder hätte wissen müssen, dass seine Gegenpartei ein KMU ist. In jedem Fall sollte er erklären, dass er verpflichtet ist, einem KMU die Daten zum Selbstkostenpreis und auf Anfrage ausführliche Informationen zur Verfügung zu stellen.

(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. ***Im Falle der missbräuchlichen Nutzung oder der Offenlegung von Daten sollte der Datenempfänger für den Schaden haftbar gemacht werden, der der betroffenen Partei entstanden ist, und sollte den Anfragen des Dateninhabers unverzüglich nachkommen.***

(47) Transparenz ist ein wichtiger Grundsatz, um sicherzustellen, dass die ***von einem*** Dateninhaber verlangte Gegenleistung angemessen ist oder, falls es sich bei dem Datenempfänger um ein ***KMU*** 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 ***die*** Datenempfänger beurteilen und überprüfen ***können***, 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. ***Die Streitbeilegungsstellen sollten jährliche Tätigkeitsberichte öffentlich zugänglich machen.***

(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. ▌ . Dies betrifft Situationen ohne Verhandlungsspielraum, in denen eine Partei eine bestimmte Vertragsklausel einbringt und das ***andere Unternehmen*** den Inhalt dieser Klausel trotz Verhandlungsversuchs nicht beeinflussen kann. Eine Vertragsklausel, die lediglich von einer Partei eingebracht und von ***dem anderen Unternehmen*** akzeptiert wird, oder eine Klausel, die zwischen den Vertragsparteien ausgehandelt und anschließend in geänderter Weise vereinbart wird, sollte nicht als einseitig auferlegt gelten. ***Alle vertraglichen Vereinbarungen***

sollten mit den Grundsätzen der Fairness, Angemessenheit und Nichtdiskriminierung (FRAND) im Einklang stehen.

(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 ***oder die das Unternehmen derzeit erhebt oder zuvor erhoben, gesammelt oder anderweitig generiert hat und die es zum Zeitpunkt der Anfrage aufbewahrt,*** 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 ***und vorbehaltlich der in dieser Verordnung oder in einem anderen Rechtsakt der Union oder der Mitgliedstaaten festgelegten Bedingungen*** 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 ***in Situationen, die keinen Notstand darstellen,*** entstehen, wenn eine öffentliche Stelle nachweisen kann, dass die Daten ***zur Erfüllung einer bestimmten, im nationalen Recht ausdrücklich vorgesehenen und festgelegten Aufgabe im öffentlichen Interesse*** erforderlich sind, ***wie z.B. die Verhütung oder Unterstützung bei der Bewältigung*** eines öffentlichen Notstands. Ein solcher Antrag kann nur gestellt werden, wenn ▌die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union ***bestimmte Daten ermittelt hat, die nicht verfügbar sind, und nur, wenn sie alle folgenden drei*** alternativen Mittel ***zur Erlangung von Daten ausgeschöpft hat: Anforderung*** der Daten ***durch freiwillige Vereinbarungen; Erwerb der Daten auf dem Markt oder Rückgriff auf bestehende Verpflichtungen zur Bereitstellung von Daten.***

(59) Diese Verordnung sollte weder für freiwillige Vereinbarungen über den Austausch von ***nicht personenbezogenen*** Daten zwischen privaten und öffentlichen Stellen gelten noch ihnen vorgreifen. ▌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 für Rechtssicherheit zu sorgen 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 ***auf Unionsrecht oder dem Recht der Mitgliedstaaten basieren und*** hinsichtlich ihres Umfangs und ihrer Granularität ***spezifisch,*** 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 ***und einer angemessenen Koordinierung*** sollten Datenverlangen, die von öffentlichen Stellen und von Organen, Einrichtungen oder sonstigen Stellen der Union gestellt werden, unverzüglich von der die Daten verlangenden Stelle ***an den Datenkoordinator des Mitgliedstaats übermittelt*** werden, ***der dafür sorgt, dass diese Verlangen in eine öffentliche im Internet zugängliche Liste aller Verlangen aufgenommen werden, die durch eine außergewöhnliche Notwendigkeit gerechtfertigt 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 ***sollten*** die ***Verordnung (EU) 2022/868 und*** die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates[1] 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. ***Sofern nach Unionsrecht oder dem Recht der Mitgliedstaaten zulässig, sollten öffentliche*** Stellen 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, ***und zwar unter der Voraussetzung, dass der Dateninhaber zeitnah informiert wird und alle Stellen dieselben Transparenzregeln einhalten wie diejenige, die die Daten ursprünglich angefordert hat, und für den Schutz von Geschäftsgeheimnissen und die Wahrung der Rechte des geistigen Eigentums gesorgt ist.***

(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

---

[1] 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).

Organ, einer anderen Einrichtung oder sonstigen Stelle der Union zu demselben Zweck eingereichten Verlangen ähnlich oder gleich ist***, oder wenn der Dateninhaber die verlangten Daten derzeit nicht erhebt oder im Vorfeld nicht erhoben, erhalten oder anderweitig generiert hat und sie zum Zeitpunkt des Verlangens nicht speichert***. Ein Dateninhaber, 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 96/9/EG des Europäischen Parlaments und des Rates[1] 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.

(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. 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. ***Die öffentlichen Stellen und die Organe, Einrichtungen oder sonstigen Stellen der Union sollten unter anderem durch die Anwendung verhältnismäßiger Sicherheitsmaßnahmen, gegebenenfalls im Einklang mit dem Unionsrecht und dem nationalen Recht, dafür sorgen, dass die Daten geschützt bleiben und ein unbefugter Zugriff verhindert wird.***

(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 angefordert wurden, so sollte dem Dateninhaber ***oder dem Träger des***

---

[1] 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).

Geschäftsgeheimnisses im Voraus die Vertraulichkeit dieser Informationen zugesichert werden***, gegebenenfalls auch durch die Verwendung von Mustervertragsbedingungen, technischen Normen und die Anwendung von Verhaltenskodizes. In Fällen, in denen eine öffentliche Stelle oder ein Organ, eine Einrichtung oder sonstige Stelle der Union oder Dritte, die die Daten erhalten, um die ihnen übertragenen Aufgaben zu erfüllen, diese Maßnahmen nicht umsetzen oder gegen die Vertraulichkeit von Geschäftsgeheimnissen verstoßen, sollte der Dateninhaber befugt sein, die Weitergabe von Daten auszusetzen, die als Geschäftsgeheimnisse identifiziert wurden. Eine solche Entscheidung, die Bereitstellung von Daten auszusetzen, kann von der öffentlichen Stelle oder dem Organ, der Einrichtung oder sonstigen Stelle der Union oder von den Dritten, an die die Daten übermittelt wurden, angefochten werden und vom Datenkoordinator des betreffenden Mitgliedstaats überprüft 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***, sofern das Verlangen zeitlich und vom Umfang her begrenzt ist und in einem angemessenen Verhältnis zum Zustand des öffentlichen Notstands steht***. 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 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***. Diese Verordnung sollte weder bestehende Vereinbarungen der Union oder der Mitgliedstaaten berühren, in denen Daten kostenlos weitergegeben werden, noch öffentliche Stellen, Organe, Einrichtungen oder sonstige Stellen der Union und Dateninhaber daran hindern, kostenlose Vereinbarungen über die freiwillige gemeinsame Datennutzung zu schließen.***

(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***, sofern diese Tätigkeiten unbedingt erforderlich sind, um dem Notstand gerecht zu werden***. ***Die öffentliche Stelle oder das Organ, die Einrichtung oder sonstige Stelle der Union sollte den Dateninhaber rechtzeitig über eine derartige Weitergabe unterrichten.*** 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 ***oder öffentlicher*** 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, ***ohne dass es zu Ausfallzeiten kommt, oder Dienste mehrerer Anbieter ohne unangemessene Kosten im Zusammenhang mit der Datenübermittlung simultan zu verwenden***, ist eine wesentliche Voraussetzung für einen vom Wettbewerb geprägten Markt mit geringeren Marktzutrittsschranken für neue Diensteanbieter ***sowie für das Sicherstellen einer besseren Resilienz der Nutzer dieser Dienste***. ***Garantien für den wirksamen Wechsel sollten auch für Kunden gelten, die von Angeboten mit großen kostenlosen Kontingenten profitieren, verstärkt werden, damit dies für Kunden nicht zu einer Abhängigkeit führt. Die Erleichterung eines Multi-Cloud-Ansatzes für Kunden von Diensten der Datenverarbeitung kann außerdem dazu beitragen, ihre digitale Betriebsstabilität zu verstärken, wie es für Anbieter von Finanzdienstleistungen in der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) anerkannt wird.***

(69a) Wechselentgelte sind Gebühren, die Anbieter von Cloud-Computing-Dienstleistungen von ihren Kunden für den Wechsel erheben. In der Regel sind diese Gebühren dazu gedacht, Kosten, die für den ursprünglichen Anbieter aufgrund des Wechsels anfallen, an den Kunden weiterzugeben, der den Wechsel wünscht. Beispiele für übliche Wechselentgelte sind Kosten im Zusammenhang mit der Übertragung der Daten von einem Anbieter zu einem anderen oder zu einem System in den eigenen Räumlichkeiten („Entgelte für den ausgehenden Datenverkehr") oder Kosten, die für spezifische Unterstützungstätigkeiten während des Wechsels anfallen. Unangemessen hohe Entgelte für den ausgehenden Datenverkehr und andere ungerechtfertigte Gebühren, die in keinem Zusammenhang mit den tatsächlichen Kosten des Wechsels stehen, behindern einen Wechsel des Anbieters durch den Kunden, schränken den freien Datenfluss ein, können den Wettbewerb einschränken und zu einer Abhängigkeit des Kunden von einem Anbieter von Datenverarbeitungsdiensten führen, indem Anreize verringert werden, einen anderen oder zusätzlichen Anbieter von Diensten auszuwählen. Aufgrund der in dieser Verordnung vorgesehenen neuen Verpflichtungen könnte der ursprüngliche Anbieter von Datenverarbeitungsdiensten bestimmte Aufgaben auslagern und Drittunternehmen benennen, um diesen Verpflichtungen nachzukommen. Der Kunde sollte nicht für die durch die Auslagerung von Diensten, die der ursprüngliche Anbieter von Datenverarbeitungsdiensten während des Wechsels eingestellt hat, entstandenen Kosten aufkommen müssen, und diese Kosten sollten als ungerechtfertigt angesehen werden. Das Datengesetz hindert einen Kunden nicht daran, Dritte für Unterstützung beim Wechsel des Anbieters zu entlohnen. Die Gebühren für den ausgehenden Datenverkehr werden von den vorherigen Anbietern von Diensten der Datenverarbeitung von den Kunden erhoben, wenn diese ihre Daten aus dem Netzwerk des Anbieters der Cloud an einen externen Speicherort verlagern möchten, insbesondere beim Wechsel von einem Anbieter zu einem anderen oder zu mehreren übernehmenden Anbietern, wenn sie ihre Daten von einem Speicherort an einen anderen verlagern möchten und dabei denselben Anbieter von Cloud-Diensten verwenden. Daher sollte im Sinne des Wettbewerbs die schrittweise Abschaffung der Entgelte im Zusammenhang mit dem Wechsel von Datenverarbeitungsdiensten insbesondere die Abschaffung von „Entgelten für den ausgehenden Datenverkehr" enthalten, die der Datenverarbeitungsdienst vom Kunden erhebt.

(70) Mit der Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates werden ***Anbieter von Datenverarbeitungsdiensten*** 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 ***Akzeptanz*** 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, ***geschäftliche, organisatorische,*** wirtschaftliche und technische Hindernisse***, darunter auch eine gebremste Geschwindigkeit der Datenübermittlung bei einem Wechsel des Kunden,*** für einen wirksamen Wechsel zwischen Datenverarbeitungsdiensten zu beseitigen.

(71) Datenverarbeitungsdienste sollten Dienste umfassen, die einen ***ortsunabhängigen und bedarfsgesteuerten Netzwerkzugriff*** auf einen ***konfigurierbaren,*** skalierbaren und elastischen Pool gemeinsam ▌verteilter Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige virtuelle oder physische Infrastrukturen, ▌Software, einschließlich Werkzeuge zur Entwicklung von Software, Speicher, Anwendungen und Dienste. ***Die Bereitstellungsmodelle für Datenverarbeitungsdienste sollten private und öffentliche Cloud-Dienste umfassen. Solche Dienste und Bereitstellungsmodelle sollten dieselben wie die in internationalen Normen definierten sein.*** Dass sich der Nutzer von Datenverarbeitungsdiensten selbst ohne Interaktion mit dem ***Anbieter von Datenverarbeitungsdiensten*** Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als ***minimaler Verwaltungsaufwand und minimale Interaktion zwischen Anbieter und Kunde*** beschrieben werden. Der Begriff „***ubiquitär***“ 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 ***von Datenverarbeitungsdiensten*** flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastisch ▌“ 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 ***genutzter Pool***“ 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. ***Digitale Dienste, die als Internetplattform im Sinne von Artikel 3 Buchstabe i [des Gesetzes über digitale Dienste] und als Online-Inhaltedienst im Sinne von Artikel 2 Absatz 5 der Verordnung (EU) 2017/1128 des Europäischen Parlaments und des Rates[1] gelten, sollten nicht als „Datenverarbeitungsdienste“ im Sinne dieser Verordnung betrachtet werden.***

(71a) Datenverarbeitungsdienste gehören zu einem oder mehreren der folgenden drei Bereitstellungsmodelle für Datenverarbeitungsdienste: IaaS (infrastructure-as-a-service), PaaS (platform-as-a-service) und SaaS (software-as-a-service). Bei diesen Modellen zur Erbringung von Diensten handelt es sich um eine spezifische, vorgefertigte Kombination von IT-Ressourcen, die von einem Anbieter von Datenverarbeitungsdiensten angeboten wird. Drei grundlegende Modelle von angebotenen Cloud-Computing-Diensten werden durch neue Variationen ergänzt, die jeweils aus einer getrennten Kombination von IT-Ressourcen bestehen, wie z. B. „Speicherung als Dienstleistung“ und „Datenbank als Dienstleistung“. Für die Zwecke dieser Verordnung können Datenverarbeitungsdienste in eine detailliertere und eine nicht erschöpfende Vielzahl unterschiedlicher „gleichwertiger Dienste“ eingeteilt werden, d. h. in Kategorien von Datenverarbeitungsdiensten, die dasselbe

---

*[1] **Verordnung (EU) 2017/1128 des Europäischen Parlaments und des Rates vom 14. Juni 2017 zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt (ABl. L 168 vom 30.6.2017, S. 1).***

Hauptziel und dieselben Hauptfunktionen sowie dieselbe Art von Datenverarbeitungsmodellen haben, die nicht mit den operativen Merkmalen des Dienstes in Zusammenhang stehen. So könnten zum Beispiel zwei Datenbanken dasselbe vorrangige Ziel verfolgen, aber nach Berücksichtigung ihres Datenverarbeitungsmodells, ihres Verbreitungsmodells und ihres gezielten Anwendungsfalls sollten diese Datenbanken in eine granuläre Unterkategorie gleichwertiger Dienste fallen. Gleichwertige Dienste können unterschiedliche und konkurrierende Merkmale wie Leistung, Sicherheit, Robustheit und Dienstqualität aufweisen.

(71b) Die Extraktion der Daten, die dem Kunden gehören, vom ursprünglichen Anbieter von Datenverarbeitungsdiensten bleibt eine der Herausforderungen, die die Wiederherstellung der Dienstfunktionen in der Infrastruktur des neuen Anbieters behindern. Um die Ausstiegsstrategie ordnungsgemäß zu planen, unnötige und aufwändige Aufgaben zu vermeiden und sicherzustellen, dass der Kunde keine seiner Daten infolge des Wechsels verliert, sollte der ursprüngliche Anbieter von Datenverarbeitungsdiensten in den Vertrag die obligatorischen Informationen über den Umfang der Daten aufnehmen, die der Kunde exportieren kann, sobald er beschließt, zu einem anderen Dienst, einem anderen Anbieter von Datenverarbeitungsdiensten oder zu einer vor Ort tätigen IKT-Infrastruktur zu wechseln. Der Anwendungsbereich der exportierbaren Daten sollte mindestens Ein- und Ausgabedaten umfassen, einschließlich relevanter Datenformate, Datenstrukturen und Metadaten, die direkt oder indirekt durch die Nutzung des Datenverarbeitungsdienstes durch den Kunden oder gemeinsam generiert werden und dem Kunden eindeutig zugeordnet werden können. Die exportierbaren Daten sollten Datenverarbeitungsdienste, Vermögenswerte Dritter oder Daten, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis oder vertrauliche Informationen darstellen, wie Daten, die sich auf die Integrität und Sicherheit des vom Datenverarbeitungsdienst bereitgestellten Dienstes beziehen, ausschließen und auch Daten ausschließen, die vom Anbieter für den Betrieb, die Wartung und die Verbesserung des Dienstes verwendet werden.

(72) Ziel dieser Verordnung ist es, den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, wozu alle ***relevanten*** 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 fortzusetzen ***und in den Genuss*** der Funktionsäquivalenz ***zu kommen***. ***Es sei darauf hingewiesen, dass die in den Anwendungsbereich fallenden Datenverarbeitungsdienste gemäß der vorliegenden Verordnung Teil des Kerngeschäfts von Anbietern sind.*** 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. ***Der Wechsel ist ein kundengesteuerter Vorgang, der drei Hauptschritte umfasst, und zwar i) Datenextraktion, d. h. das Herunterladen der Daten von einem System des vorherigen Anbieters, ii) Umwandlung, wenn die Daten eine Struktur haben, die nicht zum System des Zielspeicherorts passt, und iii) Hochladen der Daten in einen neuen Zielspeicherort. In einer bestimmten, in dieser Verordnung beschriebenen Situation sollte auch die Herauslösung eines bestimmten Dienstes aus dem Vertrag und der Wechsel zu einem anderen Anbieter als Anbieterwechsel gelten. Der Wechsel wird manchmal im Namen des Kunden von einem Dritten durchgeführt. Dementsprechend sollten alle in dieser Verordnung festgelegten Rechte und Pflichten des Kunden, einschließlich der Verpflichtung, nach Treu und Glauben zusammenzuarbeiten, so verstanden werden, dass sie unter diesen Umständen für einen entsprechenden Dritten gelten. Die Anbieter von Cloud-Computing-Diensten und die Kunden haben ein unterschiedliches Maß an Verantwortung, das von den jeweiligen Schritten des Verfahrens abhängig ist. So ist beispielsweise der vorherige Anbieter von Datenverarbeitungsdiensten dafür verantwortlich, die Daten in ein maschinenlesbares Format zu extrahieren, doch sind es der Kunde und der übernehmende Anbieter, die die Daten in die neue Umgebung hochladen, es sei denn, es wurde eine spezielle professionelle Übergangsdienstleistung in Anspruch genommen. Hindernisse für den Anbieterwechsel sind anders geartet und hängen von dem jeweiligen Schritt des Wechselvorgangs ab.*** Funktionsäquivalenz bedeutet die ***Möglichkeit, auf der Grundlage der Kundendaten*** einen Mindestfunktionsumfang eines Dienstes ***in der Umgebung eines neuen Datenverarbeitungsdienstes*** nach einem Wechsel ***wiederherzustellen, wobei*** der übernehmende Dienst ***als Reaktion auf dieselben Eingaben für gemeinsame Funktionen, der dem Kunden im Rahmen der***

vertraglichen Vereinbarung geliefert wird, ein vergleichbares Ergebnis liefert**. **Unterschiedliche Dienste können nur dann eine Funktionsäquivalenz für die gemeinsamen Kernfunktionen erreichen, wenn sowohl der vorherige als auch der übernehmende Dienstleister unabhängig voneinander dieselben Kernfunktionen anbieten. Die vorliegende Verordnung enthält keine Verpflichtung zur Erleichterung der Funktionsäquivalenz für Datenverarbeitungsdienste der Bereitstellungsmodelle PaaS oder SaaS. Relevante Metadaten, die bei der Nutzung eines Dienstes durch den Kunden erzeugt werden, sollten nach den Bestimmungen dieser Verordnung zum Anbieterwechsel übertragbar sein ***und fallen unter die Bestimmung von exportierbaren Daten**. **Die Datenverarbeitungsdienste werden in verschiedenen Branchen verwendet und weisen Unterschiede hinsichtlich der Komplexität und der Art des Dienstes auf. Dies ist insbesondere mit Blick auf den Übertragungsvorgang und den entsprechenden Zeitrahmen zu berücksichtigen.***

(72a) Um Anbieterbindungen, durch die der Wettbewerb und die Entwicklung neuer Dienste beeinträchtigt wird, zu lösen, bedarf es eines ambitionierten und innovationsfördernden regulatorischen Konzepts für Interoperabilität. Die Interoperabilität zwischen gleichwertigen Datenverarbeitungsdiensten erfordert mehrere Schnittstellen und Infrastrukturebenen sowie Software; sie beschränkt sich selten auf die einfache Frage, ob sie erreicht werden kann oder nicht. Der Aufbau einer entsprechenden Interoperabilität unterliegt vielmehr einer Kosten-Nutzen-Analyse, um zu ermitteln, ob es sinnvoll ist, die halbwegs vorhersehbaren Ergebnisse anzustreben. Die ISO/IEC 19941:2017 bildet einen wichtigen Bezugspunkt hinsichtlich der Verwirklichung der Ziele dieser Verordnung, da sie technische Erwägungen zur Klärung der Komplexität eines solchen Verfahrens umfasst.

(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, ***keine Hindernisse zu errichten und alle relevanten Hindernisse zu beseitigen und im Rahmen ihrer Möglichkeiten und im Verhältnis zu ihren jeweiligen Verpflichtungen*** jede erforderliche Hilfe und Unterstützung zu leisten, um den Wechselvorgang

erfolgreich***, sicher*** und wirksam zu gestalten. ***Diese Verordnung verpflichtet die*** Anbieter von Datenverarbeitungsdiensten ***nicht dazu,*** neue Kategorien von Datenverarbeitungsdiensten***, auch*** innerhalb der IT-Infrastruktur verschiedener Anbieter von Datenverarbeitungsdiensten oder auf deren Grundlage, zu entwickeln, um die Funktionsäquivalenz in einer anderen Umgebung als ihren eigenen Systemen zu sicherzustellen. ***Ein vorheriger Anbieter von Datenverarbeitungsdiensten hat keinen Zugang und keinen Einblick in die Umgebung des übernehmenden Anbieters von Datenverarbeitungsdiensten und sollte nicht verpflichtet sein, den Kundendienst gemäß den Anforderungen an die Funktionsäquivalenz innerhalb der Infrastruktur des übernehmenden Anbieters wiederaufzubauen. Stattdessen sollte der vorherige Anbieter im Rahmen seiner Befugnisse alle zumutbaren Maßnahmen ergreifen, um die Verwirklichung der Funktionsäquivalenz zu erleichtern, indem er Kapazitäten, angemessene Informationen, eine Dokumentation, technische Unterstützung und gegebenenfalls die erforderlichen Instrumente bereitstellt. Die Informationen, die die Anbieter von Datenverarbeitungsdiensten dem Kunden zur Verfügung stellen müssen, sollten die Ausarbeitung der Ausstiegsstrategie des Kunden unterstützen und Verfahren für die Einleitung des Wechsels vom Cloud-Computing-Dienst, die maschinenlesbaren Datenformate für den Export der Nutzerdaten, die für den Datenexport vorgesehenen Instrumente, einschließlich mindestens einer offenen Standardschnittstelle für die Datenübertragbarkeit, Informationen über bekannte technische Beschränkungen und Einschränkungen, die sich auf den Wechselvorgang auswirken könnten, und die geschätzte Zeit, die für den Abschluss des Wechsels erforderlich ist, umfassen. Der schriftliche Vertrag, in dem die Rechte des Kunden und die Pflichten des Anbieters von Cloud-Computing-Diensten festgelegt sind, sollte sich nur auf Informationen erstrecken, die dem Anbieter von Datenverarbeitungsdiensten zum Zeitpunkt des Vertragsschlusses zur Verfügung stehen.*** 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[1] eingeführt wurden, sollten davon unberührt bleiben. ***Jede verbindliche Frist im Rahmen dieser Verordnung darf die Einhaltung anderer Fristen, die in branchenspezifischen Rechtsvorschriften***

[1] 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).

festgelegt sind, nicht beeinträchtigen. Kapitel VI dieser Verordnung darf nicht so verstanden werden, dass ein Anbieter von Datenverarbeitungsdiensten daran gehindert wird, seinen Kunden neue und verbesserte Dienste, Merkmale und Funktionen anzubieten oder auf dieser Grundlage mit anderen Anbietern von Datenverarbeitungsdiensten in Wettbewerb zu treten.

(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 ***Anbietern von Datenverarbeitungsdiensten*** zu schaffen und die Rechtssicherheit in Bezug auf die Bedingungen für den Wechsel zu anderen Datenverarbeitungsdiensten zu erhöhen. Vor diesem Hintergrund sollten Nutzer und ***Anbieter von Datenverarbeitungsdiensten*** die Verwendung von Standardvertragsklauseln in Erwägung ziehen, die von einschlägigen Gremien oder Sachverständigengruppen, die nach Unionsrecht eingerichtet wurden, ausgearbeitet wurden.

(75a) Um den Wechsel zwischen Cloud-Computing-Diensten zu erleichtern, sollten alle Beteiligten, einschließlich der vorherigen und der übernehmenden Anbieter von Datenverarbeitungsdiensten, nach Treu und Glauben zusammenarbeiten, um einen wirksamen Wechsel und die sichere und rechtzeitige Übermittlung der erforderlichen Daten in einem allgemein verwendeten, maschinenlesbaren Format und mittels einer offenen Standardschnittstelle für die Datenübertragbarkeit zu ermöglichen und Dienstunterbrechungen zu vermeiden.

(75b) Datenverarbeitungsdienste, die wesentlich angepasst wurden, um einen Kundenbedarf zu erfüllen (außer Serie), oder Datenverarbeitungsdienste, die im Probebetrieb sind oder nur einen Test- und Evaluierungsdienst für Produktangebote des Unternehmens bieten, sollten von den für den Wechsel von Datenverarbeitungsdiensten geltenden Pflichten befreit werden.

(75c) Unbeschadet des Rechts des Kunden, eine Klage bei Gericht einzulegen, sollten sie Zugang zu zertifizierten Streitbeilegungsstellen haben, um Streitigkeiten im

Zusammenhang mit dem Wechsel des Anbieters von Datenverarbeitungsdiensten beizulegen.

(76) Offene Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** und -normen, die gemäß Anhang II Nummern 3 und 4 der Verordnung (EU) Nr. 1025/2021 ***des Europäischen Parlaments und des Rates***[1] im Bereich der Interoperabilität und Übertragbarkeit entwickelt wurden, ermöglichen eine ▌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 ***und Übertragbarkeit*** auf den Ebenen der Verarbeitung von Daten auf ▌PaaS ***und*** in ▌SaaS ▌erleichtern, mit marktgesteuerten Verfahren festgelegt werden können, sollte die Kommission ***wo technisch möglich*** auf der Grundlage dieser Verordnung und im Einklang mit der Verordnung (EU) Nr. 1025/2012 europäische Normungsgremien mit der Entwicklung solcher Normen ***für vergleichbare Dienste*** beauftragen können, für die solche Normen noch nicht existieren. Darüber hinaus wird die Kommission die Marktteilnehmer anhalten, einschlägige offene Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** zu entwickeln. ***Nach Konsultation der Interessenträger und unter Berücksichtigung der einschlägigen internationalen und europäischen Normen und Selbstregulierungsinitiativen*** kann die Kommission 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 ***und Übertragbarkeit*** oder offener Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** für bestimmte ***gleichwertige Dienste*** vorschreiben. ***Die Anbieter von Datenverarbeitungsdiensten sollten die Vereinbarkeit mit diesen Normen für die Interoperabilitäts- und Übertragbarkeitsspezifikationen sicherstellen und dabei der Art, Sicherheit und Integrität der von ihnen gehosteten Daten Rechnung tragen.*** Auf europäische Normen ***für die Interoperabilität und Übertragbarkeit von Datenverarbeitungsdiensten*** und

---

[1] ***Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).***

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 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 ***Verbraucher***, 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 ***und syntaktische*** Interoperabilität sollten eine wichtige Rolle bei der Bereitstellung technischer Lösungen zur Gewährleistung ***der Übertragbarkeit und*** der Interoperabilität spielen. ***Um die Bewertung der Konformität mit den geltenden Interoperabilitätsanforderungen innerhalb der gemeinsamen europäischen Datenräume, die zweckgerichtet oder branchenspezifisch bzw. branchenübergreifend sind, zu erleichtern, sollten interoperable Rahmen gemeinsamer Standards und Verfahren für den Austausch oder die gemeinsame Verarbeitung von Daten, unter anderem für die Entwicklung neuer Produkte und Dienste, die wissenschaftliche Forschung oder zivilgesellschaftliche Initiativen entwickelt werden. In dieser Verordnung werden bestimmte grundlegende Anforderungen an die Interoperabilität festgelegt. Teilnehmer innerhalb der Datenräume, bei denen es sich um Einrichtungen handelt, die die gemeinsame Datennutzung innerhalb der gemeinsamen europäischen Datenräume erleichtern oder daran beteiligt sind, einschließlich Dateninhabern, sollten diese Anforderungen erfüllen. Die Einhaltung dieser Vorschriften kann durch die Einhaltung der in dieser Verordnung festgelegten Anforderungen oder durch die Anpassung an bereits***

bestehende Normen im Rahmen einer Konformitätsvermutung erfolgen. 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 ▌ oder Teilen davon entsprechen, von einer Konformitätsvermutung ausgegangen werden. ***Normen sollten im Einklang mit Kapitel II der Verordnung (EU) Nr. 1025/2012 auf offene, technologieneutrale und integrative Weise entwickelt werden. Unter Berücksichtigung der gegebenenfalls vom Europäischen Dateninnovationsrat gemäß Artikel 30 Buchstabe f der Verordnung (EU) 2022/868 angenommenen Standpunkte,*** sollte die Kommission 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 ***könnten*** ebenfalls Teil der technischen Spezifikationen für die semantische Interoperabilität sein. ***Nach Konsultation der Interessenträger und unter Berücksichtigung der einschlägigen internationalen und europäischen Normen und Selbstregulierungsinitiativen sowie gegebenenfalls der vom Europäischen Dateninnovationsrat gemäß Artikel 30 Buchstabe f der Verordnung (EU) 2022/868 angenommenen Standpunkte*** sollte die Kommission darüber hinaus in die Lage versetzt werden, ***in Bereichen, in denen es keine harmonisierten Normen gibt, gemeinsame Spezifikationen anzunehmen und*** die Entwicklung harmonisierter Normen für die Interoperabilität ***und Übertragbarkeit*** von Datenverarbeitungsdiensten in Auftrag zu geben. ***Der Europäische Dateninnovationsrat sollte auf bestehenden europäischen und globalen Initiativen zur sektorübergreifenden Interoperabilität von Daten aufbauen. Insbesondere sollte der Europäische Dateninnovationsrat das Potenzial des durch die Verordnung (EU) Nr. 910/214 geschaffenen Rahmens für die digitale Identität von Objekten und Systemen zur Identifizierung von juristischen Personen wie der GLEIF zu diesem Zweck untersuchen.***

(79a) Um die Koordinierung bei der Durchsetzung dieser Verordnung weiter zu verbessern, sollte der Europäische Dateninnovationsrat den gegenseitigen Informationsaustausch zwischen den zuständigen Behörden fördern und die Kommission in Angelegenheiten beraten und unterstützen, die unter diese Verordnung und in die Zuständigkeiten gemäß Artikel 30 der Verordnung (EU) 2022/868 fallen. Eine Untergruppe für die Einbeziehung der Interessenträger gemäß Artikel 29 Absatz 2 Buchstabe c der genannten Verordnung sollte kontinuierlich an der Konsultation teilnehmen.

(80) Um die Interoperabilität intelligenter Verträge in Anwendungen für die gemeinsame Datennutzung zu fördern, müssen ***unter Umständen*** 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. ***Im Rahmen von*** intelligenten Verträgen ***sollte zum Beispiel sichergestellt werden, dass die Bedingungen für die gemeinsame Datennutzung eingehalten werden. Es sollten spezielle Schulungsprogramme zu*** intelligenten Verträgen ***für Unternehmen, insbesondere für KMU, gefördert werden***.

(81) Um die effiziente Durchführung dieser Verordnung zu gewährleisten, sollten die Mitgliedstaaten eine oder mehrere zuständige Behörden benennen ***und mit ausreichenden Ressourcen ausstatten***. Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so sollte er auch eine koordinierende zuständige Behörde benennen. Die zuständigen Behörden sollten ***im Einklang mit den Grundsätzen der guten Verwaltung und der gegenseitigen Amtshilfe wirksam und rechtzeitig*** zusammenarbeiten***, um die wirksame Durchführung und Durchsetzung dieser Verordnung sicherzustellen***. 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. ***Die zuständigen Behörden sollten auf Ersuchen der Behörden im Europäischen Datenschutzausschuss und im Europäischen Dateninnovationsrat zusammenarbeiten.***

(81a) Um die Koordinierung bei der Durchsetzung dieser Verordnung weiter zu verbessern, sollte der Europäische Dateninnovationsrat den gegenseitigen

Informationsaustausch zwischen den zuständigen Behörden fördern und die Kommission in Angelegenheiten beraten und unterstützen, die unter diese Verordnung fallen, wobei der Schwerpunkt auf denjenigen Angelegenheiten liegen sollte, die gemäß Artikel 30 der Verordnung (EU) 2022/868 in die Zuständigkeiten des Dateninnovationsrates fallen.

(82) Zur Durchsetzung ihrer Rechte gemäß dieser Verordnung sollten natürliche und juristische Personen das Recht haben, im Falle einer Verletzung ihrer Rechte aus dieser Verordnung mittels Einlegung einer Beschwerde ***beim Datenkoordinator, bei einer sonstigen*** zuständigen Behörde ***und vor Gericht*** dagegen vorzugehen. Diese Behörden sollten zur Zusammenarbeit verpflichtet sein, damit die Beschwerde angemessen bearbeitet und ***zügig und wirksam*** beschieden werden kann. 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[1] und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates[2] 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 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

---

1 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).

2 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).

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 ▌Datenbanken, ***die Daten enthalten,*** die durch physische Komponenten wie Sensoren eines vernetzten Produkts und verbundenen Dienstes***, d. h. durch maschinengenerierte Daten,*** gewonnen oder erzeugt wurden, das Schutzrecht sui generis gemäß Artikel 7 der Richtlinie 96/9/EG geltend machen, ***wird in dieser Verordnung klargestellt, dass*** das Schutzrecht sui generis auf solche Datenbanken keine Anwendung findet, ▌da die Schutzanforderungen ***einer umfangreichen Investition in die Gewinnung, Überprüfung oder Darstellung der Daten gemäß Artikel 7 Absatz 1 der Richtlinie 96/9/EG*** nicht erfüllt wären. ***Dies berührt nicht die mögliche Anwendung des Schutzrechts sui generis gemäß Artikel 7 der Richtlinie 96/9/EG auf Datenbanken, die Daten enthalten, die nicht in den Anwendungsbereich dieser Verordnung fallen, sofern die Schutzanforderungen gemäß Artikel 7 Absatz 1 der genannten Richtlinie erfüllt sind.***

(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 ***Teilnehmer*** von Datenräumen***, die anderen Teilnehmern von Datenräumen Daten oder Datendienste anbieten,*** 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[1] 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 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[2] 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

---

1 ABl. L 123 vom 12.5.2016, S. 1.

2 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).

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 ***und die notwendigen technischen Vorkehrungen treffen*** können, sollten sie erst ***18 Monate*** nach Inkrafttreten der Verordnung anwendbar werden. ***Nur wenn der Dateninhaber und der Hersteller ein und dieselbe Instanz sind, sollten die Verpflichtungen im Zusammenhang mit der Erbringung verbundener Dienstleistungen für vernetzte Produkte, die innerhalb den letzten fünf Jahren nach Inkrafttreten dieser Verordnung bereits in Verkehr gebracht wurden, rückwirkend gelten. Diese Verpflichtungen sollten nur dann erfüllt werden, wenn der Anbieter verbundener Dienste in der Lage ist, Mechanismen zur Gewährleistung der Erfüllung der Anforderungen gemäß Artikel 1 aus der Ferne einzurichten, und nur dann, wenn die Einrichtung solcher Mechanismen keine unverhältnismäßige Belastung für den Hersteller darstellen würde.***

(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 —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Verordnung ***werden*** harmonisierte Vorschriften ***in Bezug auf Folgendes festgelegt:***

a) die Gestaltung vernetzter Produkte, um dem Nutzer eines vernetzten Produkts Zugang zu den Daten zu ermöglichen, die von diesem vernetzten Produkt oder während der Erbringung verbundener Dienste erzeugt werden;

b) die Dateninhaber, die betroffenen Personen, Nutzern oder Datenempfängern auf Verlangen des Nutzers oder der betroffenen Person Daten zur Verfügung stellen, auf die Dateninhaber über ein verbundenes Produkt zugegriffen haben oder die bei der Erbringung einer damit verbundenen Dienstleistung erzeugt wurden;

c) faire Vertragsbedingungen für Vereinbarungen über die gemeinsame Datennutzung;

d) die Bereitstellung von Daten für öffentliche Stellen oder Organe, Einrichtungen und sonstige Stellen der Union, soweit diese Daten wegen außergewöhnlicher Notwendigkeit von öffentlichem Interesse benötigt werden;

e) die Erleichterung des Wechsels zwischen Datenverarbeitungsdiensten;

f) die Einführung von Schutzmaßnahmen gegen den unrechtmäßigen internationalen Zugang seitens der Regierung zu nicht personenbezogenen Daten;

g) Vorkehrungen für die Ausarbeitung von Interoperabilitätsnormen und gemeinsamen Spezifikationen für die zu übermittelnden und zu verwendenden Daten.

(1a) Die vorliegende Verordnung erstreckt sich auf personenbezogene und nicht personenbezogene Daten, einschließlich der folgenden Arten von Daten in den aufgeführten Zusammenhängen:

a) Kapitel II gilt für zugängliche Daten, die von vernetzten Produkten erlangt, gesammelt oder anderweitig erzeugt werden oder bei der Erbringung verbundener Dienste erzeugt werden;

b) Kapitel III gilt für alle Daten des Privatsektors, die gesetzlichen Verpflichtungen mit Blick auf die gemeinsame Datennutzung unterliegen;

c) Kapitel IV gilt für alle Daten des Privatsektors, die auf der Grundlage vertraglicher Vereinbarungen zwischen Unternehmen abgerufen und verwendet werden;

d) Kapitel V gilt für alle nicht personenbezogenen Daten des Privatsektors;

e) Kapitel VI gilt für alle von Datenverarbeitungsdiensten verarbeiteten Daten und Dienste;

f) Kapitel VII gilt für alle nicht personenbezogenen Daten, die in der Union im Besitz von Anbietern von Datenverarbeitungsdiensten sind.

(2) Diese Verordnung gilt für

a) Hersteller ***vernetzter*** Produkte und Erbringer verbundener Dienste, die in der Union in Verkehr gebracht werden, ***unabhängig vom Ort ihrer Niederlassung,*** und die Nutzer solcher ***vernetzten*** Produkte oder verbundenen Dienste ***bzw. im Fall von personenbezogenen Daten die identifizierten oder identifizierbaren Personen, auf die sich die bei der Nutzung erlangten, gesammelten oder erzeugten Daten beziehen***;

b) ***Nutzer vernetzter Produkte und verbundener Dienste in der Union und*** Dateninhaber ***unabhängig vom Ort ihrer Niederlassung***, die Datenempfängern in der Union Daten bereitstellen, ***bzw. im Fall von personenbezogenen Daten die identifizierten oder identifizierbaren Personen, auf die sich die bei der Nutzung erlangten, gesammelten oder erzeugten Daten beziehen***;

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

d) öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union ***sowie der Mitgliedstaaten***, die von Dateninhabern verlangen, Daten bereitzustellen, sofern diese Daten wegen außergewöhnlicher Notwendigkeit zur Wahrnehmung einer ***bestimmten*** Aufgabe von öffentlichem Interesse benötigt

werden, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;

e) Anbieter von Datenverarbeitungsdiensten ***unabhängig vom Ort ihrer Niederlassung***, 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 ***alle*** personenbezogene Daten, die im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten verarbeitet werden. ***Für die Erlangung, Sammlung oder Erzeugung personenbezogener Daten über die Nutzung eines Produkts oder verbundenen Dienstes bedarf es einer Rechtsgrundlage im Sinne des geltenden Datenschutzrechts.*** Diese Verordnung ***stellt keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar***. ***Diese Verordnung berührt nicht die*** Rechtsvorschriften der Union über den Schutz personenbezogener Daten ***und der Privatsphäre***, insbesondere ***nicht*** die Verordnung (EU) 2016/679***, die Verordnung (EU) 2018/1725*** und die Richtlinie 2002/58/EG, sowie ***die Vorschriften betreffend*** die Befugnisse und Zuständigkeiten der Aufsichtsbehörden. ***Im Falle eines Widerspruchs zwischen dieser Verordnung und dem Unionsrecht zum Schutz personenbezogener Daten bzw. der Privatsphäre oder dem im Einklang mit dem Unionsrecht erlassenen nationalen Recht haben die einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten zum Schutz personenbezogener Daten bzw. der Privatsphäre Vorrang.*** 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 ***und präzisieren*** die Bestimmungen dieser Verordnung das Recht auf Datenübertragbarkeit nach Artikel 20 der Verordnung (EU) 2016/679. ***Keine Bestimmung dieser Verordnung darf 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.***

(4) Diese Verordnung berührt nicht die 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 ***Ordnungswidrigkeiten*** oder der Vollstreckung von Strafen oder

verwaltungsrechtlichen Sanktionen, einschließlich der Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates[1] und der [Vorschläge über elektronische Beweismittel COM(2018)0225 und COM(2018)0226], 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, die Verteidigung, die nationale Sicherheit, die Zoll- und Steuerverwaltung sowie ***die öffentliche*** Gesundheit und ***die*** Sicherheit der Bürger. ***Diese Verordnung gilt nicht für Daten, die im Zusammenhang mit verteidigungsbezogenen Tätigkeiten, durch Verteidigungsprodukte oder -dienste oder durch Produkte oder Dienstleistungen, die für Verteidigungszwecke eingesetzt und verwendet werden, gesammelt oder erzeugt werden.***

(4a) Die vorliegende Verordnung ergänzt das Unionsrecht zur Förderung der Interessen der Verbraucher und zur Sicherstellung eines hohen Verbraucherschutzniveaus und zum Schutz der Gesundheit, Sicherheit und wirtschaftlichen Interessen der Verbraucher, einschließlich der Richtlinie 2005/29/EG, der Richtlinie 2011/83/EU und der Richtlinie 93/13/EWG, und lässt dessen Anwendbarkeit unberührt.

(4b) Die Dateninhaber sind nicht verpflichtet, natürlichen oder juristischen Personen, Organisationen oder Einrichtungen außerhalb der Union Zugang zu Daten zu gewähren, es sei denn, dass dies vom Nutzer verlangt wird oder anderweitig durch das Unionsrecht oder die nationalen Rechtsvorschriftenvorschriften zur Umsetzung des Unionsrecht vorgesehen ist.

(4c) Die in der Verordnung festgelegten Verpflichtungen stehen einem freiwilligen, rechtmäßigen gegenseitigen Austausch nicht personenbezogener Daten zwischen

---

[1] 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).

Nutzern, Dateninhabern und Datenempfängern, der vertraglich vereinbart wurde, nicht entgegen.

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; ***Inhalte oder Daten, die von dem vernetzten Produkt erlangt, erzeugt oder gesammelt oder ihm im Auftrag Dritter zum Zwecke der Speicherung oder Verarbeitung übermittelt werden, fallen nicht unter diese Verordnung;***

1a. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;

1b. „nicht personenbezogene Daten“ Daten, bei denen es sich nicht um personenbezogene Daten handelt;

1c. „Einwilligung“ eine Einwilligung im Sinne von Artikel 4 Nummer 11 der Verordnung (EU) 2016/679;

1d. „betroffene Person“ eine betroffene Person im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;

1e. „Datennutzer“ eine natürliche oder juristische Person, die rechtmäßig Zugang zu bestimmten personenbezogenen oder nicht personenbezogenen Daten hat und berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen;

2. „***vernetztes*** Produkt“ einen ▌ Gegenstand, der ***zugängliche*** Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen ▌ elektronischen Kommunikationsdienst***, eine physische Verbindung oder einen geräteinternen Zugang*** übermitteln kann und dessen Hauptfunktion nicht die Speicherung***,*** Verarbeitung ***und Übertragung*** von Daten ***im Namen Dritter*** ist;

3. „verbundener Dienst“ einen digitalen Dienst, einschließlich Software***, aber mit Ausnahme von elektronischen Kommunikationsdiensten,*** der so mit einem Produkt

verbunden ist, dass das Produkt ohne ihn eine ***oder mehrere*** seiner ***Funktionen*** nicht ausführen könnte***, und der den Zugriff des Anbieters oder des Dienstes auf Daten des vernetzten Produkts umfasst***;

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 ***anderen*** Diensten gewährt oder ***die Funktionen von Produkten*** steuert;

4a. „Verbraucher“ jede natürliche Person, die zu Zwecken handelt, die außerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen;

5. „Nutzer“ eine natürliche oder juristische Person, die ein ***vernetztes*** Produkt besitzt ***oder einen verbundenen Dienst*** in Anspruch nimmt ***oder der vom Eigentümer eines vernetzten Produkts auf der Grundlage eines Miet- oder Leasingvertrags eine vorübergehende Genehmigung erteilt wurde, das vernetzte Produkt zu nutzen oder die verbundenen Dienste in Anspruch zu nehmen, und, wenn das Produkt oder der verbundene Dienst die Verarbeitung personenbezogener Daten beinhaltet, die betroffene Person***;

6. „Dateninhaber“ eine juristische oder natürliche Person, die ***auf Daten aus dem vernetzten Produkt zugegriffen oder bei der Erbringung eines verbundenen Dienstes Daten erzeugt hat und die das vertraglich vereinbarte Recht hat, diese Daten zu nutzen, und die gemäß dieser Verordnung, dem geltenden Unionsrecht oder den nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts verpflichtet ist, dem Nutzer oder einem Datenempfänger*** bestimmte Daten zur Verfügung zu stellen;

7. „Datenempfänger“ eine juristische oder natürliche Person, die ▌ nicht der Nutzer eines ***vernetzten*** Produktes oder verbundenen Dienstes ***ist***, und ***der ein*** Dateninhaber Daten***, auf die von dem vernetzten Produkt aus zugegriffen wurde oder die während der Erbringung eines verbundenen Dienstes erzeugt wurden,*** auf ***ausdrückliches*** 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 Vorgehensweisen 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 ***zeitlich begrenzte*** Ausnahmesituation ***wie Notfälle im Bereich der öffentlichen Gesundheit, Notfälle infolge von Naturkatastrophen sowie von Menschen verursachte Katastrophen größeren Ausmaßes, einschließlich schwerer Cybersicherheitsvorfälle***, die sich negativ auf die Bevölkerung der Union, eines Mitgliedstaats oder eines Teils davon auswirkt**,** das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen**,** die wirtschaftliche Stabilität ***oder die finanzielle Stabilität*** oder die Gefahr einer erheblichen ***und umgehenden*** Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem bzw. den betroffenen Mitgliedstaaten birgt ***und nach den einschlägigen Verfahren des Unionsrechts oder des nationalen Rechts festgestellt und amtlich ausgerufen wurde***;

10a. „amtliche Statistiken” europäische Statistiken im Sinne der Verordnung (EG) Nr. 223/2009[1];

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

---

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

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 ***Standards***“, technische ▌Spezifikationen ▌, die leistungsbezogen darauf ausgerichtet sind, die Interoperabilität zwischen Datenverarbeitungsdiensten herzustellen ***und die durch ein inklusives, kollaboratives, konsensbasiertes und transparentes Verfahren angenommen wurden, von dem maßgeblich betroffene und interessierte Parteien nicht ausgeschlossen werden können***;

▌

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 ***datenbasierten Diensten, einschließlich*** Datenräumen oder Kommunikationsnetzen, Systemen, Produkten, Anwendungen oder Komponenten, Daten ***zu verarbeiten,*** auszutauschen und zu verwenden, um ihre Funktionen ***genau, effizient und einheitlich*** auszuführen;

19a. „Übertragbarkeit” die Fähigkeit eines Kunden, importierte oder unmittelbar erzeugte Daten, die dem Kunden eindeutig zugeordnet werden können, zwischen seinem eigenen System und Cloud-Diensten bzw. zwischen Cloud-Diensten verschiedener Anbieter von Cloud-Diensten zu bewegen;

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

20a. „gemeinsame europäische Datenräume“ zweck- oder bereichsspezifische oder auch bereichsübergreifende interoperable Rahmen gemeinsamer Normen und Verfahren für die gemeinsame Nutzung oder Verarbeitung von Daten für unter anderem die Entwicklung neuer Produkte und Dienste, die wissenschaftliche Forschung oder Initiativen der Zivilgesellschaft;

20b. „Metadaten“ eine strukturierte Beschreibung der Inhalte der Datennutzung, die das Auffinden der entsprechenden Daten bzw. deren Verwendung erleichtert;

20c. „Datenvermittlungsdienst“ einen Datenvermittlungsdienst im Sinne von Artikel 2 Nummer 8 der Verordnung (EU) 2022/868;

20d. „Datenaltruismus“ die freiwillige gemeinsame Nutzung von Daten im Sinne von Artikel 2 Nummer 16 der Verordnung (EU) 2022/868;

20e. „Geschäftsgeheimnis“ Informationen, die alle Anforderungen von Artikel 2 Nummer 1 der Richtlinie (EU) 2016/943 erfüllen;

20f. „Träger eines Geschäftsgeheimnisses“ einen Inhaber eines Geschäftsgeheimnisses im Sinne von Artikel 2 Nummer 2 der Richtlinie (EU) 2016/943.

KAPITEL II

DATENWEITERGABE VON UNTERNEHMEN AN VERBRAUCHER UND ZWISCHEN UNTERNEHMEN

Artikel 3

Pflicht der Zugänglichmachung ***für Nutzer von Daten, auf die von vernetzten Produkten zugegriffen wird oder die bei der Erbringung eines*** verbundenen Dienstes erzeugt ***werden***

(1) ***Vernetzte*** Produkte werden so konzipiert und hergestellt, dass ***von ihnen erhobene,*** erzeugte ***oder anderweitig erhaltende*** Daten***, auf die die Dateninhaber bzw. Datenempfänger zugreifen können,*** für den Nutzer standardmäßig ***kostenlos und*** einfach sicher und – soweit relevant ***und technisch machbar – in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format*** unmittelbar zugänglich sind. ***Die Daten müssen in der Form zur Verfügung stehen, in der sie von dem vernetzten Produkt erhoben, erhalten oder erzeugt wurden, wobei nur die minimalen Anpassungen vorgenommen werden, die erforderlich sind, um sie für***

Dritte nutzbar zu machen, einschließlich der zugehörigen Metadaten, die zur Interpretation und Nutzung der Daten benötigt werden. Informationen, die mithilfe komplexer proprietärer Algorithmen aus diesen Daten abgeleitet bzw. gefolgert wurden, insbesondere wenn dabei die Ausgabe mehrerer Sensoren in dem vernetzten Produkt kombiniert wurde, fallen nicht unter die Verpflichtung des Dateninhabers zur Weitergabe von Daten an Nutzer bzw. Datenempfänger, sofern der Nutzer und der Dateninhaber nichts anderes vereinbart haben. Falls es sich bei dem Nutzer um eine betroffene Person handelt, müssen die vernetzten Produkte die Möglichkeit bieten, ihre Rechte als betroffene Personen direkt wahrzunehmen, sofern dies technisch möglich ist. Vernetzte Produkte müssen so konzipiert und hergestellt werden, dass den betroffenen Personen unabhängig von ihrem Rechtsanspruch auf das vernetzte Produkt die Möglichkeit geboten wird, die unter diese Verordnung fallenden Produkte in einer Weise zu nutzen, die so wenig wie möglich in die Privatsphäre eingreift. Die in Unterabsatz 1 festgelegten Anforderungen müssen ohne Beeinträchtigung der Funktionalität des vernetzten Produkts und der verbundenen Dienste sowie im Einklang mit den im Unionsrecht festgelegten Datensicherheitsanforderungen erfüllt werden.

(1a) Die Dateninhaber können ein Datenverlangen ablehnen, wenn der Zugang zu den Daten durch Unionsrecht oder nationales Recht untersagt ist.

(2) Vor Abschluss ***des Kaufs eines vernetzten Produkts muss der Hersteller oder gegebenenfalls der Verkäufer*** dem Nutzer mindestens folgende Informationen ***in einfacher Weise und*** in einem klaren und verständlichen Format bereitstellen:

a) ***Art der Daten, Format, Erhebungsfrequenz, Speicherkapazität der Geräte und geschätzte Menge zugänglicher Daten, die das vernetzte Produkt erheben, erzeugen oder anderweitig erhalten kann***;

b) ob das ***vernetzte Produkt in der Lage ist***, Daten kontinuierlich und in Echtzeit zu erzeugen;

ba) ob die Daten auf dem Gerät oder auf einem entfernten Server gespeichert werden, einschließlich des Zeitraums, in dem sie gespeichert werden sollen;

c) wie der Nutzer ***kostenlos*** auf diese Daten zugreifen***, sie gegebenenfalls abrufen und ihre Löschung anfordern*** kann;

ca) die technischen Mittel für den Datenzugriff wie Software Development Kits oder Anwendungsprogrammierschnittstellen sowie ihre Nutzungsbedingungen und die Dienstqualität sind hinreichend zu beschreiben, sodass die Entwicklung entsprechender Möglichkeiten des Zugriffs begünstigt wird;

cb) ob ein Dateninhaber Träger von Geschäftsgeheimnissen oder Inhaber sonstiger Rechte des geistigen Eigentums in Bezug auf die Daten ist, auf die das vernetzte Produkt voraussichtlich zugreifen wird oder die bei der Erbringung des verbundenen Dienstes voraussichtlich erzeugt werden, und, falls nicht, die Identität des Trägers des Geschäftsgeheimnisses, wie z. B. seinen Handelsnamen und die Anschrift des Ortes, an dem er ansässig ist.

▌

(2a) Verbundene Dienste müssen so erbracht werden, dass die dabei erzeugten Daten, die die digitalisierten Nutzerhandlungen und -vorgänge abbilden, standardmäßig einfach, sicher und – soweit relevant und technisch machbar – für den Nutzer kostenlos in einem strukturierten, gängigen und maschinenlesbaren Format zusammen mit den einschlägigen Metadaten, die für die Interpretation und Nutzung erforderlich sind, direkt zugänglich sind.

(2b) Bei Abschluss einer Vereinbarung zwischen den Nutzer und einem Anbieter verbundener Dienste, die den Zugang des Anbieters zu Daten von dem vernetzten Produkt im Einklang mit Artikel 4 Absatz 6 dieser Verordnung umfasst, ist in der Vereinbarung Folgendes anzugeben:

a) Art, Umfang, Häufigkeit der Erhebung und Format der Daten, auf die der Anbieter verbundener Dienste durch das vernetzte Produkt zugreift, sowie gegebenenfalls die für den Nutzer geltenden Modalitäten für den Zugriff oder die Abfrage dieser Daten, einschließlich des Zeitraums, in dem sie gespeichert werden sollen;

b) Art und geschätzter Umfang der während der Erbringung des verbundenen Dienstes erzeugten Daten sowie die für den Nutzer geltenden Modalitäten für den Zugriff oder die Abfrage dieser Daten;

c) detaillierte, aussagekräftige Zustimmungsmöglichkeiten zur Datenverarbeitung im Sinne von Artikel 4 Absatz 11 der Verordnung (EU) 2016/679;

d) ob der Diensteanbieter, der den verbundenen Dienst erbringt, in seiner Rolle als Dateninhaber beabsichtigt, die Daten, auf die über das verbundene Produkt zugegriffen wird, selbst zu verwenden oder einem oder mehreren Dritten die Nutzung der Daten zu dem mit dem Nutzer vereinbarten Zwecke zu gestatten;

e) den Handelsnamen des Anbieters des verbundenen Dienstes, seine Rechtsträgerkennung, Kontaktdaten und die Anschrift des Ortes, an dem er ansässig ist, und gegebenenfalls andere Datenverarbeitungsparteien;

f) gegebenenfalls die Kommunikationsmittel, mit denen der Nutzer den Anbieter rasch kontaktieren und effizient mit seinem Personal kommunizieren kann;

g) wie der Nutzer veranlassen kann, dass die Daten an einen Datenempfänger weitergegeben werden, und wie er gegebenenfalls die Einwilligung zur Weitergabe der Daten widerrufen kann;

h) ob der Dateninhaber Träger von Geschäftsgeheimnissen oder Inhaber sonstiger Rechte des geistigen Eigentums in Bezug auf die Daten ist, die bei der Verwendung des Produkts oder des verbundenen Dienstes voraussichtlich erzeugt werden, und, falls nicht, die Identität des Trägers des Geschäftsgeheimnisses, wie z. B. seinen Handelsnamen, seine Rechtsträgerkennung und die Anschrift des Ortes, an dem er ansässig ist;

i) wie der Nutzer Berechtigungen verwalten kann, um in die Nutzung von Daten einzuwilligen, nach Möglichkeit mit Optionen für eine detaillierte Einwilligung, darunter auch die Option, eine einem Dateninhaber zur Nutzung der Nutzerdaten oder den von einem Dateninhaber benannten Dritten erteilte Einwilligung zurückzuziehen oder geografische Ortsanschriften auszuschließen;

j) die Dauer der Vereinbarung zwischen dem Nutzer und dem Anbieter des verbundenen Dienstes sowie die Modalitäten für die vorzeitige Kündigung einer solchen Vereinbarung sowie den Mindestzeitraum, für den garantiert ist,

dass für den verbundenen Dienst Aktualisierungen in Bezug auf Sicherheit und Funktionalität bereitgestellt werden;

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

Artikel 3a

Datenkompetenz

(1) Bei der Durchführung dieser Verordnung fördern die Union und die Mitgliedstaaten Maßnahmen und Instrumente zur Entwicklung von Datenkompetenz, und zwar branchenübergreifend und unter Berücksichtigung der unterschiedlichen Bedürfnisse der betroffenen Gruppen von Nutzern, Verbrauchern und Unternehmen, unter anderem durch Aus- und Weiterbildungs-, Qualifizierungs- und Umschulungsprogramme und unter Sicherstellung eines ausgewogenen Verhältnisses in Bezug auf Geschlecht und Alter, um eine faire Datengesellschaft und einen fairen Datenmarkt zu ermöglichen.

Artikel 4

Die Rechte und Pflichten der Nutzer ***und Dateninhaber*** auf den Zugang zu den Daten***, auf die von vernetzten Produkten zugegriffen wird oder die bei der Erbringung verbundener Dienste erzeugt werden,*** und auf deren Nutzung ***und Bereitstellung***

(1) Soweit der Nutzer nicht direkt vom Produkt aus auf die Daten zugreifen kann, ***stellen*** Dateninhaber dem Nutzer ***alle Daten, auf die sie über ein verbundenes Produkt zugreifen oder die bei der Erbringung verbundener Dienste erzeugt werden,*** unverzüglich***, auf einfache und sichere Weise und in einem umfassenden strukturierten, gängigen und maschinenlesbaren Format***, kostenloskostenlos und***, soweit relevant und technisch machbar,*** kontinuierlich und in Echtzeit zur Verfügung***; dies umfasst auch die Bereitstellung aller aus diesen Daten abgeleiteten personenbezogenen Daten für eine betroffene Person gemäß Artikel 15 der Verordnung (EU) 2016/679, zusammen mit den entsprechenden Metadaten. Die Daten werden in der Form bereitgestellt, in der sie von dem vernetzten Produkt abgerufen oder von dem verbundenen Dienst erzeugt wurden, wobei nur***

geringfügige Anpassungen vorgenommen werden, die erforderlich sind, um sie für Dritte nutzbar zu machen, einschließlich der zugehörigen Metadaten, die für die Interpretation und Nutzung der Daten benötigt werden. Informationen, die durch komplexe proprietäre Algorithmen aus diesen Daten abgeleitet oder gefolgert werden, insbesondere wenn sie die Ausgabe mehrerer Sensoren in dem vernetzten Produkt kombinieren, fallen nicht unter die Verpflichtung des Dateninhabers zur Weitergabe von Daten an Nutzer oder Datenempfänger, es sei denn, zwischen dem Nutzer und dem Dateninhaber wurde eine andere Vereinbarung getroffen. Jedes an einen Dateninhaber gerichtete Ersuchen auf Datenzugang sollte auf einfaches Verlangen auf elektronischem Wege ***erfolgen***, soweit dies technisch machbar ist***, und gegebenenfalls den Typ, die Art oder den Umfang der angeforderten Daten angeben***.

(1a) Dateninhaber können ein Datenverlangen ablehnen, wenn der Zugang zu den Daten durch Unionsrecht oder nationales Recht verboten ist.

(1b) Nutzer und Dateninhaber können sich vertraglich darauf einigen, den Zugang zu oder die Verwendung oder die weitere gemeinsame Nutzung von Daten zu beschränken oder zu untersagen, wenn dies die gesetzlich vorgeschriebene Sicherheit des Produkts beeinträchtigen könnte. Jede Partei kann den Fall an den Datenkoordinator verweisen, damit dieser beurteilt, ob eine solche Beschränkung gerechtfertigt ist, insbesondere im Hinblick auf schwerwiegende Beeinträchtigungen der Gesundheit, der Sicherheit und des Wohlergehens von Menschen. Die zuständigen sektoralen Behörden erhalten in diesem Zusammenhang die Möglichkeit, technisches Fachwissen zur Verfügung zu stellen.

(1c) Wenn alle Bestimmungen dieser Verordnung und die in der vertraglichen Vereinbarung zwischen den Parteien vereinbarten Bedingungen eingehalten werden, haftet ein Dateninhaber gegenüber dem Nutzer nicht für Schäden, die sich aus den bereitgestellten Daten ergeben, sofern der Dateninhaber die Daten rechtmäßig im Einklang mit dem Unionsrecht und den nationalen Rechtsvorschriften verarbeitet hat und die einschlägigen Cybersicherheitsanforderungen und gegebenenfalls die technischen und organisatorischen Maßnahmen zur Wahrung der Vertraulichkeit der gemeinsam genutzten Daten erfüllt hat. Bei der Einhaltung dieser Verordnung haftet ein Nutzer, der Daten, auf die aus dem verbundenen Produkt zugegriffen wurde oder die er auf ein Verlangen gemäß Artikel 4 Absatz 1 erhalten hat, rechtmäßig einem

Dritten zur Verfügung stellt, oder ein Datenempfänger, der ihm von einem Dateninhaber zur Verfügung gestellte Daten rechtmäßig an einen Dritten weitergibt, nicht für Schäden, die sich aus der Weitergabe dieser Daten ergeben, sofern der Nutzer oder der Datenempfänger die Daten im Einklang mit dem Unionsrecht und den nationalen Rechtsvorschriften verarbeitet und den einschlägigen Cybersicherheitsanforderungen und gegebenenfalls den technischen und organisatorischen Maßnahmen zur Wahrung der Vertraulichkeit der gemeinsam genutzten Daten nachgekommen ist.

(1d) Die Dateninhaber dürfen die Ausübung der Rechte oder die Wahlmöglichkeiten der Nutzer nicht unangemessen erschweren, auch nicht dadurch, dass sie den Nutzern in nicht neutraler Weise Wahlmöglichkeiten anbieten oder die Autonomie, die Entscheidungsfreiheit oder die freie Wahl des Nutzers durch die Struktur, die Gestaltung, die Funktion oder die Funktionsweise einer Benutzeroberfläche oder eines Teils davon unterläuft oder beeinträchtigen.

(2) ***Die*** Dateninhaber ***verlangen*** vom Nutzer keine Informationen, die über das hinausgehen, was erforderlich ist, um dessen Eigenschaft als Nutzer gemäß Absatz 1 zu überprüfen. ***Die*** Dateninhaber ***bewahren*** 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. ***Ist eine Identifizierung gesetzlich vorgeschrieben, ermöglichen es die Dateninhaber den Nutzern, sich mit der EUid-Brieftasche gemäß der Verordnung (EU) Nr. 914/2014 zu identifizieren und zu authentifizieren.***

(3) Geschäftsgeheimnisse ***sind zu wahren und*** werden nur offengelegt, wenn vorab alle besonderen Maßnahmen ***gemäß der Richtlinie (EU) 2016/943*** getroffen worden sind, die erforderlich sind, um ***ihre*** Vertraulichkeit, insbesondere gegenüber Dritten, zu wahren. Der Dateninhaber ***oder, falls er nicht gleichzeitig der Dateninhaber ist, der Inhaber der Geschäftsgeheimnisse bestimmt die Daten, die als Geschäftsgeheimnisse geschützt sind***, und kann mit dem Nutzer ***technische und organisatorische*** Maßnahmen zur Wahrung der Vertraulichkeit der gemeinsam genutzten Daten, insbesondere gegenüber Dritten***, sowie Haftungsbestimmungen*** vereinbaren. ***Zu diesen technischen und organisatorischen Maßnahmen gehören gegebenenfalls Mustervertragsbestimmungen, vertrauliche Vereinbarungen,***

strenge Zugangsprotokolle, technische Standards und die Anwendung von Verhaltenskodizes. In Fällen, in denen der Nutzer diese Maßnahmen nicht umsetzt oder die Vertraulichkeit von Geschäftsgeheimnissen untergräbt, kann der Dateninhaber die Weitergabe von als Geschäftsgeheimnisse eingestuften Daten aussetzen. In solchen Fällen muss der Dateninhaber dem Datenkoordinator des Mitgliedstaats, in dem er gemäß Artikel 31 dieser Verordnung niedergelassen ist, unverzüglich mitteilen, dass er die Weitergabe der Daten ausgesetzt hat, und angeben, welche Maßnahmen nicht umgesetzt wurden oder bei welchen Geschäftsgeheimnissen gegen die Vertraulichkeit verstoßen wurde. Möchte der Nutzer die Entscheidung des Dateninhabers, die Weitergabe der Daten auszusetzen, anfechten, so entscheidet der Datenkoordinator innerhalb einer angemessenen Frist, ob die Weitergabe der Daten wieder aufgenommen wird oder nicht, und gibt, wenn ja, an, unter welchen Bedingungen sie wieder aufgenommen wird.

(4) Der Nutzer darf ▌ aufgrund eines Verlangens nach Absatz 1 erlangte Daten nicht zur Entwicklung eines Produktes oder eines Teils davon nutzen, das mit dem Produkt, von dem die Daten stammen, in ***direktem*** Wettbewerb steht***, und er darf diese Daten nicht nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers zu erlangen***.

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

(4b) Die Nutzer haben das Recht, nicht personenbezogene Daten, auf die über das verbundene Produkt zugegriffen wird oder die aufgrund eines Verlangens nach Absatz 1 erhalten wurden, entweder direkt, über einen Dateninhaber oder über Anbieter von Datenvermittlungsdiensten im Sinne der Verordnung (EU) 2022/868 zu kommerziellen oder nichtkommerziellen Zwecken an einen Datenempfänger weiterzugeben. Die Weitergabe von Daten zwischen einem Nutzer und einem Datenempfänger erfolgt über vertragliche Vereinbarungen, und die Bestimmungen des Kapitels IV über faire, angemessene und nichtdiskriminierende Bedingungen gelten entsprechend für die vertraglichen Vereinbarungen zwischen Nutzern und Datenempfängern.

(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 ***alle Bedingungen und Regeln des geltenden Datenschutzrechts eingehalten sind, insbesondere wenn*** es dafür eine gültige Rechtsgrundlage gemäß Artikel 6 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 der Verordnung (EU) 2016/679 ***und des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG*** erfüllt sind.

(6) ***Dateninhaber dürfen*** nicht personenbezogene Daten, ***auf die sie über ein vernetztes Produkt zugreifen*** oder die ***im Zuge der Bereitstellung eines*** verbundenen Dienstes erzeugt werden, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer nutzen. Der Dateninhaber darf ***die Nutzung des Produkts oder des verbundenen Dienstes nicht davon abhängig machen, dass der Nutzer ihm die Verarbeitung von Daten gestattet, die für die Funktionalität des Produkts oder die Erbringung des verbundenen Dienstes nicht erforderlich sind. Der Dateninhaber löscht die Daten, sobald sie für den vertraglich vereinbarten Zweck nicht mehr benötigt werden. Die Dateninhaber und Nutzer dürfen*** solche Daten, die bei der Nutzung des Produktes oder verbundenen Dienstes ***erlangt, gesammelt oder*** erzeugt werden, nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden ***der anderen Partei*** oder in die Nutzung des Produktes oder verbundenen Dienstes durch ***die andere Partei*** zu erlangen, wenn dies die gewerbliche Position ***der anderen Partei*** auf den Märkten, auf denen der Nutzer tätig ist, untergraben könnte.

(6a) Dateninhaber dürfen nicht personenbezogene Daten, auf die sie über das vernetzte Produkt gemäß Artikel 3 Absatz 2 Buchstabe a zugreifen, Dritten weder zu kommerziellen noch zu nichtkommerziellen Zwecken zur Verfügung stellen, außer zur Erfüllung ihrer Verpflichtungen gegenüber dem Nutzer. Gegebenenfalls verpflichten die Dateninhaber Dritte vertraglich, die von ihnen erhaltenen Daten nicht erneut weiterzugeben.

(6b) Ermöglicht die vertragliche Vereinbarung zwischen dem Nutzer und dem Dateninhaber die Verwendung von nicht personenbezogenen Daten, auf die sie über das vernetzte Produkt gemäß Artikel 3 Absatz 2a Buchstabe a zugreifen, kann der Dateninhaber diese Daten zu folgenden Zwecken verwenden:

a) Verbesserung der Funktionsweise des vernetzten Produkts oder der verbundenen Dienste;

b) Entwicklung neuer Produkte oder Dienste;

c) Anreicherung, Manipulation oder Zusammenführung mit anderen Daten, auch mit dem Ziel, den sich daraus ergebenden Datensatz Dritten zur Verfügung zu stellen, solange der abgeleitete Datensatz es nicht ermöglicht, einzelne Datenelemente zu ermitteln, die von dem vernetzten Produkt an den Dateninhaber übermittelt wurden, und es Dritten nicht erlaubt ist, diese Datenelemente aus dem Datensatz abzurufen.

(6c) Die Nutzer haben in Geschäftsbeziehungen zwischen Unternehmen das Recht, Datenempfängern oder Dateninhabern unter allen rechtmäßigen vertraglichen Bedingungen Daten zur Verfügung zu stellen, unter anderem durch die Vereinbarung, die weitere gemeinsame Nutzung dieser Daten zu beschränken oder einzuschränken, und als Gegenleistung für den Verzicht auf ihr Recht, diese Daten rechtmäßig zu verwenden oder weiterzugeben, eine angemessene Vergütung zu erhalten. Die Datenempfänger oder Dateninhaber dürfen das Angebot eines damit verbundenen Dienstes oder dessen Geschäftsbedingungen, einschließlich der Preisgestaltung, nicht von einer solchen Zustimmung des Nutzers abhängig machen oder den Nutzer in irgendeiner anderen Weise zwingen, täuschen oder manipulieren, damit er die Daten unter derartigen Vertragsbedingungen zur Verfügung stellt.

Artikel 5

Recht ***des Nutzers auf*** Weitergabe von Daten an Dritte

(1) Auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei***, beispielsweise eines autorisierten Datenvermittlungsdiensts im Sinne der Verordnung (EU) 2022/868, stellen die Dateninhaber*** die Daten***, auf die sie von einem vernetzten Produkt aus zugreifen oder die bei der Erbringung*** eines damit verbundenen Dienstes ***erzeugt werden,*** einem Dritten unverzüglich***, auf einfache und sichere Weise, in einem umfassenden, strukturierten, allgemein verwendeten und maschinenlesbaren Format***, für den Nutzer kostenlos, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, und***, soweit relevant und technisch machbar,*** kontinuierlich und in Echtzeit bereit. ***Handelt es sich bei dem Nutzer um eine betroffene Person, so werden personenbezogene Daten für die von der betroffenen Person angegebenen Zwecke verarbeitet, wie z. B.***

a) die Erbringung von Anschlussdiensten, wie die Wartung und Reparatur des Produkts, einschließlich der Erbringung eines Anschlussdienstes, der mit einem vernetzten Produkt oder verbundenen Dienst des Dateninhabers in Wettbewerb steht;

b) die Ermöglichung der Aktualisierung der Software des vernetzten Produkts oder verbundenen Dienstes durch den Nutzer, insbesondere zur Behebung von Sicherheits- und Nutzbarkeitsproblemen;

c) spezifische, in der Union anerkannte Datenvermittlungsdienste oder spezifische Dienste, die von in der Union anerkannten datenaltruistischen Organisationen gemäß den Bedingungen und Anforderungen der Kapitel III und IV der Verordnung (EU) 2022/868 erbracht werden.

Die Daten werden in der Form bereitgestellt, in der sie von dem Produkt abgerufen wurden, wobei nur geringfügige Anpassungen vorgenommen werden, die erforderlich sind, um sie für Dritte nutzbar zu machen, einschließlich der zugehörigen Metadaten, die für die Interpretation und Nutzung der Daten benötigt werden. Informationen, die durch komplexe proprietäre Algorithmen aus diesen Daten abgeleitet oder gefolgert werden, insbesondere wenn sie die Ausgabe mehrerer Sensoren in dem vernetzten Produkt kombinieren, fallen nicht unter die Verpflichtung des Dateninhabers zur Weitergabe von Daten an Nutzer oder Datenempfänger, es sei denn, zwischen dem Nutzer und dem Dateninhaber wurde eine andere Vereinbarung getroffen.

(1a) Das Recht nach Absatz 1 gilt nicht für Daten, die aus der Nutzung eines Produkts oder einem damit verbundenen Dienst im Zusammenhang mit der Erprobung anderer neuer Produkte, Stoffe oder Verfahren, die noch nicht auf dem Markt sind, gewonnen wurden, es sei denn, die Verwendung durch einen Dritten wird durch die Vereinbarung zwischen dem Unternehmen und dem Nutzer gestattet, mit dem der Nutzer die Verwendung eines seiner Produkte zur Erprobung anderer neuer Produkte, Stoffe oder Verfahren vereinbart hat.

(2) Ein Unternehmen, das zentrale Plattformdienste erbringt und für mindestens einen dieser Dienste nach Artikel [...] der Verordnung ***(EU) 2022/1925*** als Torwächter benannt wurde, kommt nicht als zulässiger ***Datenempfänger*** 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 ***Datenempfänger*** braucht keine Informationen herauszugeben, die über das hinausgehen, was erforderlich ist, um dessen Eigenschaft als Nutzer oder ***Datenempfänger*** gemäß Absatz 1 zu überprüfen. ***Die*** Dateninhaber ***bewahren*** keine Informationen über den Zugang des ***Datenempfängers*** zu den verlangten Daten auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des ***Datenempfängers*** und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist.

(4) Der ***Datenempfänger*** darf keine Zwangsmittel einsetzen oder ▌ Lücken in der technischen Infrastruktur eines 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 ***erlangt, gesammelt oder*** 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 ***ausdrücklich*** zugestimmt und hat die technische Möglichkeit, diese Zustimmung jederzeit ***auf einfache Weise*** zu widerrufen.

(6) ***Handelt es sich bei der*** betroffene Person ***nicht um den Nutzer, der den Zugang verlangt,*** so ***darf der Dateninhaber*** personenbezogene Daten, die bei ***ihrer*** Nutzung eines Produktes oder verbundenen Dienstes ***erlangt, gesammelt oder*** erzeugt werden, ***und von dieser Nutzung abgeleitete oder gefolgerte Daten einem Dritten*** nur dann ***bereitstellen***, wenn es dafür eine gültige Rechtsgrundlage gemäß Artikel ***6*** der

Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 der Verordnung (EU) 2016/679 ***und des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG*** 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 ***des Ersuchens*** unbedingt erforderlich ist und der Dritte alle zwischen ihm und dem Dateninhaber ***oder dem Inhaber der Geschäftsgeheimnisse, wenn dieser nicht gleichzeitig der Dateninhaber ist,*** vereinbarten besonderen Maßnahmen ***vor der Offenlegung*** getroffen hat, die erforderlich sind, um die Vertraulichkeit des Geschäftsgeheimnisses zu wahren. In diesem Fall ***bestimmt der Dateninhaber oder der Inhaber der Geschäftsgeheimnisse die Daten, die*** als Geschäftsgeheimnisse ***geschützt werden,*** und die ***technischen und organisatorischen*** Maßnahmen zur Wahrung ***ihrer*** Vertraulichkeit ***sowie die Haftungsbestimmungen***. ***Diese technischen und organisatorischen Maßnahmen werden*** in der Vereinbarung zwischen dem Dateninhaber ***oder dem Inhaber der Geschäftsgeheimnisse*** und dem Dritten festgelegt***, gegebenenfalls auch durch Mustervertragsbestimmungen, strenge Zugangsprotokolle, vertrauliche Vereinbarungen, technische Standards und die Anwendung von Verhaltenskodizes. In Fällen, in denen der Dritte diese Maßnahmen nicht umsetzt oder die Vertraulichkeit von Geschäftsgeheimnissen untergräbt, kann der Dateninhaber die Weitergabe von als Geschäftsgeheimnisse eingestuften Daten aussetzen. In solchen Fällen muss der Dateninhaber dem Datenkoordinator des Mitgliedstaats, in dem er gemäß Artikel 31 niedergelassen ist, unverzüglich mitteilen, dass er die Weitergabe der Daten ausgesetzt hat, und angeben, welche Maßnahmen nicht umgesetzt wurden oder bei welchen Geschäftsgeheimnissen gegen die Vertraulichkeit verstoßen wurde. Möchte der Dritte die Entscheidung des Dateninhabers, die Weitergabe der Daten auszusetzen, anfechten, so entscheidet der Datenkoordinator innerhalb einer angemessenen***

Frist, ob die Weitergabe der Daten wieder aufgenommen wird oder nicht, und gibt, falls dies der Fall ist, an, unter welchen Bedingungen sie wieder aufgenommen wird.

(9) Das Recht gemäß Absatz 1 darf die Rechte anderer ***betroffener*** Personen ***gemäß den geltenden Datenschutzvorschriften*** nicht beeinträchtigen.

Artikel 6

Pflichten ***von Datenempfängern***, die Daten auf Verlangen des Nutzers erhalten

(1) Ein ***Datenempfänger*** verarbeitet ▌ ihm nach Artikel 5 bereitgestellte personenbezogene Daten nur für die Zwecke und unter den Bedingungen, die er mit dem Nutzer vereinbart hat, und ***wenn alle Bedingungen und Regeln des geltenden Datenschutzrechts eingehalten sind, insbesondere 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 und des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG erfüllt sind, und*** – soweit personenbezogene Daten betroffen sind – vorbehaltlich der Rechte der betroffenen Person. ***Der Datenempfänger*** löscht die Daten, sobald sie für den vertraglich vereinbarten Zweck nicht mehr benötigt werden***, sofern mit dem Nutzer nicht etwas anderes vereinbart wurde***.

(2) Der ***Datenempfänger*** darf nicht

a) ***die Ausübung der Rechte oder die Wahlmöglichkeiten der Nutzer übermäßig erschweren, auch nicht indem er den Nutzern Wahlmöglichkeiten auf nicht neutrale Weise anbietet, oder*** den Nutzer in irgendeiner Weise zwingen, täuschen oder manipulieren ***oder*** – auch mittels einer digitalen Schnittstelle mit dem Nutzer ***oder eines Teils davon, einschließlich ihrer Struktur, Gestaltung, Funktion oder Art der Bedienung*** – die Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten des Nutzers untergraben oder beeinträchtigen;

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 steht im Einklang mit jener Verordnung***;

c) die erhaltenen Daten einem anderen Dritten bereitstellen, ***ohne den Nutzer in einer klaren und leicht zugänglichen Weise darauf hinzuweisen und seine ausdrückliche vertragliche Zustimmung einzuholen***;

d) die erhaltenen Daten einem Unternehmen, das zentrale Plattformdienste erbringt und für mindestens einen dieser Dienste gemäß Artikel ***3*** der ***[Verordnung (EU) 2022/1925*** (Gesetz über digitale Märkte)] als Torwächter 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; ***auch darf der Datenempfänger nicht personenbezogene Daten, die bei der Nutzung des Produkts oder verbundenen Dienstes erzeugt werden, nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Dateninhabers oder in die Nutzung durch den Dateninhaber zu erlangen, wenn dies die gewerbliche Position des Dateninhabers auf den Märkten, auf denen der Dateninhaber tätig ist, untergraben könnte.***

ea) die erhaltenen Daten in einer Weise verwenden, die die Sicherheit des Produkts oder des verbundenen Dienstes bzw. der verbundenen Dienste beeinträchtigt;

eb) gegebenenfalls die mit dem Dateninhaber oder dem Inhaber der Geschäftsgeheimnisse gemäß Artikel 5 Absatz 8 dieser Verordnung getroffenen Maßnahmen missachten und die Vertraulichkeit von Geschäftsgeheimnissen verletzen;

ec) die Daten verwenden, um vertrauliche Informationen über den Schutz kritischer Infrastrukturen im Sinne von Artikel 2 Buchstabe d der Richtlinie 2008/114/EG zu stören.

▌

(2a) Der Dritte trägt die Verantwortung, für die Sicherheit und den Schutz der Daten zu sorgen, die er von einem Dateninhaber erhält.

Artikel 7

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

(1) Die Pflichten nach diesem Kapitel gelten nicht für ▌ Unternehmen ▌, 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***, und sofern das Kleinst- oder Kleinunternehmen nicht als Unterauftragnehmer mit der Herstellung oder dem Entwurf eines Produktes oder der Erbringung eines verbundenen Dienstes beauftragt wurde***.

(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 vereinbart er mit einem Datenempfänger die Modalitäten für die Bereitstellung der Daten, und*** dies geschieht zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise im Einklang mit den Bestimmungen dieses Kapitels und des Kapitels IV.

(2) 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 ***in Bezug auf die Modalitäten der Weitergabe von Daten*** 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. ***Hat*** ein Datenempfänger ***begründete Bedenken***, dass die Bedingungen, unter denen ihm Daten bereitgestellt werden, diskriminierend sind, so ***legt der Dateninhaber dem Datenempfänger unverzüglich den Nachweis vor, der belegt***, dass keine Diskriminierung vorliegt.

(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.

(5a) ***Dateninhaber und Datenempfänger treffen alle erforderlichen rechtlichen, organisatorischen und technischen Maßnahmen, um die Sicherheit und Integrität der Datenübermittlung zu gewährleisten.***

(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 4 Absatz 3, des Artikels 5 Absatz 8 und*** 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 ***im Rahmen von Geschäftsbeziehungen zwischen Unternehmen*** vereinbart wird, muss ***diskriminierungsfrei und*** angemessen sein. ***Dateninhaber, Datenempfänger oder Dritte dürfen von den Verbrauchern oder betroffenen Personen weder direkt noch indirekt ein Entgelt, einen Ausgleich oder Kosten im Zusammenhang mit der gemeinsamen Nutzung von Daten oder dem Zugang zu Daten verlangen.***

(2) Ist der Datenempfänger ***eine gemeinnützige Forschungsorganisation oder ein KMU*** im Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/EG ***und haben diese Unternehmen keine Partnerunternehmen oder verbundenen Unternehmen gemäß der Begriffsbestimmung in Artikel 3 des Anhangs der Empfehlung 2003/361/EG und sind keine KMU***, 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. ***Im Falle eines KMU informiert der Dateninhaber aktiv über die Verpflichtung, die Daten vorzugsweise auf der Grundlage eines kostenorientierten Modells bereitzustellen.***

(2a) Die Kommission arbeitet Leitlinien zur Festlegung von Kriterien für Kategorien von Kosten im Zusammenhang mit der Bereitstellung von Daten aus, die die Grundlage für die Gewährung eines Ausgleichs gemäß Absatz 1 bilden.

(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) ***Nutzer,*** Dateninhaber und Datenempfänger haben Zugang zu Streitbeilegungsstellen, die nach Absatz 2 dieses Artikels zugelassen sind, um Streitigkeiten in Bezug auf ***die Erfüllung der Verpflichtung des Dateninhabers, dem Datenempfänger auf Verlangen des Nutzers Daten zur Verfügung zu stellen,*** 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***, 9 und 13*** 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 ***des Mitgliedstaats, in dem die Stelle niedergelassen ist,*** 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.

(7a) Die Streitbeilegungsstellen machen jährliche Tätigkeitsberichte öffentlich zugänglich. Jeder Jahresbericht muss insbesondere folgende Angaben umfassen:

a) die Anzahl der eingegangenen Streitigkeiten;

b) eine Zusammenstellung der Ergebnisse dieser Streitigkeiten;

c) den durchschnittlichen Zeitaufwand bei der Beilegung der Streitigkeiten;

d) die häufigsten Gründe, die zu Streitigkeiten zwischen den Parteien führen.

(7b) Um den Austausch von Informationen und bewährten Verfahren zu erleichtern, kann die öffentliche Streitbeilegungsstelle beschließen, Empfehlungen beizufügen, wie solche Probleme zu vermeiden oder zu beheben sind.

(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 ***und Verschlüsselung***, anwenden, um eine unbefugte Offenlegung und einen unbefugten Zugang zu den Daten***, einschließlich Metadaten,*** zu verhindern und die Einhaltung der Artikel ***4, 5, 6, 8,*** 9 und 10 sowie der für die Datenbereitstellung vereinbarten Vertragsbedingungen sicherzustellen. ***Bei solchen*** technischen Schutzmaßnahmen dürfen ***weder Datenempfänger unterschiedlich behandelt noch verhindert werden,*** dass ein Nutzer sein Recht, wirksam eine Kopie zu erhalten***, Daten abzurufen, zu verwenden oder auf diese zuzugreifen oder*** 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. ***Legt ein Nutzer oder Dateninhaber konkrete schlüssige Beweise für die unrechtmäßige Verwendung oder die unbefugte Weitergabe der Daten an Dritte durch den Datenempfänger vor, so stellt der Datenempfänger auf Anfrage des Nutzers oder Dateninhabers Informationen darüber bereit, wie die Daten verwendet wurden oder an wen sie weitergegeben wurden.***

(2) Hat ein Datenempfänger dem Dateninhaber zwecks Erlangung der Daten ▌ falsche Informationen gegeben, Täuschungen und Zwangsmittels eingesetzt oder

offenkundige Lücken in der dem Schutz der Daten dienenden technischen Infrastruktur des Dateninhabers missbraucht, die bereitgestellten Daten für nicht genehmigte Zwecke***, einschließlich der Entwicklung eines Produkts, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht, im Sinne von Artikel 6 Absatz 2 Buchstabe e,*** genutzt oder ▌Daten ***unrechtmäßig*** an eine andere Partei weitergegeben, ***haftet der Datenempfänger für den Schaden, der dem Geschädigten durch die missbräuchliche Verwendung oder Weitergabe der Daten entstanden ist, und*** muss ***den Aufforderungen*** des Dateninhabers ***oder des Inhabers der Geschäftsgeheimnisse, falls es sich nicht um dieselbe juristische Person handelt,*** unverzüglich nachkommen und

a) die bereitgestellten Daten ▌und alle etwaigen Kopien davon ***löschen***,

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,

ba) den Nutzer über die unbefugte Nutzung oder Offenlegung der Daten und über die Maßnahmen informieren, die ergriffen wurden, um die unbefugte Nutzung oder Offenlegung der Daten zu unterbinden,

bb) den Dateninhaber über die Offenlegung dieser Daten unterrichten.

(2a) Der Nutzer hat die gleichen Befugnisse wie der Dateninhaber und der Datenempfänger hat die gleichen Pflichten nach Absatz 2, wenn der Datenempfänger gegen Artikel 6 Absatz 2 Buchstaben a und b verstoßen hat.

▌

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 ***nichtig***.

(2a) Eine Vertragsklausel in einer Datenweitergabevereinbarung zwischen Dateninhabern und Datenempfängern, die zum Nachteil der betroffenen Personen die Anwendung ihrer Rechte auf Privatsphäre und Datenschutz untergräbt, davon abweicht oder ihre Wirkung abändert, ist nichtig.

(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 ▌ 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 anderen Unternehmen einseitig auferlegt hat, ▌ ist für letzteres Unternehmen ***bzw. den Datenempfänger oder Datennutzer*** nicht bindend, wenn sie missbräuchlich ist.

(1a) Eine Vertragsbedingung gilt nicht als missbräuchlich, wenn sie aus anwendbarem Unionsrecht hervorgeht.

(2) Eine Vertragsklausel ist missbräuchlich, wenn sie ***die Fähigkeit der Partei, der die Klausel einseitig auferlegt wurde, objektiv beeinträchtigt, ihr berechtigtes geschäftliches Interesse an den betreffenden Daten zu schützen*** und 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***, oder wenn sie ein erhebliches Ungleichgewicht zwischen den Rechten und Pflichten der Vertragsparteien verursacht***.

(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, ***einschließlich, wenn diese Daten ohne die vorherige Zustimmung der jeweiligen Parteien sensible Geschäftsdaten enthalten, oder Daten, die als Geschäftsgeheimnis oder durch Rechte des geistigen Eigentums geschützt sind***;

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;

ca) die einseitige Wahl des zuständigen Gerichts oder die Zahlung der mit dem Verfahren verbundenen Kosten vorschreiben

cb) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, die Vereinbarung innerhalb einer angemessenen Frist zu kündigen.

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 aufgrund des Vertrags zu zahlenden Vorlaufpreis oder eine andere wesentliche Bedingung für die Weitergabe der Daten erheblich zu ändern, ohne dass die andere Partei das Recht hat, den Vertrag zu kündigen, oder*** 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.

(6a) Die Partei, die die beanstandete Klausel vorgelegt hat, kann sich nicht darauf berufen, dass es sich um eine missbräuchliche Klausel handelt.

(7) Dieser Artikel gilt weder für Vertragsklauseln, in denen der Hauptgegenstand des Vertrags festgelegt wird, noch ***berührt er die Möglichkeit der Parteien, den zu zahlenden Preis auszuhandeln***.

(8) Die Parteien eines unter Absatz 1 fallenden Vertrags ***schließen*** die Anwendung dieses Artikels nicht ***aus***, ***weichen*** davon nicht ***ab*** und ***ändern*** dessen Wirkungen nicht ***ab***.

(8a) Dieser Artikel gilt für alle neuen nach dem ... [Datum des Inkrafttretens dieser Verordnung] geschlossenen Verträge. Den Unternehmen wird eine Frist von drei Jahren ab diesem Zeitpunkt eingeräumt, um bestehende vertragliche Verpflichtungen, die Gegenstand dieser Verordnung sind, zu überprüfen.

(8b) ***Angesichts der Geschwindigkeit, in der Innovationen auf den Märkten auftreten, wird die Liste der missbräuchlichen Vertragsklauseln in Artikel 13 regelmäßig von der Kommission überprüft und erforderlichenfalls entsprechend den neuen Geschäftspraktiken aktualisiert.***

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 ***ein spezifisches, hinreichend begründetes sowie zeitlich befristetes und in seinem Umfang begrenztes*** Verlangen stellt ein Dateninhaber***, der eine juristische Person ist,*** einer öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union, die eine außergewöhnliche Notwendigkeit der Nutzung der verlangten Daten nachweist, ***nicht personenbezogene*** Daten bereit***, die zum Zeitpunkt des Verlangens verfügbar sind, einschließlich Metadaten***.

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

(2a) ***Dieses Kapitel schließt freiwillige Vereinbarungen zwischen Unternehmen und öffentlichen Stellen und Organen, Einrichtungen oder sonstigen Stellen der Union über die gemeinsame Nutzung von Daten zum Zwecke der Erbringung öffentlicher Dienstleistungen nicht aus, auch für außergewöhnliche Bedürfnisse, sofern diese in ihren Verträgen festgelegt sind.***

Artikel 15

Außergewöhnliche Notwendigkeit der Datennutzung ▌

Eine außergewöhnliche Notwendigkeit der Nutzung ***nicht personenbezogener*** Daten im Sinne dieses Kapitels ***ist zeitlich befristet und im Umfang begrenzt und*** liegt ▌ unter den folgenden Umständen vor:

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

b) ***die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union handelt in Situationen, die keinen Notstand darstellen, auf der Grundlage von Unions- oder nationalem Recht und hat bestimmte Daten ermittelt, die ihr nicht zur Verfügung stehen und die*** erforderlich ***sind, um eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse zu erfüllen, wie die Vorbeugung eines öffentlichen Notstands oder die*** Erholung nach einem öffentlichen Notstand***, wobei die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union nicht in der Lage ist, diese Daten auf einem der folgenden Wege zu beschaffen: durch eine freiwillige Vereinbarung, durch Erwerb der Daten auf dem Markt oder durch Rückgriff auf bestehende Verpflichtungen zur Bereitstellung von Daten.***

▌

Artikel 15a

Zentrale Stelle für die Bearbeitung von Verlangen öffentlicher Stellen

(1) Der nach Artikel 31 benannte Datenkoordinator ist für die Koordinierung der Anträge der öffentlichen Stellen des betreffenden Mitgliedstaats gemäß Artikel 14 Absatz 1 zuständig, um sicherzustellen, dass die Anträge den Anforderungen dieses Kapitels entsprechen, und übermittelt sie dem Dateninhaber. Er sorgt dafür, dass nicht unterschiedliche öffentliche Stellen in seinem Hoheitsgebiet mehrere Anfragen an denselben Dateninhaber richten.

(2) Die Mitgliedstaaten unterrichten regelmäßig die Kommission über die Anträge gemäß Artikel 14 Absatz 1.

(3) Benötigt eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union aufgrund einer außergewöhnlichen Notwendigkeit gemäß Artikel 14 Absatz 1 Daten desselben Dateninhabers in mehr als einem Mitgliedstaat, so arbeiten die zuständigen Behörden der Mitgliedstaaten gemäß Artikel 22 zusammen, um ihre Anfragen zu koordinieren, wo dies erforderlich ist, um den Verwaltungsaufwand für die Dateninhaber so gering wie möglich zu halten.

(4) Die Kommission entwickelt ein Musterformular für Anträge gemäß Artikel 17.

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) ▌ Dieses Kapitel ***gilt*** nicht für öffentliche Stellen sowie Organe, Einrichtungen und sonstige Stelle der Union, ***die*** Tätigkeiten der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung durchführen, oder für Zoll- oder Steuerverwaltung. 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.

(2a) Unternehmen, die in den Anwendungsbereich dieses Kapitels fallen, unterrichten ihre Nutzer darüber, dass Daten im Falle außergewöhnlicher Umstände weitergegeben werden könnten.

Artikel 17

Datenbereitstellungsverlangen

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

a) ***Daten in ihrem Zuständigkeitsbereich anfordern und*** angeben, welche ***Datensätze*** benötigt werden,

b) die außergewöhnliche Notwendigkeit, für die die Daten verlangt werden***, und die Einhaltung der in Artikel 15 genannten Bedingungen nachweisen***,

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

ca) wenn möglich, angeben, wann die Daten von all den Parteien, die Zugang zu den Daten haben, voraussichtlich gelöscht werden,

cb) die Wahl des Dateninhabers, an den das Verlangen gerichtet ist, begründen,

cc) alle anderen öffentlichen Stellen oder Organe, Einrichtungen oder sonstigen Stellen der Union und Dritten angeben, denen die angeforderten Daten voraussichtlich zur Verfügung gestellt werden;

cd) die Identität des Dritten im Sinne von Absatz 4 dieses Artikels und Artikel 21 dieser Verordnung offenlegen;

ce) alle einschlägigen IKT-Sicherheitsmaßnahmen in Bezug auf die Übertragung und Speicherung von Daten anwenden;

d) die Rechtsgrundlage für das Datenverlangen angeben;

da) die geografischen Grenzen angeben, die für das Datenverlangen gelten;

e) die Frist angeben, innerhalb deren die Daten bereitzustellen sind ***und*** 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***;***

ea) eine Erklärung über den rechtmäßigen und sicheren Umgang mit den angeforderten Daten abgeben, einschließlich der Wahrung der Vertraulichkeit von Geschäftsgeheimnissen;

eb) sicherstellen, dass die Bereitstellung der Daten den Dateninhaber nicht in eine Situation bringt, die gegen Unionsrecht oder nationales Recht verstößt, oder eine Haftung des Dateninhabers für Verstöße oder Schäden infolge des von einer öffentlichen Stelle oder einem Organ, einer Einrichtungen oder einer sonstigen Stelle der Union beantragten Datenzugangs begründet.

(2) Ein Datenverlangen nach Absatz 1 muss

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

aa) über die zuständige Behörde eingereicht werden,

ab) genaue Angaben zur Art der angeforderten Daten enthalten und sich auf die Daten beziehen, die dem Dateninhaber zum Zeitpunkt des Verlangens zur Verfügung stehen,

b) im Hinblick auf die Granularität und den Umfang der verlangten Daten sowie die Häufigkeit des Zugangs zu den verlangten Daten ***gerechtfertigt sein und*** 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; ***gegebenenfalls müssen darin die Maßnahmen, die gemäß Artikel 19 Absatz 2 zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen zu treffen sind, gegebenenfalls auch durch die Verwendung von Mustervertragsbedingungen, technischen Normen und Verhaltenskodizes, angegeben sein,***

d) ***nur*** nicht personenbezogene Daten betreffen,

e) dem Dateninhaber Aufschluss über die Sanktionen geben, die nach Artikel 33 von ***einem Datenkoordinator*** nach Artikel 31 verhängt werden, wenn er dem Verlangen nicht nachkommt,

f) ***dem in Artikel 31 genannten Datenkoordinator übermittelt werden, der das Verlangen*** unverzüglich im Internet veröffentlicht, ***der Datenkoordinator kann die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union unterrichten, wenn der Dateninhaber die angeforderten Daten bereits als Antwort auf ein zuvor zu demselben Zweck von einer anderen öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union eingereichtes Verlangen bereitgestellt hat.***

(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 ***und der Verordnung (EU) 2022/868*** zur Verfügung stellen. Die Richtlinie (EU) 2019/1024 ***und die Verordnung (EU) 2022/868 finden*** keine Anwendung auf nach diesem Kapitel erlangte Daten im Besitz öffentlicher Stellen.

(4) Durch Absatz 3 wird eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union nicht daran gehindert, nach diesem Kapitel erlangte Daten mit anderen öffentlichen Stellen und mit Organen, Einrichtungen oder sonstigen Stellen der Union ***zwecks*** Wahrnehmung der in Artikel 15 genannten Aufgaben auszutauschen***, wie in dem Verlangen gemäß Absatz 1 Buchstabe cc angegeben,*** oder die Daten einem Dritten bereitzustellen, den sie im Rahmen einer öffentlich

zugänglichen Vereinbarung mit technischen Inspektionen oder anderen Aufgaben betraut hat. ***Dadurch werden Dritte vertraglich verpflichtet, die Daten nicht für andere Zwecke zu verwenden und nicht an Dritte weiterzugeben, wenn eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union Daten gemäß diesem Absatz übermittelt oder zur Verfügung stellt, und sie teilt dies dem Dateninhaber, von dem die Daten empfangen wurden, unverzüglich mit. Innerhalb von fünf Tagen nach Erhalt dieser Mitteilung ist der Dateninhaber berechtigt, einen begründeten Einwand gegen diese Übermittlung oder Zurverfügungstellung von Daten vorzulegen. Im Fall einer Zurückweisung des begründeten Einwands durch die öffentliche Stelle, das Organ, die Einrichtung oder sonstige Stelle der Union kann der Dateninhaber die Angelegenheit dem in Artikel 31 genannten Datenkoordinator zur Kenntnis bringen.*** Die öffentlichen Stellen oder Organe, Einrichtungen oder sonstigen Stellen der Union ***sowie Dritte, die die Daten erhalten, müssen den in*** Artikel 19 ***festgelegten Pflichten nachkommen***.

Die gemäß diesem Kapitel erhaltenen Daten dürfen nur für den in dem Ersuchen genannten Zweck verwendet werden. Öffentliche Stellen, Organe, Einrichtungen oder sonstige Stellen der Union verpflichten Dritte, mit denen sie sich über die Weitergabe von Daten gemäß Absatz 4 verständigt haben, die Daten nicht für andere Zwecke zu verwenden und nicht an andere Parteien weiterzugeben.

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 ***unter Berücksichtigung der Zeit, die für die notwendigen technischen, organisatorischen und rechtlichen Maßnahmen erforderlich ist,*** 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 ***30*** Arbeitstagen nach Eingang das Verlangen aus einem der folgenden Gründe ablehnen oder dessen Änderung beantragen:

a) die Daten ***stehen dem Dateninhaber zum Zeitpunkt des Verlangens nicht zur Verfügung***, ***aa)***
die vorgehaltenen Sicherheitsmaßnahmen betreffend die Übermittlung, Speicherung und Wahrung der Vertraulichkeit sind unzureichend,

ab) ein ähnliches Verlangen zu demselben Zweck wurde bereits von einer anderen öffentlichen Stelle oder einem Organ, einer Einrichtung oder einer sonstigen Stelle der Union gestellt und der Dateninhaber wurde nicht gemäß Artikel 19 Absatz 1 Buchstabe c über die Vernichtung der Daten unterrichtet.

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

▌

(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 ▌pseudonymisiert der Dateninhaber die ***bereitzustellenden personenbezogenen*** Daten.

(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 ***der*** in Artikel 31 genannte ***Datenkoordinator*** mit der Angelegenheit befasst***, wovon das Recht unbeschadet bliebe, gemäß dem geltenden Unionsrecht oder dem geltenden nationalen Recht die Streitigkeit einem Zivil- oder Verwaltungsgericht vorzulegen***.

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***, und ein statistisches Amt oder eine Forschungsorganisation, das bzw. die Daten aufgrund eines Verlangens nach Artikel 21 Absatz 1 erhalten hat***,

▌

b) trifft – soweit die Verarbeitung personenbezogener Daten erforderlich ist – technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen***, sorgt für ein hohes Maß an Sicherheit und beugt der unbefugten Offenlegung von Daten vor***,

ba) führt die erforderlichen technischen und organisatorischen Maßnahmen zur Beherrschung von Cyberrisiken durch, die die Vertraulichkeit, Integrität oder Verfügbarkeit der verlangten Daten beeinträchtigen könnten,

bb) unterrichtet den Dateninhaber, von dem die Daten erhalten wurden, über jeden Cybervorfall, der die Vertraulichkeit, Integrität oder Verfügbarkeit der erhaltenen Daten beeinträchtigt, so früh wie möglich, spätestens jedoch 72 Stunden, nachdem er den Vorfall festgestellt hat, und zwar unbeschadet der Meldepflichten gemäß der Verordnung (EU) XXX/XXXX (EUIBAL) und der Richtlinie (EU) 2022/2555. Diese Stellen haften für Schäden aufgrund einer Cybersicherheitsverletzung, wenn sie nicht die Maßnahmen nach Absatz 1 Buchstabe ba ergriffen haben.

c) ***löscht*** die Daten, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und teilt dem Dateninhaber die ***Löschung*** der Daten unverzüglich mit.

(1a) Öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellen der Union oder Dritte, die Daten gemäß diesem Kapitel erhalten, dürfen nicht

a) die erhaltenen Daten verwenden, um Produkte oder Dienste zu entwickeln oder bestehende Produkte oder Dienste zu verbessern, die mit dem Produkt oder Dienst, von dem die Daten stammen, im Wettbewerb stehen,

b) die erhaltenen Daten verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktions- oder Betriebsmethoden des Dateninhabers zu erlangen, und sie dürfen die Daten zu diesem Zweck auch nicht an einen anderen Dritten weitergeben, oder

c) die Daten für einen dieser Zwecke an einen anderen Dritten weitergeben.

(2) Eine Offenlegung von 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 ***eines*** Verlangens ***nach Artikel 15***

unerlässlich ist. In diesem Fall ***muss der Dateninhaber die Daten bestimmen, die als Geschäftsgeheimnis geschützt sind***. ***Die*** öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union trifft ***vorab alle erforderlichen und geeigneten technischen und organisatorischen*** Maßnahmen***, die mit dem Dateninhaber oder mit dem Inhaber der Geschäftsgeheimnisse, falls es sich nicht um dieselbe juristische Person handelt, vereinbart wurden,*** um die Vertraulichkeit dieser Geschäftsgeheimnisse zu wahren***, gegebenenfalls auch durch die Verwendung von Mustervertragsbedingungen und technischen Normen sowie die Anwendung von Verhaltenskodizes***.

(2a) ***Wenn eine öffentliche Stelle oder ein Organ, eine Einrichtung oder eine sonstige Stelle der Union einem Dritten Daten zur Wahrnehmung der Aufgaben, mit denen sie bzw. es aufgrund der Beauftragung mit technischen Inspektionen oder sonstigen Aufgaben gemäß Artikel 17 Absatz 4 betraut wurde, übermittelt oder bereitstellt, so werden die vom Dateninhaber als solche bestimmten Geschäftsgeheimnisse nur in dem Umfang offengelegt, in dem sie für den Dritten unbedingt erforderlich sind, um die ausgelagerten Aufgaben wahrzunehmen, und sie werden nur offengelegt, sofern alle erforderlichen spezifischen Maßnahmen, die zwischen dem Dateninhaber und dem Dritten vereinbart wurden, im Voraus getroffen werden, einschließlich technischer und organisatorischer Maßnahmen zur Wahrung der Vertraulichkeit dieser Geschäftsgeheimnisse, gegebenenfalls auch durch die Verwendung von Mustervertragsbedingungen und technischen Standards sowie die Anwendung von Verhaltenskodizes.***

(2b) ***In Fällen, in denen die öffentliche Stelle bzw. das Organ, die Einrichtung oder die sonstige Stelle der Union, die bzw. das Daten angefordert hat, oder der Dritte, dem die Daten gemäß Artikel 17 Absatz 4 bereitgestellt wurden, diese Maßnahmen nicht umsetzt oder gegen die Vertraulichkeit von Geschäftsgeheimnissen verstößt, ist der Dateninhaber befugt, die Weitergabe von als Geschäftsgeheimnisse eingestuften Daten auszusetzen. In solchen Fällen teilt der Dateninhaber dem Datenkoordinator des Mitgliedstaats, in dem er gemäß Artikel 31 niedergelassen ist, unverzüglich mit, dass er die Weitergabe der Daten ausgesetzt hat, und angeben, welche Maßnahmen nicht umgesetzt wurden oder bei welchen Geschäftsgeheimnissen gegen die Vertraulichkeit verstoßen wurde. Möchte die öffentliche Stelle oder das Organ, die Einrichtung oder die sonstige Stelle der Union oder der Dritte die Entscheidung des***

Dateninhabers, die Weitergabe der Daten auszusetzen, anfechten, so entscheidet der Datenkoordinator innerhalb einer angemessenen Frist, ob die Weitergabe der Daten wiederaufgenommen wird oder nicht, und gibt, wenn ja, an, unter welchen Bedingungen sie wiederaufgenommen wird.

(2c) Eine öffentliche Stelle oder ein Organ, eine Einrichtung oder sonstige Stelle der Union ist für die Sicherheit der erhaltenen Daten verantwortlich.

(2) Eine öffentliche Stelle oder ein Organ, eine Einrichtung oder sonstige Stelle der Union unterrichtet den Dateninhaber im Falle einer Verletzung der Sicherheit so bald wie möglich, spätestens jedoch innerhalb von 48 Stunden.

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, ***sofern in den Rechtsvorschriften der Union oder der Mitgliedstaaten nichts anderes bestimmt ist. Die öffentlichen Stellen oder die Organe, Einrichtungen und sonstigen Stellen der Union, die die Daten erhalten haben, erkennen den Beitrag des Dateninhabers auf dessen Anfrage hin öffentlich an.***

(2) ▌Der Dateninhaber ***hat Anspruch auf eine faire Vergütung*** für die Bereitstellung von Daten nach einem Verlangen gemäß Artikel 15 ***Buchstaben b***, wobei dieser Ausgleich ***mindestens*** die technischen und organisatorischen Kosten ***deckt***, die durch die Erfüllung des Verlangens entstehen, ***gegebenenfalls*** einschließlich der Kosten einer Anonymisierung und technischen Anpassung, zuzüglich einer angemessenen Marge. Auf Anfrage der öffentlichen Stellen oder der Organe, der Einrichtungen oder der sonstigen Stellen der Union, die die Daten verlangt haben, übermittelt der Dateninhaber Informationen über die Grundlage für die Berechnung der Kosten und der angemessenen Marge.

(2a) Möchte die öffentliche Stelle oder das Organ, die Einrichtung oder sonstige Stelle der Union die Höhe der vom Dateninhaber geforderten Vergütung anfechten, so ist der in Artikel 31 genannte Datenkoordinator des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, über die Angelegenheit in Kenntnis zu setzen.

Artikel 21

Beitrag von Forschungsorganisationen oder statistischen Ämtern im Zusammenhang mit außergewöhnlichen Notwendigkeiten

(1) Öffentliche Stellen sowie Organe, Einrichtungen und sonstige Stellen der Union sind berechtigt, die nach diesem Kapitel erhaltenen Daten an Personen oder Organisationen zur Durchführung wissenschaftlicher Forschungstätigkeiten oder Analysen, die ***zur Erfüllung des*** Zwecks, für den die Daten verlangt wurden, ***erforderlich*** sind, oder an nationale statistische Ämter, ***an die Mitglieder des Europäischen Systems der Zentralbanken*** und an Eurostat zur Erstellung amtlicher Statistiken weiterzugeben.

(2) Personen oder Organisationen, die Daten nach Absatz 1 erhalten, dürfen ***ausschließlich*** gemeinnützig oder im Rahmen einer im Unionsrecht oder im Recht der Mitgliedstaaten anerkannten Aufgabe von öffentlichem Interesse tätig sein. Dies umfasst keine Organisationen, die ***in erheblichem Maße*** dem 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 öffentliche Stellen oder Organe, Einrichtungen oder sonstige Stellen der Union ***beabsichtigen,*** Daten nach Absatz 1 ***zu übermitteln oder bereitzustellen,*** teilen sie dies dem Dateninhaber, von dem sie die Daten erhalten hat, mit. ***Die Mitteilung muss die Identität und die Kontaktdaten der Einzelpersonen oder Organisationen, die die Daten erhalten, den Zweck der Übermittlung oder Zurverfügungstellung der Daten und den Zeitraum, für den die empfangende Stelle die Daten verwendet, enthalten. Innerhalb von fünf Tagen nach Erhalt der in Unterabsatz 1 genannten Mitteilung ist der Dateninhaber berechtigt, einen begründeten Einwand gegen diese Übermittlung oder Zurverfügungstellung von Daten vorzulegen. Wird der Einwand von der öffentlichen Stelle, dem Organ, der Einrichtung oder der sonstigen Stelle der Union zurückgewiesen, kann der Dateninhaber den begründeten Einwand dem in Artikel 31 genannten Datenkoordinator vorlegen.***

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 dem in Artikel 31 genannten ***Datenkoordinator*** des betreffenden Mitgliedstaats mit. Dies gilt auch für Zugangsverlangen von Organen, Einrichtungen und sonstigen Stellen der Union. ***Das Verlangen wird von der zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, ordnungsgemäß geprüft.***

(4) Nach Eingang der Mitteilung nach Absatz 3 berät der ***Datenkoordinator*** 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 des ***Datenkoordinators*** Rechnung.

KAPITEL VI

WECHSEL ZWISCHEN DATENVERARBEITUNGSDIENSTEN

Artikel 22a

Begriffsbestimmungen

Für die Zwecke dieses Kapitels bezeichnet der Ausdruck

(1) „Datenverarbeitungsdienst“ eine digitale Dienstleistung, die einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsamen Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen ermöglicht, die einem Kunden zur Verfügung gestellt werden und mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters schnell bereitgestellt und freigegeben werden können;

(2) „in eigenen Räumlichkeiten“ IKT-Infrastruktur und Rechenressourcen, die vom Kunden geleast wird bzw. werden oder seinem Eigentum steht bzw. stehen und die sich in seinem eigenen Rechenzentrum befindet bzw. befinden und von ihm oder einem Dritten betrieben wird bzw. werden;

(3) „gleichwertiger Dienst“ eine Reihe von Datenverarbeitungsdiensten, die dasselbe Hauptziel haben und dasselbe Dienstmodell für die Datenverarbeitung aufweisen;

(4) „Datenübertragbarkeit von Datenverarbeitungsdiensten“ die Fähigkeit des Cloud-Dienstes, seine exportierbaren Daten zwischen den Datenverarbeitungsdiensten des Kunden zu verschieben und anzupassen, auch in unterschiedlichen Einsatzmodellen;

(5) „Wechsel“ den Vorgang, bei dem ein Kunde eines Datenverarbeitungsdienstes von der Nutzung eines Datenverarbeitungsdienstes zu einem zweiten gleichwertigen oder anderen Dienst übergeht, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, auch durch Extraktion, Umwandlung und Hochladen der Daten, wobei der vorherige Anbieter von Datenverarbeitungsdiensten, der Kunde und der übernehmende Anbieter der Datenverarbeitungsdienste einbezogen werden;

(6) „exportierbare Daten“ die Eingabe- und Ausgabedaten einschließlich Metadaten, die unmittelbar und mittelbar durch die Nutzung des Datenverarbeitungsdienstes durch den Kunden erzeugt oder gemeinsam erzeugt werden, mit Ausnahme der Vermögenswerte oder Daten eines Anbieters von Datenverarbeitungsdiensten oder Dritter, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis oder vertrauliche Informationen darstellen;

(7) „Funktionsäquivalenz“ die Möglichkeit, auf der Grundlage der Kundendaten ein Mindestmaß an Funktionalität in der Umgebung eines neuen Datenverarbeitungsdienstes nach dem Wechsel wiederherzustellen, wenn der übernehmende Dienst als Reaktion auf dieselbe Eingabe für gemeinsame Funktionen, die dem Kunden im Rahmen der vertraglichen Vereinbarung geliefert werden, ein vergleichbares Ergebnis erbringt;

(8) „Extraktionsgebühren“ Datenübertragungsgebühren, die Kunden eines Anbieters von Datenverarbeitungsdiensten für die Extraktion ihrer Daten über das Netz aus

der IKT-Infrastruktur eines Anbieters von Datenverarbeitungsdiensten in Rechnung gestellt werden.

Artikel 23

Beseitigung von Hindernissen für einen wirksamen Wechsel zwischen Anbietern von Datenverarbeitungsdiensten

(1) Anbieter von Datenverarbeitungsdiensten treffen ***im Rahmen ihrer Möglichkeiten*** die in den Artikeln 24, ***24a, 24b,*** 25 und 26 vorgesehenen Maßnahmen, ***die es*** Kunden ***ermöglichen,*** zu einem anderen Datenverarbeitungsdienst ***zu*** wechseln, der einen ***gleichwertigen*** Dienst abdeckt und von einem anderen ***Anbieter von Datenverarbeitungsdiensten erbracht wird, oder unter Umständen mehrere Anbieter von Datenverarbeitungsdiensten gleichzeitig in Anspruch zu nehmen.*** Insbesondere ***dürfen*** Anbieter ***eines*** Datenverarbeitungsdiensts ***keine*** gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse ***errichten*** und müssen derlei Hindernisse gegebenenfalls beseitigen, durch die Kunden daran gehindert werden,

a) den Vertrag über den Dienst nach einer Kündigungsfrist von höchstens ***60*** Kalendertagen zu kündigen, ***es sei denn, zwischen dem Kunden und dem Anbieter wird ausdrücklich eine alternative Kündigungsfrist vereinbart, sofern beide Parteien gleichermaßen Einfluss auf den Inhalt der vertraglichen Vereinbarung haben;***

b) neue Verträge mit einem anderen Anbieter von Datenverarbeitungsdiensten für einen ***gleichwertigen*** Dienst ▌ zu schließen;

c) die ***exportierbaren*** Daten, Anwendungen und anderen digitalen Vermögenswerte ***des Kunden*** zu einem anderen Anbieter von Datenverarbeitungsdiensten ***oder zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu übertragen, auch nach Inanspruchnahme eines kostenlosen Angebots;***

d) die Funktionsäquivalenz ***bei der Nutzung*** des ***neuen*** Dienstes in der IT-Umgebung des bzw. der anderen Anbieter von Datenverarbeitungsdiensten, die einen ***gleichwertigen*** Dienst ▌ abdecken, gemäß Artikel 26 ***zu erreichen***.

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

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 ***oder, falls vorhanden, zu einer IKT-Infrastruktur in eigenen Räumlichkeiten*** werden in einem schriftlichen Vertrag eindeutig festgelegt***, der dem Kunden vor Vertragsunterzeichnung in benutzerfreundlicher Weise zur Verfügung gestellt wird***. Unbeschadet der Richtlinie () 2019/770 ***stellt der Anbieter von Datenverarbeitungsdiensten sicher, dass die vertragliche Vereinbarung*** mindestens Folgendes enthält:

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 ***exportierbaren*** Daten ▌, Anwendungen und digitalen Vermögenswerte ***unverzüglich und in keinem Fall zu einem späteren Zeitpunkt als nach Ablauf einer*** verbindlichen Übergangsfrist von höchstens ***90*** Kalendertagen ***auf eine IKT-Infrastruktur in eigenen Räumlichkeiten*** zu übertragen, einer Frist, in der der ***Anbieter von Datenverarbeitungsdiensten***

i) den Wechselvorgang ***angemessen begleitet und erleichtert***;

ii) ***gebührende Sorgfalt walten lässt, um den Geschäftsbetrieb und ein hohes Maß an Sicherheit des Dienstes aufrechtzuerhalten und unter Berücksichtigung der beim Wechsel erzielten Fortschritte im größtmöglichen Umfang*** Kontinuität bei der Erbringung der ***relevanten*** Funktionen oder Dienste ***innerhalb der Infrastrukturkapazität des vorherigen Anbieters von Datenverarbeitungsdiensten und gemäß den vertraglichen Verpflichtungen*** sicherzustellen;

iia) klare Informationen bezüglich bekannter Risiken für die Kontinuität bei der Erbringung der jeweiligen Funktionen oder Dienste seitens des vorherigen Anbieters von Datenverarbeitungsdiensten bereitstellt;

aa) eine Liste der zusätzlichen Dienste, die die Kunden zur Erleichterung des Wechsels in Anspruch nehmen können, z. B. einen Test des Wechsels;

ab) die Verpflichtung des Anbieters von Datenverarbeitungsdiensten, die Ausarbeitung der für die vertraglich vereinbarten Dienste relevanten Ausstiegsstrategie des Kunden zu unterstützen, unter anderem durch die Bereitstellung aller relevanten Informationen;

b) ***eine ausführliche*** Spezifikation aller Kategorien von Daten und Anwendungen, ***die während des Wechsels portierbar sind,*** einschließlich mindestens aller ***exportierbaren Daten***;

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

ca) die Verpflichtung des Anbieters von Datenverarbeitungsdiensten, alle exportierbaren Daten des früheren Kunden nach Ablauf des in Absatz 1 Buchstabe c genannten Zeitraums zu löschen;

(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 ***14*** Arbeitstagen nach der Veranlassung des Anbieterwechsels mit, ***wobei er*** die technische Undurchführbarkeit ***ordnungsgemäß begründet und*** einen alternativen Übergangszeitraum ***angibt***, der ***neun*** 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. ***Der Kunde behält das Recht, diesen Zeitraum bei Bedarf vor oder während des Wechsels zu verlängern.***

Artikel 24a

Informationspflicht der übernehmenden Anbieter von Datenverarbeitungsdiensten

Der übernehmende Anbieter von Datenverarbeitungsdiensten stellt dem Kunden Informationen über die verfügbaren Verfahren für den Wechsel und die Übertragung auf den Datenverarbeitungsdienst zur Verfügung, wenn er das Ziel der Übertragung ist, einschließlich Informationen über verfügbare Übertragungsmethoden und -formate sowie über Einschränkungen und technische Beschränkungen, die dem übernehmenden Anbieter von Datenverarbeitungsdiensten bekannt sind.

Artikel 24b

Verpflichtung zum Handeln nach Treu und Glauben

Alle Beteiligten, einschließlich der übernehmenden Anbieter von Datenverarbeitungsdiensten, arbeiten nach Treu und Glauben zusammen, um den Wechsel effizient zu gestalten, die rechtzeitige Übermittlung der erforderlichen Daten zu ermöglichen und die Kontinuität des Dienstes aufrechtzuerhalten.

Artikel 25

Schrittweise Abschaffung der Wechselentgelte

(1) Ab dem [***Datum des Inkrafttretens dieser Verordnung***] verlangen die Anbieter von Datenverarbeitungsdiensten von den ***Kunden, die Verbraucher sind,*** für den Wechsel keine Entgelte mehr.

(2) Vom [Datum X, Tag des Inkrafttretens ***dieser Verordnung***] bis zum [Datum X+3 Jahre] dürfen die Anbieter von Datenverarbeitungsdiensten ***von den Kunden im Rahmen von Geschäftsbeziehungen zwischen Unternehmen*** für den Wechsel ermäßigte Entgelte verlangen***, insbesondere Extraktionsgebühren***.

(2a) Ab dem [3 Jahre nach Inkrafttreten dieser Verordnung] dürfen die Anbieter von Datenverarbeitungsdiensten für den Wechsel keine Entgelte mehr 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 ***und müssen mit den zwingend durchzuführenden Vorgängen verknüpft sein, die der Anbieter der Datenverarbeitungsdienste im Rahmen des Wechsels durchführen muss.***

(3a) Standardabonnement- oder -dienstleistungsentgelte sowie Entgelte für professionelle Übergangsdienste, die der Anbieter von Datenverarbeitungsdiensten auf Verlangen des Kunden zur Unterstützung des Wechsels erbringt, gelten nicht als Wechselentgelte im Sinne dieses Artikels.

(3b) Vor dem Abschluss einer vertraglichen Vereinbarung mit einem Kunden stellt der Anbieter von Datenverarbeitungsdiensten dem Kunden eindeutige Informationen zur Verfügung, in denen die gemäß Absatz 2 vom Kunden für den Wechsel zu zahlenden Entgelte sowie die in Absatz 3a beschriebenen Gebühren und Entgelte dargelegt werden, und er stellt Informationen über die etwaigen Dienste, die mit einem hoch komplexen oder kostspieligen Wechsel verbunden sind, oder über Fälle bereit, in denen ein Wechsel ohne eine erhebliche Beeinträchtigung der Daten, Anwendung oder Struktur des Dienstes nicht möglich ist. Der Anbieter von Datenverarbeitungsdiensten macht diese Informationen den Kunden gegebenenfalls über einen speziellen Abschnitt seiner Website oder auf andere leicht zugängliche Weise öffentlich zugänglich.

(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 ***den Absätzen 1 und 2*** vorgesehene Abschaffung ***und Verringerung*** der Wechselentgelte innerhalb der jeweiligen in ***diesen Absätzen*** 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, ***treffen in ihrer Macht stehende angemessene Maßnahmen,*** um es zu erleichtern, 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 ***erreicht, sofern die Funktionsäquivalenz vom übernehmenden Anbieter von Datenverarbeitungsdiensten festgestellt wird***. ***Der vorherige Anbieter von Datenverarbeitungsdiensten erleichtert den Ablauf, indem er Kapazitäten, angemessene Information, Dokumentation, technische Unterstützung und gegebenenfalls die notwendigen Instrumente bereitstellt.***

(2) ***Die Anbieter von*** Datenverarbeitungsdiensten ▌, ***einschließlich*** der Anbieter der ***übernehmenden*** Datenverarbeitungsdienste***,*** stellen ***zur Erleichterung des Wechsels zwischen diesen Diensten und der Datenübertragbarkeit und Interoperabilität*** offene Schnittstellen öffentlich und kostenlos bereit. ***Gemäß Absatz 1 dieses Artikels ermöglichen diese Dienste es auch, dass ein bestimmter Dienst, bei dem es keine nennenswerten Hindernisse gibt, aus dem Vertrag entflochten und auf interoperable Weise für einen Wechsel verfügbar gemacht werden kann.***

(3) ▌Die Anbieter von Datenverarbeitungsdiensten gewährleisten die Kompatibilität mit offenen ***Interoperabilitäts- und Übertragbarkeitsspezifikationen*** oder europäischen Interoperabilitätsnormen, die gemäß Artikel 29 Absatz 5 ▌benannt werden.

(3a) Die Anbieter von Datenverarbeitungsdiensten, für die eine neue offene Interoperabilitäts- und Übertragbarkeitsspezifikation oder europäische Norm in dem in Artikel 29 Absatz 5 genannten Zentralspeicher veröffentlicht wurde, haben das Recht auf einen einjährigen Übergang zur Einhaltung der in Absatz 3 dieses Artikels genannten Pflicht.

(4) Bestehen für den betreffenden ***gleichwertigen*** Dienst ▌keine offenen ***Interoperabilitäts- und Übertragbarkeitsspezifikationen*** oder europäischen Normen nach Absatz 3 ***dieses Artikels***, so exportiert der Anbieter von Datenverarbeitungsdiensten auf Verlangen des Kunden, ***sofern es technisch machbar ist,*** alle ***exportierbaren Daten in einem strukturierten, gängigen und maschinenlesbaren Format, wie dem Kunden gemäß der in Artikel 24 Absatz 1 Buchstabe ab genannten Ausstiegsstrategie mitgeteilt wird, es sei denn, vom Kunden wird ein anderes Format akzeptiert***.

(4a) Anbieter von Datenverarbeitungsdiensten sind nicht verpflichtet, neue Technologien oder Dienste zu entwickeln, geschützte oder vertrauliche Daten oder Technologien gegenüber einem Kunden oder einem anderen Anbieter von Datenverarbeitungsdiensten offenzulegen oder die Sicherheit und Integrität des Dienstes eines Kunden oder Anbieters zu beeinträchtigen.

Artikel 26a

Befreiungen für bestimmte Datenverarbeitungsdienste

(1) Die Pflichten gemäß Artikel 23 Absatz 1 Buchstabe d und den Artikeln 25 und 26 gelten nicht für Datenverarbeitungsdienste, die nach Kundenwünschen eingerichtet wurden.

(2) Die in diesem Kapitel festgelegten Pflichten gelten nicht für Datenverarbeitungsdienste, die kostenlos bereitgestellt werden, versuchsweise in Betrieb sind oder nur einen Test- und Evaluierungsdienst für Produktangebote des Unternehmens bieten.

Artikel 26b

Streitbeilegung

(1) Die Kunden haben Zugang zu gemäß Artikel 10 Absatz 2 zertifizierten Streitbeilegungsstellen, um Streitigkeiten im Zusammenhang mit Verletzungen der Rechte der Kunden und der Pflichten der Anbieter von Datenverarbeitungsdiensten bezüglich des Wechsels zwischen Anbietern solcher Dienste beizulegen. Der Kunde hat das Recht, Dritten die Verfolgung seiner Rechtsansprüche in seinem Namen zu ermöglichen.

(2) Artikel 10 Absätze 3 bis 9 gelten für die Beilegung von Streitigkeiten zwischen Kunden und Anbietern von Datenverarbeitungsdiensten bezüglich des Wechsels zwischen Anbietern solcher Dienste.

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 ▌technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen, um eine internationale Übermittlung oder einen staatlichen Zugriff ***von Drittländern*** auf ***solche*** in der Union gespeicherten nicht personenbezogenen Daten zu verhindern, ***wenn damit gegen*** das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats ***verstoßen würde***.

(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 nach einer Überprüfung durch die einschlägigen zuständigen Stellen oder Behörden gemäß dieser Verordnung betreffend die Beurteilung, ob zusätzlich zu den einschlägigen nationalen Rechtsvorschriften oder des Unionsrechts die folgenden Bedingungen erfüllt sind:***

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 Kommission, des Datenkoordinators*** gemäß dieser Verordnung ***oder einschlägiger zuständiger Stellen oder Behörden*** einholen, um festzustellen, ob diese Bedingungen erfüllt sind, insbesondere wenn er der Auffassung ist, dass sich die Entscheidung ***Geschäftsgeheimnisse und andere*** sensible Geschäftsdaten ***sowie Inhalte, die durch***

Rechte des geistigen Eigentums geschützt sind, betreffen oder die nationalen Sicherheits- oder Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten beeinträchtigen könnte. ***Hat der Adressat binnen eines Monats keine Antwort erhalten oder kommen die zuständigen Behörden in ihrer Stellungnahme zu dem Schluss, dass die Voraussetzungen nicht erfüllt sind, so lehnt der Adressat die Aufforderung zur Übermittlung oder Bereitstellung von Daten aus diesen Gründen ab.***

Der durch die Verordnung ***() 2022/868*** eingesetzte Europäische Dateninnovationsrat, ***auf den in Artikel 31a der vorliegenden Verordnung Bezug genommen wird,*** 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 auf der Grundlage einer angemessenen Auslegung des Verlangens ***durch die einschlägig zuständige Stelle oder Behörde*** die zulässige Mindestmenge der darin verlangten Daten bereit.

(4a) Hat der Anbieter von Datenverarbeitungsdiensten Grund zu der Annahme, dass die Übermittlung nicht personenbezogener Daten oder der Zugang zu solchen Daten dazu führen könnte, dass nicht personenbezogene oder anonymisierte Daten erneut identifiziert werden, holt er bei den jeweils nach den anwendbaren Datenschutzbestimmungen zuständigen Stellen oder Behörden eine Genehmigung ein, bevor die Daten übermittelt werden bzw. Zugang dazu gewährt wird.

(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 ***von Datenräumen***

(1) ***Teilnehmer*** von Datenräumen***, die anderen Teilnehmern Daten oder Datendienste anbieten,*** 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 ***in maschinenlesbarem Format*** 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***, sofern dies technisch machbar ist und das reibungslose Funktionieren des Produkts nicht beeinträchtigt***;

d) es werden die Mittel bereitgestellt, mit denen die Interoperabilität ***von Verträgen über die gemeinsame Datennutzung*** 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, ***nach Anhörung des Europäischen Dateninnovationsrats gemäß Artikel 29 und Artikel 30 Buchstaben f und h der Verordnung (EU) 2022/868 und*** gemäß Artikel 38 ***der vorliegenden Verordnung*** delegierte Rechtsakte zur Ergänzung dieser Verordnung durch eine nähere Bestimmung der in Absatz 1 ***dieses Artikels*** genannten wesentlichen Anforderungen zu erlassen.

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

(3a) Die Teilnehmer in einem bestimmten Datenraum einigen sich auf die Regeln, nach denen die Verantwortlichkeiten hinsichtlich dieser Anforderungen zwischen den Teilnehmern festgelegt werden.

(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 ***und im Einklang mit Kapitel II der Verordnung (EU) Nr. 1025/2012 in einer offenen, transparenten, technologieneutralen, industriegesteuerten und inklusiven Weise entwickelt werden, wobei gegebenenfalls bestehende internationale Standards, bewährte Verfahren, Normen, technische Spezifikationen und einschlägige Normen für Quelloffenheit sowie die Bedürfnisse von KMU zu berücksichtigen sind***.

(5) Die Kommission ***kann*** nötigenfalls im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen ***erlassen***, 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. ***Vor dem Erlass dieser Durchführungsrechtsakte holt die Kommission gemäß Artikel 30 Buchstabe f der Verordnung (EU) 2022/868 den Rat des Europäischen Dateninnovationsrats ein und berücksichtigt seine einschlägigen Standpunkte, und*** sie erlässt diese Durchführungsrechtsakte gemäß dem Prüfverfahren nach Artikel 39 Absatz 2.

(6) Die Kommission kann ***vom Europäischen Dateninnovationsrat gemäß Artikel 30 Buchstabe h der Verordnung (EU) 868/2022 vorgeschlagene*** 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 ***und Übertragbarkeit*** von Datenverarbeitungsdiensten

(1) Offene Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** und europäische Normen für die Interoperabilität ***und Übertragbarkeit*** von Datenverarbeitungsdiensten

a) müssen***, soweit dies technisch machbar ist,*** leistungsbezogen darauf ausgerichtet sein, die Interoperabilität ***und Übertragbarkeit*** zwischen verschiedenen Datenverarbeitungsdiensten, die ***gleichwertige Dienste*** abdecken, herzustellen;

b) müssen die Übertragbarkeit digitaler Vermögenswerte zwischen verschiedenen Datenverarbeitungsdiensten, die ***gleichwertige Dienste*** abdecken, verbessern;

c) müssen, soweit dies technisch machbar ist, die Funktionsäquivalenz zwischen ***in Artikel 26 Absatz 1 genannten*** Datenverarbeitungsdiensten, die ***gleichwertige Dienste*** abdecken, ***erleichtern***;

ca) dürfen die Sicherheit und Integrität der Dienste und Daten nicht beeinträchtigen;

cb) müssen auf eine Art und Weise gestaltet sein, die technische Fortschritte und die Einbindung neuer Funktionen und Innovationen in Datenverarbeitungsdienste ermöglicht.

(2) Offene Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** und europäische Normen für die Interoperabilität ***und Übertragbarkeit*** 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 Interoperabilitäts- ***und Übertragbarkeitsspezifikationen*** müssen mit Anhang II Nummern 3 und 4 der Verordnung (EU) Nr. 1025/2012 übereinstimmen.

(3a) Offene Interoperabilitäts- und Übertragbarkeitsspezifikationen und europäische Normen dürfen nicht den Markt für Datenverarbeitungsdienste verzerren oder die Entwicklung jeglicher neuen konkurrierenden und innovativen Technologien oder Lösungen oder jeglicher auf ihnen beruhenden Technologien oder Lösungen einschränken.

(4) ***Nach Berücksichtigung einschlägiger internationaler und europäischer Normen und Selbstregulierungsinitiativen*** kann die Kommission gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen, Entwürfe für europäische Normen für ***gleichwertige*** Datenverarbeitungsdienste auszuarbeiten. ***Bei der Normung ist den Bedürfnissen von KMU Rechnung zu tragen.***

(5) Für die Zwecke des Artikels 26 Absatz 3 dieser Verordnung wird der Kommission die Befugnis übertragen, ***nach Anhörung des Europäischen Dateninnovationsrats gemäß Artikel 29 und Artikel 30 Buchstaben f und h der Verordnung (EU) 2022/868 und*** gemäß Artikel 38 der vorliegenden Verordnung delegierte Rechtsakte ***zur Ergänzung der vorliegenden Verordnung*** zu erlassen, um die Fundstellen offener ▌Normen für die Interoperabilität ***und Übertragbarkeit*** von Datenverarbeitungsdiensten im ***von einschlägigen Normungsorganisationen oder in***

Anhang II Absatz 3 der Verordnung (EU) Nr. 1025/2012 genannten Organisationen entwickelten Zentralspeicher der Union für Normen für die Interoperabilität ***und Übertragbarkeit*** 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

Die Partei, die intelligente Verträge ▌ im Zusammenhang mit einer Datenbereitstellungsvereinbarung ***anbietet***, muss die folgenden wesentlichen Anforderungen erfüllen:

a) Robustheit ***und Zugriffskontrolle***: Gewährleistung, dass der intelligente Vertrag so konzipiert wurde, dass er ***strenge Zugriffskontrollmechanismen und*** 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; ***in diesem Zusammenhang sollten die Bedingungen, unter denen ein intelligenter Vertrag zurückgesetzt oder angewiesen werden kann, den Betrieb zu beenden oder zu unterbrechen, klar und transparent festgelegt werden. Es sollte insbesondere bewertet werden, unter welchen Bedingungen eine nicht einvernehmliche Beendigung oder Unterbrechung zulässig sein sollte;***

ba) Gleichwertigkeit: Ein intelligenter Vertrag muss das gleiche Maß an Schutz und Rechtssicherheit bieten wie andere Verträge, die mit anderen Mitteln zustande gekommen sind;

bb) Schutz der Vertraulichkeit von Geschäftsgeheimnissen: Gewährleistung, dass ein intelligenter Vertrag so konzipiert ist, dass die Vertraulichkeit von Geschäftsgeheimnissen im Einklang mit dieser Verordnung sichergestellt ist.

▌

KAPITEL IX

ANWENDUNG UND DURCHSETZUNG

Artikel 31

Datenkoordinator

(1) Jeder Mitgliedstaat benennt eine ***unabhängige zuständige Koordinierungsbehörde („Datenkoordinator"),*** die für die Anwendung und Durchsetzung dieser Verordnung verantwortlich ***ist, die diesem Mitgliedstaat übertragenen Tätigkeiten koordiniert, im Hinblick auf die Durchführung dieser Verordnung als zentrale Kontaktstelle gegenüber der Kommission fungiert und den Mitgliedstaat in dem in Artikel 31a genannten Europäischen Dateninnovationsrat vertritt***.

(1a) 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. Der Europäische Datenschutzbeauftragte ist für die Überwachung der Anwendung dieser Verordnung zuständig, insofern Organe, Einrichtungen und sonstige Stellen der Union davon betroffen sind. Artikel 62 der Verordnung (EU) 2018/1725 gilt gegebenenfalls sinngemäß. Die Aufgaben und Befugnisse der Aufsichtsbehörden werden im Hinblick auf die Verarbeitung personenbezogener Daten wahrgenommen.

(2) Unbeschadet des Absatzes 1 dieses Artikels ***sorgt der Datenkoordinator für die Zusammenarbeit der zuständigen nationalen Behörden, die für die Überwachung anderer Rechtsakte der Union oder nationaler Rechtsakte im Bereich Daten und elektronische Kommunikationsdienste zuständig sind, wobei Folgendes gilt***:

▌

b) Bei besonderen sektoralen Problemen des ***Datenzugangs*** im Zusammenhang mit der Anwendung dieser Verordnung bleibt die Zuständigkeit der

Fachbehörden ***unbeschadet der Bestimmungen über Zuständigkeitskonflikte*** 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 ***des Datenkoordinators*** 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 ***und Entscheidung über*** Beschwerden über mutmaßliche Verstöße gegen diese Verordnung, angemessene Untersuchung des Beschwerdegegenstands und ***regelmäßige*** 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 ***wirksamer, verhältnismäßiger und*** abschreckender finanzieller Sanktionen, die auch Zwangsgelder und Geldstrafen mit Rückwirkung umfassen können, ▌oder Einleitung von Gerichtsverfahren zur Verhängung von Geldbußen;

e) Beobachtung ***der Entwicklungen in Technologie und Wirtschaft***, die für die Bereitstellung und Nutzung von Daten von Bedeutung sind***, zum Zweck der besseren Durchsetzung dieser Verordnung***;

f) Zusammenarbeit mit den ***Datenkoordinatoren*** anderer Mitgliedstaaten, um die einheitliche***, rasche und wirksame*** Anwendung dieser Verordnung sicherzustellen, einschließlich des unverzüglichen Austauschs aller relevanten Informationen auf elektronischem Wege;

fa) Zusammenarbeit mit allen nach anderen Rechtsvorschriften der Union einschlägigen zuständigen Behörden sowie mit dem Europäischen

Datenschutzausschuss und dem Europäischen Dateninnovationsrat, um sicherzustellen, dass die Pflichten aus dieser Verordnung im Einklang mit anderen Rechtsvorschriften der Union durchgesetzt werden;

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 ***Datenkoordinatoren*** bei der Wahrnehmung der ihnen nach Absatz 3 übertragenen Aufgaben und Befugnisse untereinander sowie ***mit dem Europäischen Dateninnovationsrat und*** gegebenenfalls auch mit der für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörde ***und dem Europäischen Datenschutzbeauftragten*** zusammen, um für die einheitliche Anwendung der vorliegenden Verordnung zu sorgen. In solchen Fällen benennen die betreffenden Mitgliedstaaten eine koordinierende zuständige Behörde.

(5) Die Mitgliedstaaten teilen der Kommission ***und dem Dateninnovationsrat*** die Namen der ***Datenkoordinatoren*** 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 ***handeln die Datenkoordinatoren unabhängig und unparteiisch***, unterliegen 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 ***der Datenkoordinator in ausreichendem Umfang*** mit ***personellen und technischen*** Mitteln***, Fachkenntnissen, Räumlichkeiten und Infrastruktur*** ausgestattet wird, damit er seine Aufgaben gemäß dieser Verordnung angemessen und effizient wahrnehmen kann.

(7a) Rechtsträger, die in den Anwendungsbereich dieser Verordnung fallen, unterliegen der Gerichtsbarkeit des Mitgliedstaats, in dem der Rechtsträger niedergelassen ist.

(7b) Ein Nutzer, Dateninhaber oder Datenempfänger, bei dem es sich um eine juristische Person handelt und der nicht in der Union niedergelassen ist, aber den Verpflichtungen aus dieser Verordnung unterliegt, benennt in einem der Mitgliedstaaten, in denen seine jeweiligen Gegenparteien niedergelassen sind, einen gesetzlichen Vertreter.

(7c) Die nach dieser Verordnung zuständigen Behörden sind befugt, von Nutzern, Dateninhabern oder Datenempfängern, bei denen es sich um juristische Personen handelt, oder von ihren gesetzlichen Vertretern alle Informationen anzufordern, die nötig sind, um die Einhaltung der Anforderungen aus dieser Verordnung zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(7d) Benennt ein Nutzer, Dateninhaber oder Datenempfänger, bei dem es sich um eine juristische Person handelt und der nicht in der Union niedergelassen ist, keinen gesetzlichen Vertreter oder stellt der gesetzliche Vertreter auf Ersuchen der zuständigen Behörde nicht die erforderlichen Informationen zur Verfügung, die die Einhaltung dieser Verordnung umfassend belegen, so ist die zuständige Behörde befugt, den Beginn der Erbringung verbundener Dienste durch Dateninhaber aufzuschieben oder die Erbringung solcher Dienste oder Anträge von Nutzern oder Datenempfängern, bei denen es sich um juristische Personen handelt, auf Zugang zu Daten des Dateninhabers auszusetzen, bis der gesetzliche Vertreter benannt ist oder die erforderlichen Informationen bereitgestellt werden.

Artikel 31a

Amtshilfe

(1) Im Hinblick auf eine einheitliche und effiziente Anwendung dieser Verordnung arbeiten die Datenkoordinatoren und die Kommission eng zusammen und leisten einander gegenseitige Amtshilfe. Die gegenseitige Amtshilfe umfasst insbesondere den Austausch aller Informationen gemäß diesem Artikel auf elektronischem Wege und die Pflicht des Datenkoordinators des betreffenden Mitgliedstaats, alle

zuständigen Behörden und die Kommission über die Einleitung einer Untersuchung zu informieren.

(2) Für die Zwecke einer Untersuchung kann der Datenkoordinator am Niederlassungsort andere Datenkoordinatoren ersuchen, bestimmte in ihrem Besitz befindliche Informationen zu übermitteln oder ihre Untersuchungsbefugnisse in Bezug auf bestimmte in ihrem Mitgliedstaat befindliche Informationen auszuüben. Gegebenenfalls kann der Datenkoordinator, der ein solches Verlangen erhält, andere zuständige Behörden oder andere Behörden des betreffenden Mitgliedstaats mit einbeziehen.

(3) Der Datenkoordinator, der das Verlangen gemäß Absatz 2 erhält, kommt diesem Verlangen nach und unterrichtet die zuständige Behörde des betreffenden Mitgliedstaats unverzüglich über die getroffenen Maßnahmen.

(4) Der Europäische Dateninnovationsrat fördert den gegenseitigen Informationsaustausch zwischen den zuständigen Behörden und berät und unterstützt die Kommission in allen Angelegenheiten, die unter diese Verordnung und gemäß Artikel 30 der Verordnung (EU) 2022/868 in den Zuständigkeitsbereich des Innovationsrates fallen. Die Datenkoordinatoren vertreten die Mitgliedstaaten in dem mit der Verordnung (EU) 2022/868 eingerichteten Europäischen Dateninnovationsrat.

Artikel 32

Recht auf Beschwerde bei ***einem Datenkoordinator***

(1) Unbeschadet eines anderen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs haben natürliche und juristische Personen das Recht, einzeln oder ▌ gemeinsam bei ***dem Datenkoordinator*** 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. ***Eine solche Beschwerde kann sich aus der Aussetzung der Weitergabe von als Geschäftsgeheimnis eingestuften Daten ergeben, nachdem die entsprechende Mitteilung des Dateninhabers gemäß Artikel 4 Absatz 3, Artikel 5 Absatz 8 oder Artikel 19 Absatz 2b eingegangen ist.***

(2) ***Der Datenkoordinator***, bei dem die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer ***im Einklang mit dem nationalen Recht*** über den Stand des Verfahrens und die getroffene Entscheidung.

(3) Die zuständigen Behörden arbeiten ***von Anfang an*** zusammen, um Beschwerden ***wirksam und rechtzeitig*** zu bearbeiten und zu lösen, und ***setzen*** dazu unter anderem ***angemessene Fristen für den Erlass förmlicher Entscheidungen, stellen die Gleichbehandlung der Parteien, den Anspruch von Beschwerdeführern auf rechtliches Gehör und das Recht auf Akteneinsicht während des gesamten Verfahrens sicher und*** tauschen 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 32a

Vertretung

(1) Unbeschadet der Richtlinie (EU) 2020/1828 oder jeder anderen Art von Vertretung nach nationalem Recht haben die Nutzer, die Dateninhaber und die Datenempfänger zumindest das Recht, eine Einrichtung, Organisation oder Vereinigung mit der Wahrnehmung der mit dieser Verordnung übertragenen Rechte in ihrem Namen zu beauftragen, sofern die Einrichtung, Organisation oder Vereinigung alle folgenden Bedingungen erfüllt:

a) Sie verfolgt keine Gewinnerzielungsabsicht;

b) sie wurde nach dem Recht eines Mitgliedstaats ordnungsgemäß gegründet;

c) aus ihren satzungsmäßigen Zielen ergibt sich ein berechtigtes Interesse daran, die Einhaltung dieser Verordnung sicherzustellen.

Artikel 32b

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine zuständige Behörde

(1) Jeder Nutzer, Dateninhaber und Datenempfänger hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen ihn betreffenden rechtsverbindlichen Beschluss einer zuständigen Behörde.

(2) Jeder Nutzer hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen Rechtsbehelf, wenn die zuständige Behörde die Beschwerde nicht zügig bearbeitet oder den Nutzer, Dateninhaber und Datenempfänger nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 32 eingereichten Beschwerde unterrichtet.

(3) Für Verfahren gegen eine zuständige Behörde sind die Gerichte des Mitgliedstaats zuständig, in dem der Nutzer oder die ihn vertretende Organisation seinen bzw. ihren gewöhnlichen Aufenthalt oder Arbeitsplatz oder seine bzw. ihre Niederlassung hat.

(4) Kommt es zu einem Verfahren gegen den Beschluss einer zuständigen Behörde, dem eine Stellungnahme oder ein Beschluss des Innovationsrates im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.

Artikel 32c

Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Der Nutzer, Dateninhaber oder Datenempfänger hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs – darunter im Rahmen der Richtlinie (EU) 2020/1828 und einschließlich des Rechts

auf Beschwerde bei einer zuständigen Behörde gemäß Artikel 32b – das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn er der Ansicht ist, dass die ihm aufgrund dieser Verordnung zustehenden Rechte infolge der Nichteinhaltung dieser Verordnung verletzt wurden.

(2) Für Klagen gegen einen Dateninhaber, einen Dritten oder einen Datenempfänger sind die Gerichte des Mitgliedstaats zuständig, in dem der Nutzer seinen gewöhnlichen Aufenthalt, seinen Arbeitsort oder seine Niederlassung hat.

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.

(1a) Die Mitgliedstaaten berücksichtigen die folgenden nicht erschöpfenden Kriterien für die Verhängung von Sanktionen aufgrund von Verstößen gegen diese Verordnung:

a) Art, Schwere, Umfang und Dauer des Verstoßes;

b) Maßnahmen, die die verstoßende Partei ergriffen hat, um den durch den Verstoß verursachten Schaden zu mindern oder zu beheben;

c) frühere Verstöße der verstoßenden Partei;

d) die finanziellen Vorteile, die die verstoßende Partei durch den Verstoß erzielt, oder die Verluste, die sie durch ihn vermieden hat, sofern diese Vorteile oder Verluste zuverlässig festgestellt werden können;

e) sonstige erschwerende oder mildernde Umstände im jeweiligen Fall.

(2) Die Mitgliedstaaten teilen der Kommission, ***dem Europäischen Datenschutzausschuss und dem Europäischen Dateninnovationsrat*** diese Vorschriften und Maßnahmen bis zum [Datum des Geltungsbeginns der Verordnung] mit und melden ***ihnen*** unverzüglich etwaige spätere Änderungen. ***Die Kommission führt ein leicht zugängliches öffentliches Register dieser Maßnahmen und aktualisiert es regelmäßig.***

(3) Bei Verstößen gegen die Pflichten gemäß den Kapiteln 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 gemäß Kapitel 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 ***sowie Standardvertragsklauseln für Cloud-Computing-Verträge, die auf den Grundsätzen der Fairness, Angemessenheit und Diskriminierungsfreiheit (Fair, reasonable and non-discriminatory – FRAND) beruhen***, um die Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit ausgewogenen vertraglichen Rechten und Pflichten zu unterstützen. ***Diese Mustervertragsbedingungen regeln mindestens die folgenden Elemente:***

a) das Recht auf eine vorzeitige Beendigung des Vertrags und die Bedingungen für die Entschädigung im Falle einer vorzeitigen Beendigung;

b) Leitlinien betreffend die Speicherung von Daten;

c) die Lesbarkeit der Daten für den Nutzer, einschließlich Informationen zu Metadaten und zur Entschlüsselung;

d) den Schutz und die Wahrung der Vertraulichkeit von Geschäftsgeheimnissen im Einklang mit dieser Verordnung.

Die in Unterabsatz 1 genannten Mustervertragsbedingungen werden veröffentlicht und unentgeltlich in einem einfach verwendbaren elektronischen Format zur Verfügung gestellt.

KAPITEL X

UNANWENDBARKEIT DES SUI-GENERIS-RECHTS IM RAHMEN DER RICHTLINIE ***96/9/EG AUF DATENBANKEN, DIE BESTIMMTE DATEN ENTHALTEN***

Artikel 35

Datenbanken, die bestimmte Daten enthalten

Das in Artikel 7 der Richtlinie 96/9/EG festgelegte spezifische Schutzrecht sui generis findet keine Anwendung auf Datenbanken, die Daten enthalten, die bei der Nutzung eines ***in den Anwendungsbereich dieser Verordnung fallenden*** 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 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

(1) 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) die Nutzung von Daten durch Nutzer, Dateninhaber, Datenempfänger und Dritte, die Entwicklung der Monetarisierungspraktiken in der europäischen Datenwirtschaft sowie die Entwicklung der Modalitäten des Datenaustauschs, einschließlich der Wettbewerbsdynamik in Datenräumen und Datenvermittlungsdiensten,

-aa) die Auswirkungen der zur Einhaltung dieser Verordnung und insbesondere von Kapitel II erforderlichen technischen und administrativen Pflichten auf

Teilnehmer aus der Industrie, auch mit Blick auf die Ausnahmeregelungen für KMU,

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

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

ba) ob die Bestimmungen dieser Verordnung, die sich auf Geschäftsgeheimnisse beziehen, die Wahrung von Geschäftsgeheimnissen sicherstellen, ohne den Zugang zu Daten und deren gemeinsame Nutzung zu behindern, und insbesondere ob und wie die Vertraulichkeit von Geschäftsgeheimnissen in der Praxis trotz ihrer Offenlegung im Zusammenhang mit der gemeinsamen Nutzung von Daten mit Dritten und der Weitergabe durch Unternehmen an Behörden sichergestellt wird. Diese Bewertung wird in enger Verbindung mit dem Bewertungsbericht gemäß Artikel 18 Absatz 3 der Richtlinie (EU) 2016/943, der bis zum 9. Juni 2026 erwartet wird, durchgeführt,

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,

ea) die Wechselwirkung zwischen dieser Verordnung und anderen einschlägigen Rechtsvorschriften der Union, um etwaige widersprüchliche Regelungen, Überregulierung oder Gesetzeslücken zu ermitteln,

eb) der Beitrag dieser Verordnung zur Sicherstellung der wirtschaftlichen Attraktivität des Erhebens und der Nutzung hochwertiger Datensätze durch Unternehmen der Union,

ec) der Beitrag dieser Verordnung zu Innovation und zur Förderung der Entwicklung von Hightech-Start-ups und Hightech-KMU sowie zur

Ermöglichung des Zugangs europäischer Nutzer zu modernsten Computing-Diensten,

ed) die Anwendung und das Funktionieren von Artikel 27 betreffend den internationalen Zugang zu Daten und deren internationale Übermittlung.

(1a) Die Kommission legt dem Europäischen Parlament und dem Rat auf der Grundlage dieses Berichts gegebenenfalls einen Rechtsetzungsvorschlag zur Änderung dieser Verordnung vor.

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 [***18*** Monate nach dem Datum des Inkrafttretens dieser Verordnung].

Die Verpflichtungen gemäß Artikel 4 Absatz 1 gelten für verbundene Dienste, die in den letzten fünf Jahren vor Inkrafttreten dieser Verordnung in Verkehr gebracht wurden, jedoch nur, wenn der Anbieter eines verbundenen Diensts in der Lage ist, Mechanismen, mit denen die Erfüllung der Anforderungen gemäß Artikel 4 Absatz 1 sichergestellt werden kann, aus der Ferne einzusetzen und wenn der Einsatz solcher Mechanismen den Hersteller oder Anbieter der verbundenen Dienste nicht unverhältnismäßig belasten würde.

Geschehen zu …

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