

# Data Act

*Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)*

Mit den Erwägungsgründen – die Zuordnung zu einzelnen Artikeln ist nicht offiziell. Eine Fassung ohne die Erwägungsgründe findet sich auf <https://datenrecht.ch/gesetzestexte/data-act/>.

Die Texte wurden automatisiert konvertiert – wir danken für Hinweise auf Fehler an [hello@datenrecht.ch](mailto:hello@datenrecht.ch).

Kapitel I Allgemeine Bestimmungen

Kapitel II Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Kapitel III Pflichten der Dateninhaber, die gemäss dem Unionsrecht verpflichtet sind, Daten bereitzustellen

Kapitel IV Missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen

Kapitel V Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen aussergewöhnlicher Notwendigkeit

Kapitel VI Wechsel zwischen Datenverarbeitungsdiensten

Kapitel VII Unrechtmässiger staatlicher Zugang zu und unrechtmässige staatliche Übermittlung von nicht-personenbezogenen Daten im internationalen Umfeld

Kapitel VIII Interoperabilität

Kapitel IX Anwendung und Durchsetzung

Kapitel X Schutzrecht Sui Generis nach der Richtlinie 96/9/EG

Kapitel XI Schlussbestimmungen

# Kapitel I Allgemeine Bestimmungen

(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. Dieselben Daten können unbegrenzt für verschiedene Zwecke verwendet und weiterverwendet werden, ohne dass dadurch Qualität oder Quantität beeinträchtigt wird.

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

(3) In Sektoren mit zahlreichen Kleinstunternehmen sowie Kleinunternehmen und mittleren Unternehmen im Sinne von Artikel 2 des Anhangs der Empfehlung 2003/361/ der Kommission (5) (KMU) mangelt es häufig an digitalen Kapazitäten und Kompetenzen für die Erhebung, Analyse und Nutzung von Daten; zudem ist der Zugang oftmals eingeschränkt, weil ein einziger Akteur im System die Daten hält oder weil Daten oder Datendienste an sich bzw. über Grenzen hinweg nicht interoperabel sind.

(4) Um den Bedürfnissen der digitalen Wirtschaft gerecht zu werden und die Hindernisse für einen reibungslos 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, Produktdaten oder verbundene Dienstdaten zu nutzen. Daher sollten die Mitgliedstaaten in den Angelegenheiten, die in den Anwendungsbereich der vorliegenden Verordnung fallen, keine zusätzlichen nationalen Anforderungen annehmen oder aufrechterhalten, sofern das in der vorliegenden Verordnung nicht ausdrücklich vorgesehen ist, da dies ihre direkte und einheitliche Anwendung beeinträchtigen würde. Ferner sollten auf Unionsebene ergriffene Maßnahmen die Verpflichtungen und Zusagen, die sich aus den von der Union geschlossenen internationalen Handelsabkommen ergeben, unberührt lassen.

(5) Mit dieser Verordnung wird sichergestellt, dass die Nutzer eines vernetzten Produkts oder verbundenen Dienstes in der Union zeitnah auf die Daten zugreifen können, die bei der Nutzung dieses vernetzten Produkts oder verbundenen Dienstes generiert werden, und dass diese Nutzer die Daten verwenden und auch an Dritte ihrer Wahl weitergeben können. Sie verpflichtet Dateninhaber, die Daten unter bestimmten Umständen den Nutzern und Dritten ihrer Wahl bereitzustellen. Ferner wird sichergestellt, dass Dateninhaber den Datenempfängern in der Union Daten zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und auf transparente Weise bereitstellen. Privatrechtliche Vorschriften sind im Gesamtrahmen für die Datenweitergabe 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 und der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union die Daten bereitstellen, die im Falle außergewöhnlicher Notwendigkeit zur Wahrnehmung einer spezifischen Aufgabe im öffentlichen Interesse erforderlich

sind. Darüber hinaus soll mit dieser Verordnung der Wechsel zwischen Datenverarbeitungsdiensten erleichtert und die Interoperabilität von Daten sowie von Mechanismen und Diensten für die Datenweitergabe in der Union verbessert werden. Diese Verordnung sollte nicht so ausgelegt werden, dass sie Dateninhabern ein neues Recht auf die Nutzung von Daten verleiht, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden.

(6) Die Datengenerierung ist das Ergebnis der Handlungen mindestens zweier Akteure, insbesondere des Entwicklers oder Herstellers eines vernetzten Produkts, bei dem es sich in vielen Fällen auch um einen Erbringer verbundener Dienste handeln kann, und des Nutzers des vernetzten Produkts oder des verbundenen Dienstes. Es stellen sich Fragen der Fairness in der digitalen Wirtschaft, da die von solchen vernetzten Produkten oder verbundenen Diensten erfassten Daten ein wichtiges Gut für Folgemarkt-Dienste, Nebendienste und sonstige Dienste sind. Um die wichtigen wirtschaftlichen Vorteile von Daten zu nutzen sowie um Unternehmen in der Union für die Weitergabe von Daten auf der Grundlage freiwilliger Vereinbarungen und für die Entwicklung einer datengetriebenen Wertschöpfung zu gewinnen, ist ein allgemeiner Ansatz für die Zuweisung von Rechten für den Datenzugang und die Datennutzung der Gewährung ausschließlicher Zugangs- und Nutzungsrechte vorzuziehen. In dieser Verordnung sind horizontale Regelungen vorgesehen, denen das Unionsrecht oder das nationale Recht folgen könnten, das die besonderen Gegebenheiten der betreffenden Sektoren Rechnung zu angeht.

(119) Da die Ziele dieser Verordnung, nämlich die Gewährleistung einer fairen Aufteilung des Wertes von Daten auf die Akteure der Datenwirtschaft und Förderung eines fairen Zugangs zu Daten und ihrer Nutzung, um zur Schaffung eines echten Binnenmarktes für Daten beizutragen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs und der Wirkungen der Maßnahme und der grenzüberschreitenden Nutzung der Daten auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

## **Artikel 1 Gegenstand und Anwendungsbereich**

(1) Diese Verordnung enthält harmonisierte Vorschriften unter anderem über

- a)* die Bereitstellung von Produktdaten und verbundenen Dienstdaten für den Nutzer des vernetzten Produkts oder verbundenen Dienstes,
- b)* die Bereitstellung von Daten durch Dateninhaber für Datenempfänger,
- c)* die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer spezifischen Aufgabe von öffentlichem Interesse besteht,
- d)* die Erleichterung des Wechsels zwischen Datenverarbeitungsdiensten,
- e)* die Einführung von Schutzmaßnahmen gegen den unrechtmäßigen Zugang Dritter zu nicht-personenbezogenen Daten und
- f)* die Entwicklung von Interoperabilitätsnormen für Daten, die abgerufen, übertragen und genutzt werden sollen.

- (2) Die vorliegende Verordnung erstreckt sich auf personenbezogene und nicht-personenbezogene Daten, einschließlich der folgenden Arten von Daten, in den folgenden Zusammenhängen:
- a) Kapitel II gilt für Daten, mit Ausnahme von Inhalten, die die Leistung, Nutzung und Umgebung von vernetzten Produkten und verbundenen Diensten betreffen;
  - b) Kapitel III gilt für alle Daten des Privatsektors, die rechtlichen Verpflichtungen mit Blick auf die Datenweitergabe unterliegen;
  - c) Kapitel IV gilt für alle Daten des Privatsektors, die auf der Grundlage von Verträgen zwischen Unternehmen abgerufen und genutzt werden;
  - d) Kapitel V gilt für alle Daten des Privatsektors mit Schwerpunkt auf nicht-personenbezogenen Daten;
  - e) Kapitel VI gilt für alle von Anbietern von Datenverarbeitungsdiensten verarbeiteten Daten und Dienste;
  - f) Kapitel VII gilt für alle nicht-personenbezogenen Daten, die in der Union von Anbietern von Datenverarbeitungsdiensten gehalten werden.
- (3) Diese Verordnung gilt für
- a) Hersteller vernetzter Produkte, die in der Union in Verkehr gebracht werden, und Anbieter verbundener Dienste, unabhängig vom Ort der Niederlassung dieser Hersteller oder Anbieter;
  - b) die Nutzer der unter Buchstabe a genannten vernetzten Produkte oder verbundenen Dienste in der Union;
  - c) Dateninhaber, unabhängig vom Ort ihrer Niederlassung, die Datenempfängern in der Union Daten bereitstellen;
  - d) Datenempfänger in der Union, denen Daten bereitgestellt werden;
  - e) öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union, die von Dateninhabern verlangen, Daten bereitzustellen, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer speziellen Aufgabe im öffentlichen Interesse besteht, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;
  - f) Anbieter von Datenverarbeitungsdiensten, unabhängig vom Ort ihrer Niederlassung, die Kunden in der Union solche Dienste anbieten;
  - g) Teilnehmer an Datenräumen und Anbieter von Anwendungen, die intelligente Verträge verwenden, und Personen, deren gewerbliche, geschäftliche oder berufliche Tätigkeit die Einführung intelligenter Verträge für andere im Zusammenhang mit der Durchführung einer Vereinbarung umfasst.
- (4) Wird in dieser Verordnung auf vernetzte Produkte oder verbundene Dienste Bezug genommen, so gilt, dass diese Bezugnahmen auch virtuelle Assistenten einschließen, soweit diese mit einem vernetzten Produkt oder verbundenen Dienst interagieren.
- (5) Diese Verordnung gilt unbeschadet des Unionsrechts und des nationalen Rechts über den Schutz personenbezogener Daten, die Privatsphäre, die Vertraulichkeit der Kommunikation und die Integrität von Endgeräten, die für personenbezogene Daten gelten, die im Zusammenhang mit den in der vorliegenden Verordnung festgelegten Rechten

und Pflichten verarbeitet werden, insbesondere der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie 2002/58/, einschließlich der Befugnisse und Zuständigkeiten der Aufsichtsbehörden und der Rechte der betroffenen Personen. Soweit Nutzer betroffene Personen sind, ergänzen die in Kapitel II dieser Verordnung festgelegten Rechte das Auskunftsrecht von betroffenen Personen und das Recht auf Datenübertragbarkeit gemäß Artikel 15 bzw. Artikel 20 der Verordnung (EU) 2016/679. Im Falle eines Widerspruchs zwischen der vorliegenden Verordnung und dem Unionsrecht in Bezug auf den Schutz personenbezogener Daten bzw. der Privatsphäre oder den im Einklang mit dem Unionsrecht erlassenen nationalen Rechtsvorschriften haben das Unionsrecht oder das nationale Recht zum Schutz personenbezogener Daten bzw. der Privatsphäre Vorrang.

(7) Das Grundrecht auf den Schutz personenbezogener Daten wird insbesondere durch die Verordnungen (EU) 2016/679 (6) und (EU) 2018/1725 (7) des Europäischen Parlaments und des Rates gewahrt. Die Richtlinie 2002/58/ des Europäischen Parlaments und des Rates (8) schützt darüber hinaus die Privatsphäre und die Vertraulichkeit der Kommunikation, unter anderem mittels Bedingungen für die Speicherung personenbezogener und nicht-personenbezogener Daten auf Endgeräten und den Zugang dazu. Diese Gesetzgebungsakte der Union 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 Schutz personenbezogener Daten und zum Schutz der Privatsphäre, insbesondere die Verordnungen (EU) 2016/679 und (EU) 2018/1725 und die Richtlinie 2002/58/, und lässt es unberührt. Keine Bestimmung dieser Verordnung sollte dahingehend angewandt oder ausgelegt werden, dass das Recht auf den Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation abgeschwächt oder eingeschränkt wird. Jegliche Verarbeitung personenbezogener Daten nach dieser Verordnung sollte dem Datenschutzrecht der Union entsprechen, einschließlich dem Erfordernis einer gültigen Rechtsgrundlage für die Verarbeitung gemäß Artikel 6 der Verordnung (EU) 2016/679 und gegebenenfalls den Bedingungen des Artikels 9 der genannten Verordnung und des Artikels 5 Absatz 3 der Richtlinie 2002/58/. Die vorliegende Verordnung stellt keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber dar. Die vorliegende Verordnung verpflichtet die Dateninhaber, Nutzern Dritten seiner Wahl oder auf Anfrage eines Nutzers personenbezogene Daten bereitzustellen. Ein solcher Zugang sollte im Falle personenbezogener Daten gewährt werden, die vom Dateninhaber auf der Grundlage einer der in Artikel 6 der Verordnung (EU) 2016/679 genannten Rechtsgrundlagen verarbeitet werden. Handelt es sich bei dem Nutzer nicht um die betroffene Person, so bietet die vorliegende Verordnung keine Rechtsgrundlage für die Gewährung des Zugangs zu personenbezogenen Daten oder für deren Bereitstellung an Dritte und sollte nicht so verstanden werden, dass sie dem Dateninhaber ein neues Recht auf die Nutzung personenbezogener Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert wurden, verleiht. In diesen Fällen könnte es im Interesse des Nutzers liegen, die Erfüllung der Anforderungen des Artikels 6 der Verordnung (EU) 2016/679 zu ermöglichen. Da die vorliegende Verordnung die Datenschutzrechte der betroffenen Personen nicht beeinträchtigen sollte, kann der Dateninhaber Datenzugangsverlangen in diesen Fällen unter anderem nachkommen, indem er personenbezogene Daten anonymisiert oder, wenn ohne Weiteres verfügbare Daten personenbezogene Daten mehrerer betroffener Personen enthalten, nur personenbezogene Daten des Nutzers übermittelt.

- (6) Die vorliegende Verordnung gilt weder für freiwillige Vereinbarungen über den Datenaustausch zwischen privaten und öffentlichen Stellen – insbesondere freiwillige

Vereinbarungen über die Datenweitergabe -, noch greift sie ihnen vor. Die vorliegende Verordnung berührt nicht die Rechtsakte der Union und die nationalen Rechtsakte 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 insbesondere die Verordnungen (EU) 2021/784, (EU) 2022/2065 und (EU) 2023/1543 und die Richtlinie (EU) 2023/1544 oder die internationale Zusammenarbeit in diesem Bereich. Die vorliegende Verordnung gilt nicht für die Datenerhebung, die Datenweitergabe, die Datennutzung oder den Datenzugang gemäß der Verordnung (EU) 2015/847 und der Richtlinie (EU) 2015/849. Die vorliegende Verordnung gilt nicht in den nicht unter das Unionsrecht fallenden Bereichen und berührt keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, unabhängig von der Art der Einrichtung, die von den Mitgliedstaaten mit der Wahrnehmung von Aufgaben im Zusammenhang mit diesen Zuständigkeiten betraut wurde, oder ihre Befugnis, andere wesentliche staatliche Funktionen zu wahren, einschließlich der Gewährleistung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung. Die vorliegende Verordnung berührt nicht die Zuständigkeiten der Mitgliedstaaten in Bezug auf die Zoll- und Steuerverwaltung oder die Gesundheit und Sicherheit der Bürger.

(10) Diese Verordnung berührt nicht Rechtsvorschriften der Union nationale Rechtsvorschriften über die Datenweitergabe, den Datenzugang und die Datennutzung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder zur Verfolgung von Straftaten oder der Strafvollstreckung oder für Zoll- und Steuerzwecke, unabhängig davon, auf welcher Rechtsgrundlage nach dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) diese Rechtsvorschriften der Union erlassen wurden, oder Rechtsvorschriften über die internationale Zusammenarbeit in diesem Bereich, insbesondere auf der Grundlage des Übereinkommens des Europarats über Computerkriminalität (ETS Nr. 185), das am 23. November 2001 in Budapest unterzeichnet wurde. Zu diesen Rechtsvorschriften gehören die Verordnungen (EU) 2021/784 (12), (EU) 2022/2065 (13) und (EU) 2023/1543 (14) des Europäischen Parlaments und des Rates und die Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates (15). Die vorliegende Verordnung gilt nicht für die Erhebung oder das Teilen von oder den Zugang zu oder die Nutzung von Daten gemäß der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates (16) sowie der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates (17). Die vorliegende Verordnung gilt nicht für nicht unter das Unionsrecht fallende Bereiche und berührt nicht die Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, die Zoll- und Steuerverwaltung oder die Gesundheit und Sicherheit der Bürgerinnen und Bürger, unabhängig von der Art des Rechtsträgers, der von den Mitgliedstaaten mit der Wahrnehmung von Aufgaben im Zusammenhang mit diesen Zuständigkeiten betraut wurde.

- (7) Mit der vorliegenden Verordnung wird der Selbstregulierungsansatz der Verordnung (EU) 2018/1807 ergänzt, indem allgemein geltende Verpflichtungen in Bezug auf den Cloud-Wechsel hinzugefügt werden.
- (8) Diese Verordnung berührt nicht die Rechtsakte der Union und die nationalen Rechtsakte zur Gewährleistung des Schutzes der Rechte des geistigen Eigentums, insbesondere die Richtlinien 2001/29/, 2004/48/ und (EU) 2019/790.

(13) Diese Verordnung berührt nicht die Rechtsakte der Union und der Mitgliedstaaten zum Schutz der Rechte des geistigen Eigentums, darunter die Richtlinien 2001/29/

(19), 2004/48/ (20) und (EU) 2019/790 (21) des Europäischen Parlaments und des Rates.

- (9) Die vorliegende Verordnung ergänzt, und berührt nicht, das Unionsrecht, mit dem die Interessen der Verbraucher gefördert und ein hohes Verbraucherschutzniveau sichergestellt sowie die Gesundheit, Sicherheit und wirtschaftlichen Interessen der Verbraucher geschützt werden, insbesondere die Richtlinien 93/13/EWG, 2005/29/ und 2011/83/EU.

(11) Sofern nicht ausdrücklich in der vorliegenden Verordnung vorgesehen, sollten 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, von dieser Verordnung unberührt bleiben.

(28) Bei Verträgen zwischen einem Dateninhaber und einem Verbraucher als Nutzer eines vernetzten Produkts oder verbundenen Dienstes, das bzw. der Daten generiert, gilt das Verbraucherrecht der Union, insbesondere die Richtlinien 93/13/EWG und 2005/29/, damit ein Verbraucher keinen missbräuchlichen Vertragsklauseln unterliegt. Für die Zwecke dieser Verordnung sollten missbräuchliche Vertragsklauseln, die einem Unternehmen einseitig auferlegt werden, für das betreffende Unternehmen nicht verbindlich sein.

- (10) Diese Verordnung steht dem Abschluss freiwilliger rechtmäßiger Verträge über die Datenweitergabe – einschließlich auf der Grundlage der Gegenseitigkeit geschlossener Verträge -, die den Anforderungen dieser Verordnung entsprechen, nicht entgegen.

(9) Sofern in der vorliegenden Verordnung nicht anders vorgesehen, lässt sie das nationale Vertragsrecht, einschließlich der Vorschriften über das Zustandekommen von Verträgen, ihre Gültigkeit oder ihre Rechtsfolgen oder über die Auswirkungen der Beendigung eines Vertrags, unberührt. Die vorliegende Verordnung ergänzt das Unionsrecht zur Förderung der Interessen der Verbraucher und zur Gewährleistung eines hohen Verbraucherschutzniveaus sowie zum Schutz ihrer Gesundheit, Sicherheit und wirtschaftlichen Interessen, insbesondere die Richtlinie 93/13/EWG des Rates (9) und der Richtlinien 2005/29/ (10) und 2011/83/EU (11) des Europäischen Parlaments und des Rates, und lässt es unberührt.

(115) Diese Verordnung sollte Vorschriften unberührt lassen, die besonderen Bedürfnissen einzelner Sektoren oder Bereichen von öffentlichem Interesse Rechnung tragen. Solche Vorschriften können zusätzliche Anforderungen an die technischen Aspekte des Datenzugangs, wie Schnittstellen für den Datenzugang, oder an 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 oder Sicherheitsanforderungen, einschließlich Anforderungen an die Cybersicherheit. Diese Verordnung sollte auch spezifischere Vorschriften im Zusammenhang mit der Entwicklung gemeinsamer europäischer Datenräume oder – vorbehaltlich der in dieser Verordnung festgelegten Ausnahmen – Unionsrecht oder nationales Recht zur Zugänglichmachung von Daten und zur Genehmigung ihrer Nutzung für die Zwecke der wissenschaftlichen Forschung unberührt lassen.

(116) Diese Verordnung sollte die Anwendung der Wettbewerbsvorschriften, insbesondere der Artikel 101 und 102 AEUV unberührt lassen. Die in dieser Verordnung vorgesehenen Vorschriften dürfen nicht dazu verwendet werden, den Wettbewerb entgegen den Vorschriften des AEUV einzuschränken.

## Artikel 2 Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. **“Daten”** jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material;
2. **“Metadaten”** eine strukturierte Beschreibung der Inhalte oder der Nutzung von Daten, die das Auffinden eben jener Daten bzw. deren Verwendung erleichtert;
3. **“personenbezogene Daten”** personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;
4. **“nicht-personenbezogene Daten“** Daten, die keine personenbezogenen Daten sind;
5. **“vernetztes Produkt”** einen Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist;

(14) Vernetzte Produkte, die mittels ihrer Komponenten oder Betriebssysteme Daten über ihre Leistung, Nutzung oder Umgebung erlangen, generieren oder erheben und die diese Daten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln können – häufig als Internet der Dinge bezeichnet –, sollten in den Anwendungsbereich dieser Verordnung fallen, mit Ausnahme von Prototypen. Beispiele für solche elektronischen Kommunikationsdienste umfassen insbesondere terrestrische Telefonnetze, Fernseekabelnetze, Satellitennetze und Nahfeldkommunikationsnetze. Vernetzte Produkte kommen in allen Bereichen der Wirtschaft und Gesellschaft vor, einschließlich in privaten, zivilen oder gewerblichen Infrastrukturen, Fahrzeugen, medizinischer Ausrüstung, Lifestyle-Ausrüstung, Schiffen, Luftfahrzeugen, Haushaltsgeräten und Konsumgütern, Medizin- und Gesundheitsprodukten oder landwirtschaftlichen und industriellen Maschinen und Anlagen. Durch die Entscheidungen der Hersteller bei der Konzeption und gegebenenfalls durch das Unionsrecht oder das nationale Recht, mit dem sektorspezifischer Bedürfnisse und Ziele angegangen werden, oder durch die einschlägigen Entscheidungen der Wettbewerbsbehörden sollte vorgegeben werden, welche Daten von einem vernetzten Produkt bereitgestellt werden können.

(22) Die vernetzten 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, zugänglich gemacht werden. Der Zugang zu Datenspeichern auf dem Gerät kann über kabelgebundene oder drahtlose lokale Funknetze ermöglicht werden, die mit einem öffentlich verfügbaren elektronischen Kommunikationsdienst oder Mobilfunknetz verbunden sind. Bei dem Server kann es sich um die eigenen lokalen Serverkapazitäten des Herstellers oder um die eines Dritten oder eines Cloud-Diensteanbieters handeln. Auftragsverarbeiter im Sinne von Artikel 4 Nummer 8 der Verordnung (EU) 2016/679 gelten nicht als Dateninhaber. Sie können jedoch ausdrücklich vom Verantwortlichen im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 beauftragt werden, Daten bereitzustellen. Vernetzte Produkte können so konzipiert sein, dass der Nutzer oder ein Dritter die Daten auf dem vernetzten Produkt, auf einer Rechnerinstanz des Herstellers oder in einer von dem Nutzer oder Dritten ausgewählten Informations- und Kommunikationstechnologie-(IKT)-Umgebung verarbeiten kann.

(23) Virtuelle Assistenten spielen eine immer wichtigere Rolle bei der Digitalisierung des Verbraucherumfelds und des beruflichen Umfelds und dienen als benutzerfreundliche Schnittstelle für die Wiedergabe von Inhalten, das Erlangen von Informationen oder die Aktivierung von Produkten, 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. Unter Umständen möchte der Nutzer diese Daten Drittherstellern bereitstellen, um neuartige intelligente Dienste zu aktivieren. Virtuelle Assistenten sollten unter das in dieser Verordnung vorgesehene Datenzugangsrecht fallen. Unter das in dieser Verordnung vorgesehene Datenzugangsrecht sollten auch Daten fallen, die generiert werden, wenn ein Nutzer über einen virtuellen Assistenten, der von einem anderen Rechtsträger als dem Hersteller des vernetzten Produkts bereitgestellt wird, mit einem vernetzten Produkt interagiert. Allerdings sollten nur die aus der Interaktion zwischen dem Nutzer und einem vernetzten Produkt oder verbundenen Dienst über den virtuellen Assistenten anfallenden Daten von dieser Verordnung gedeckt sein. Vom virtuellen Assistenten erstellte Daten, die nicht mit der Verwendung eines vernetzten Produkts oder verbundenen Dienstes zusammenhängen, sind nicht von dieser Verordnung gedeckt.

(16) Diese Verordnung ermöglicht es Nutzern vernetzter Produkte, Folgemarkt-Dienste, Nebendienste und sonstige Dienste zu nutzen, die auf Daten basieren, die von in diese Produkte eingebetteten Sensoren erhoben werden, wobei die Erhebung dieser Daten von potenziellem Nutzen für die Verbesserung der Leistung der vernetzten Produkte ist. Es ist wichtig, einerseits die Märkte für die Bereitstellung solcher mit Sensoren ausgestatteter vernetzter Produkte und damit verbundener Dienste und andererseits die Märkte für nicht verwandte Software und Inhalte wie Text-, Audio- oder audiovisuelle Inhalte, die häufig Rechten des geistigen Eigentums unterliegen, voneinander abzugrenzen. Daher sollten Daten, die von solchen mit Sensoren ausgestatteten vernetzten Produkten generiert werden, wenn ihre Nutzer Inhalte – unter anderem zur Nutzung durch einen Online-Dienst – aufzeichnen, übermitteln, anzeigen lassen oder abspielen, sowie die Inhalte selbst, die häufig Rechten des geistigen Eigentums unterliegen, nicht unter diese Verordnung fallen. Diese Verordnung sollte auch nicht für Daten gelten, die von dem vernetzten Produkt für die Zwecke der Speicherung oder Verarbeitung im Namen anderer Parteien, die keine Nutzer sind, erlangt oder generiert wurden oder auf die über das vernetzte Produkt zugegriffen wurde oder die an es übermittelt wurden, wie es etwa bei Servern oder Cloud-Infrastrukturen, die von ihren Eigentümern ausschließlich im Auftrag Dritter betrieben werden, unter anderem zur Nutzung durch einen Online-Dienst, der Fall sein kann.

6. “**verbundener Dienst**” einen digitalen Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt, – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen;

(17) Für Produkte, die zum Zeitpunkt des Erwerbs, der Anmietung oder des Leasings so mit einem verbundenen Dienst vernetzt sind, dass das vernetzte Produkt ohne diesen Dienst eine oder mehrere seiner Funktionen nicht ausführen könnte, oder der anschließend vom Hersteller oder von einem Dritten mit dem Produkt vernetzt wird, um die Funktionen des vernetzten Produkts zu ergänzen oder anzupassen, müssen

Vorschriften festgelegt werden. Im Rahmen solcher verbundenen Dienste werden Daten zwischen dem vernetzten Produkt und dem Diensteanbieter ausgetauscht, das heißt, sie sollten als Dienste verstanden werden, die ausdrücklich mit dem Betrieb der Funktionen des vernetzten Produkts verknüpft sind, wie im Fall von Diensten, die gegebenenfalls Befehle an das vernetzte Produkt übermitteln, die sich wiederum auf dessen Aktivität oder Verhalten auswirken können. Dienste, die sich nicht auf den Betrieb des vernetzten Produkts auswirken und durch die keine Daten oder Befehle des Diensteanbieters an das vernetzte Produkt übermittelt werden, sollten nicht als verbundene Dienste gelten. Zu solchen Diensten könnten z. B. zusätzliche Beratungs-, Analyse- oder Finanzdienstleistungen oder regelmäßige Reparatur- und Wartungsdienste gehören. Verbundene Dienste können als Teil eines Kauf-, Miet- oder Leasingvertrags angeboten werden. Verbundene Dienste könnten auch für Produkte derselben Art erbracht werden, und Nutzer sollten ihre Erbringung – unter Berücksichtigung der Beschaffenheit des vernetzten Produkts und öffentlicher Erklärungen, die im Vorfeld des Vertragsschlusses von dem Verkäufer oder im Auftrag des Verkäufers, Vermieters, Leasinggebers oder anderer Personen in vorgelagerten Gliedern der Vertragskette, einschließlich des Herstellers, abgegeben wurden – vernünftigerweise erwarten können. Diese verbundenen Dienste können, unabhängig von den Datenerhebungsmöglichkeiten des vernetzten Produkts, mit dem sie verbunden sind, selbst Daten generieren, die für den Nutzer von Wert sind. Diese Verordnung sollte auch für verbundene Dienste gelten, die nicht vom Verkäufer, Vermieter oder Leasinggeber selbst, sondern von einem Dritten erbracht werden. Bei Zweifeln, 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.

7. **“Verarbeitung”** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Daten oder Datensätzen, wie etwa das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, der Abruf, das Abfragen, die Nutzung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
8. **“Datenverarbeitungsdienst”** eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können;

(80) Datenverarbeitungsdienste sollten Dienste umfassen, die den ortsunabhängigen und bedarfsgesteuerten Netzzugang zu einem konfigurierbaren, skalierbaren und elastischen gemeinsam genutzten Pool verteilter Ressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie etwa Netze, Server oder sonstige virtuelle oder physische Infrastrukturen, Software – einschließlich Tools zur Entwicklung von Software -, Speicher, Anwendungen und Dienste. Dass sich Kunden von Datenverarbeitungsdiensten selbst, ohne Interaktion mit dem Anbieter von Datenverarbeitungsdiensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen können, könnte als minimaler Verwaltungsaufwand und minimale Interaktion zwischen Anbieter und Kunde beschrieben werden. Der Begriff “ortsunabhängig” wird verwendet, um zu beschreiben, dass die Bereitstellung der Rechenkapazitäten über das Netz und der Zugang zu ihnen über Mechanismen erfolgt, 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 zugewiesen werden, um Nachfrageschwankungen auszugleichen. Der Begriff "elastisch" dient zur Beschreibung der Rechenressourcen, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, um je nach Arbeitsaufkommen zügig verfügbare Ressourcen auf- bzw. abbauen zu können. Der Begriff "gemeinsam genutzter Pool" dient zur Beschreibung der Rechenressourcen, die mehreren Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei die Verarbeitung jedoch für jeden Nutzer getrennt erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Der Begriff "verteilt" dient zur Beschreibung der Rechenressourcen, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und sich koordinieren. Der Begriff "hochgradig verteilt" dient zur Beschreibung der Datenverarbeitungsdienste, bei denen Daten näher an dem Ort verarbeitet werden, an dem sie generiert oder erhoben 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.

(81) Der generische Begriff "Datenverarbeitungsdienste" umfasst eine beträchtliche Zahl von Diensten mit einer sehr großen Bandbreite an unterschiedlichen Anwendungszwecken, Funktionen und technischen Strukturen. Nach allgemeinem Verständnis von Anbietern und Nutzern und im Einklang mit weit verbreiteten Standards fallen Datenverarbeitungsdienste unter eines oder mehrere der folgenden drei Modelle für die Bereitstellung von Datenverarbeitungsdiensten, nämlich "Infrastructure-as-a-Service" (IaaS), "Platform-as-a-Service" (PaaS) und "Software-as-a-Service" (SaaS). Bei diesen Modellen für die Bereitstellung von Diensten handelt es sich um eine spezifische, vorgefertigte Kombination von IKT-Ressourcen, die von einem Anbieter von Datenverarbeitungsdiensten angeboten wird. Diese drei grundlegenden Bereitstellungsmodelle für Datenverarbeitungsdienste werden weiter durch neue Variationen ergänzt, die jeweils eine ganz bestimmte Kombination von IKT-Ressourcen aufweisen, wie z. B. "Storage-as-a-Service" und "Database-as-a-Service". Datenverarbeitungsdienste können detaillierter kategorisiert und in eine nicht erschöpfende Liste von Datenverarbeitungsdiensten unterteilt werden, die dasselbe Hauptziel und dieselben Hauptfunktionen sowie dieselbe Art von Datenverarbeitungsmodellen haben, die nicht mit den operativen Merkmalen des Dienstes (gleiche Dienstart) in Zusammenhang stehen. Dienste, die der gleichen Dienstart angehören, können zwar dasselbe Modell für die Bereitstellung von Datenverarbeitungsdiensten aufweisen, doch während zwei Datenbanken dem Anschein nach dasselbe Hauptziel haben können, könnten sie nach Berücksichtigung ihres Datenverarbeitungsmodells, ihres Vertriebsmodells und der Anwendungsfälle, auf die sie ausgerichtet sind, in eine detailliertere Unterkategorie vergleichbarer Dienste fallen. Dienste der gleichen Dienstart können unterschiedliche und konkurrierende Merkmale wie Leistung, Sicherheit, Robustheit und Qualität des Dienstes aufweisen.

9. "**gleiche Dienstart**" eine Reihe von Datenverarbeitungsdiensten, die dasselbe Hauptziel haben und dasselbe Dienstmodell für die Datenverarbeitung sowie dieselben Hauptfunktionen aufweisen;
10. "**Datenvermittlungsdienst**" einen Datenvermittlungsdienst im Sinne von Artikel 2 Nummer 11 der Verordnung (EU) 2022/868;
11. "**betroffene Person**" eine betroffene Person gemäß Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;

12. **“Nutzer”** eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt;

(18) Unter dem Nutzer eines vernetzten Produkts sollte eine natürliche oder juristische Person, z. B. ein Unternehmen, ein Verbraucher oder eine öffentliche Stelle, verstanden werden, die Eigentümer eines vernetzten Produkts oder – beispielsweise durch einen Miet- oder Leasingvertrag – Inhaber bestimmter befristeter Rechte auf Zugang zu Daten aus dem vernetzten Produkt oder auf deren Nutzung ist oder verbundene Dienste für das vernetzte Produkt in Anspruch nimmt. Diese Zugangsrechte sollten in keiner Weise eine Änderung der oder einen Eingriff in die Rechte betroffener Personen, die möglicherweise mit einem vernetzten Produkt oder einem verbundenen Dienst interagieren, in Bezug auf die von dem vernetzten Produkt oder während der Erbringung verbundener Dienste generierten personenbezogenen Daten bewirken. Der Nutzer trägt die Risiken und genießt die Vorteile der Nutzung des vernetzten Produkts und sollte auch Zugang zu den von ihm generierten Daten haben. Er sollte daher berechtigt sein, aus den von diesem vernetzten Produkt und allen verbundenen Diensten generierten Daten Nutzen zu ziehen. Ein Eigentümer, Mieter oder Leasingnehmer sollte ebenfalls als Nutzer gelten, auch in Fällen, in denen mehrere Rechtsträger als Nutzer gelten können. Im Falle mehrerer Nutzer kann jeder einzelne Nutzer auf unterschiedliche Weise zur Datengenerierung beitragen und ein Interesse an verschiedenen Formen der Nutzung haben; Beispiele sind das Flottenmanagement für ein Leasingunternehmen oder Mobilitätslösungen für Einzelpersonen, die einen Car-Sharing-Dienst nutzen.

(21) Gelten mehrere Personen oder Rechtsträger als Nutzer, beispielsweise im Falle gemeinschaftlichen Eigentums oder wenn ein Eigentümer, Mieter oder Leasingnehmer gemeinsame Rechte am Datenzugang oder an der Datennutzung besitzt, so sollte die Konzeption des vernetzten Produkts oder verbundenen Dienstes oder der entsprechenden Schnittstelle jedem Nutzer den Zugang zu den von diesen generierten Daten ermöglichen. Die Nutzung von vernetzten Produkten, die Daten generieren, erfordert in der Regel, dass ein Nutzerkonto eingerichtet wird. Ein solches Konto ermöglicht es dem Nutzer, durch den Dateninhaber, bei dem es sich um den Hersteller handeln kann, identifiziert zu werden. Es kann auch als Kommunikationsmittel und zur Einreichung und Bearbeitung von Datenzugangsverlangen verwendet werden. Haben mehrere Hersteller oder Erbringer verbundener Dienste gemeinsam vernetzte Produkte an denselben Nutzer verkauft, vermietet oder verleast bzw. integrierte Dienste für diesen erbracht, so sollte sich der Nutzer an jede der Parteien wenden, mit der er einen Vertrag geschlossen hat. Hersteller oder Entwickler eines vernetzten Produkts, das in der Regel von mehreren Personen verwendet wird, sollten die erforderlichen Mechanismen einrichten, die gegebenenfalls die Einrichtung getrennter Nutzerkonten für einzelne Personen oder die Nutzung desselben Nutzerkontos durch mehrere Personen ermöglichen. Kontobezogene Lösungen sollten es den Nutzern ermöglichen, ihre Konten und die damit verbundenen Daten zu löschen, und könnten für Nutzer insbesondere in Fällen, in denen das Eigentum an dem Produkt auf andere Personen übergeht oder andere Personen das vernetzte Produkt nutzen, die Möglichkeit vorsehen, den Datenzugang, die Datennutzung oder die Datenweitergabe zu beenden oder deren Einstellung zu beantragen. Der Zugang sollte dem Nutzer auf der Grundlage einfacher Antragsverfahren gewährt werden, die eine automatische Ausführung ermöglichen und keine Prüfung oder Freigabe durch den Hersteller oder Dateninhaber erfordern. Dies bedeutet, dass die Daten nur bereitgestellt werden sollten, wenn der Nutzer tatsächlich Zugang wünscht. Ist die automatische Ausführung des Datenzugangsverlangens, beispielsweise über ein Nutzerkonto oder die mit dem vernetzten Produkt oder dem verbundenen Dienst bereitgestellte mobile Anwendung, nicht möglich, so sollte der Hersteller dem Nutzer mitteilen, wie auf die Daten zugegriffen werden kann.

13. **“Dateninhaber”** eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat;
14. **“Datenempfänger”** eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt;
15. **“Produktdaten”** Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – abgerufen werden können;

(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 Parteien, die an der Datenweitergabe – einschließlich der Datenweitergabe im Anwendungsbereich dieser Verordnung – beteiligt sind, technische und organisatorische Maßnahmen zum Schutz dieser Rechte ergreifen. Zu diesen Maßnahmen gehören nicht nur Pseudonymisierung und Verschlüsselung, sondern auch der Einsatz zunehmend verfügbarer Technik, die es ermöglicht, Algorithmen direkt am Ort der Datengenerierung einzusetzen und wertvolle Erkenntnisse zu gewinnen, ohne dass die Daten zwischen den Parteien übertragen bzw. die Rohdaten oder strukturierten Daten selbst unnötig kopiert werden.

16. **“verbundene Dienstdaten”** Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nutzer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden;

(15) Die Daten stellen digitalisierte Nutzerhandlungen und -vorgänge dar und sollten dementsprechend für den Nutzer zugänglich sein. Die Vorschriften für den Zugang zu und die Nutzung von Daten von vernetzten Produkten und verbundenen Diensten im Rahmen dieser Verordnung betreffen sowohl Produktdaten als auch verbundene Dienstdaten. Produktdaten bezeichnet Daten, die durch die Nutzung eines vernetzten Produkts generiert werden und die der Hersteller so konzipiert hat, dass sie von einem Nutzer, Dateninhaber oder Dritten – gegebenenfalls einschließlich des Herstellers – aus dem vernetzten Produkt abgerufen werden können. Verbundene Dienstdaten bezeichnet Daten, die ebenfalls die Digitalisierung von Nutzerhandlungen oder -vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und während der Erbringung eines verbundenen Dienstes durch den Anbieter generiert werden. Unter Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden, sollten absichtlich aufgezeichnete Daten oder Daten verstanden werden, die indirekt durch Nutzerhandlungen generiert werden, wie z. B. Daten über die Umgebung oder Interaktionen des vernetzten Produkts. Diese Daten

sollten Daten über die Nutzung eines vernetzten Produkts einschließen, die von einer Benutzerschnittstelle oder über einen verbundenen Dienst generiert werden, und sollten sich nicht auf die Information beschränken, dass ein Produkt oder Dienst genutzt wurde, sondern alle Daten umfassen, die das vernetzte Produkt infolge einer solchen Nutzung generiert, wie z. B. automatisch von Sensoren generierte Daten und Daten, die von eingebetteten Anwendungen aufgezeichnet werden, einschließlich Anwendungen, die den Hardwarestatus und Funktionsstörungen angeben. Zu diesen Daten sollten auch Daten gehören, die von dem vernetzten Produkt oder verbundenen Dienst generiert werden, während der Nutzer inaktiv ist, etwa wenn er beschließt, ein vernetztes Produkt für einen bestimmten Zeitraum nicht zu verwenden, sondern es im Bereitschaftszustand zu belassen oder sogar auszuschalten, da sich der Status eines vernetzten Produkts oder seiner Komponenten, beispielsweise seiner Batterien, ändern kann, wenn sich das vernetzte Produkt im Bereitschaftszustand befindet oder ausgeschaltet ist. Daten, die nicht wesentlich verändert werden, d. h. Daten in Rohform, auch als Quell- oder Primärdaten bezeichnet, die sich auf Datenpunkte beziehen, die ohne jegliche weitere Form der Verarbeitung automatisch generiert werden, sowie Daten, die vor der Weiterverarbeitung und Auswertung aufbereitet wurden, um sie verständlich und nutzbar zu machen, fallen in den Anwendungsbereich dieser Verordnung. Dazu gehören Daten, die von einem einzelnen Sensor oder einer Gruppe miteinander verbundener Sensoren erhoben wurden, um die erfassten Daten für vielfältigere Anwendungsfälle verständlich zu machen, indem eine physikalische Größe oder Eigenschaft oder die Veränderung einer physikalischen Größe, wie Temperatur, Druck, Durchflussmenge, Ton, pH-Wert, Flüssigkeitsstand, Position, Beschleunigung oder Geschwindigkeit, bestimmt wird. Der Begriff "aufbereitete Daten" sollte nicht so ausgelegt werden, dass der Dateninhaber dazu verpflichtet ist, wesentliche Investitionen in die Bereinigung und Transformation der Daten vorzunehmen. Die Daten, die bereitzustellen sind, sollten die einschlägigen Metadaten, einschließlich ihres grundlegenden Kontexts und Zeitstempels, umfassen, um die Daten in Kombination mit anderen Daten, z. B. Daten, die sortiert und mit anderen, mit ihnen verbundenen Datenpunkten klassifiziert wurden oder die in ein gängiges Format umformatiert wurden, nutzbar zu machen. Derartige 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, unter anderem indem sie die Wartung und Reparatur der betreffenden vernetzten Produkte erleichtern. Dagegen sollten aus solchen Daten gefolgerte oder abgeleitete Informationen, die das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind (insbesondere mittels komplexer proprietärer Algorithmen, einschließlich solcher, die Teil proprietärer Software sind), nicht in den Anwendungsbereich dieser Verordnung fallen, und somit sollten Dateninhaber bei diesen Daten auch nicht dazu verpflichtet sein, sie einem Nutzer oder Datenempfänger bereitzustellen, es sei denn, der Nutzer und der Dateninhaber haben etwas anderes vereinbart. Zu diesen Daten könnten 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 erhoben werden und möglicherweise Rechten des geistigen Eigentums unterliegen.

17. **“ohne Weiteres verfügbare Daten”** Produktdaten und verbundene Dienstdaten, die ein Dateninhaber ohne unverhältnismäßigen Aufwand rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, wobei über eine einfache Bearbeitung hinausgegangen wird;

(20) In der Praxis sind nicht alle Daten, die durch vernetzte Produkte oder verbundene Dienste generiert werden, für ihre Nutzer leicht zugänglich, und es gibt häufig nur begrenzte Möglichkeiten in Bezug auf die Übertragbarkeit von Daten, die durch mit dem Internet vernetzte Produkte generiert werden. Die Nutzer sind daher nicht

in der Lage, die Daten zu erlangen, die erforderlich sind, um Reparatur- und andere Dienste in Anspruch zu nehmen, und Unternehmen sind nicht in der Lage, innovative, bequeme und effizientere Dienste anzubieten. In vielen Sektoren können die Hersteller, da sie die Kontrolle über die technische Konzeption der vernetzten Produkte oder verbundener Dienste haben, bestimmen, welche Daten generiert werden und wie darauf zugegriffen werden kann, obwohl sie keinen Rechtsanspruch auf diese Daten haben. Daher muss sichergestellt werden, dass vernetzte Produkte so konzipiert und hergestellt sowie damit verbundene Dienste so konzipiert und erbracht werden, dass die Produktdaten und die verbundenen Dienstdaten, einschließlich der entsprechenden Metadaten, die zur Auslegung und Nutzung dieser Daten erforderlich sind, und zwar auch, um die Daten abrufen, nutzen oder weitergeben zu können, für einen Nutzer stets leicht und sicher zugänglich sind, und dies kostenlos, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format. Produktdaten und verbundene Dienstdaten, die ein Dateninhaber rechtmäßig von dem vernetzten Produkt oder verbundenen Dienst erhält oder erhalten kann, etwa aufgrund der Konzeption des vernetzten Produkts, des Vertrags des Dateninhabers mit dem Nutzer über die Erbringung verbundener Dienste und seiner technischen Mittel für den Datenzugang ohne unverhältnismäßig hohen Aufwand, werden als "ohne Weiteres verfügbare Daten" bezeichnet. Von ohne Weiteres verfügbaren Daten ausgenommen sind Daten, die bei der Produktnutzung generiert werden, sofern das vernetzte Produkt nicht dafür ausgelegt ist, dass solche Daten außerhalb der Komponente, in der sie generiert werden, oder des vernetzten Produkts als Ganzem gespeichert oder übermittelt werden. Diese Verordnung sollte daher nicht dahingehend ausgelegt werden, dass die Verpflichtung zur Speicherung von Daten auf der zentralen Rechneinheit eines vernetzten Produkts besteht. Das Fehlen einer solchen Verpflichtung sollte den Hersteller oder Dateninhaber nicht daran hindern, solche Anpassungen auf freiwilliger Basis mit dem Nutzer zu vereinbaren. Die Konzeptionspflichten nach Maßgabe dieser Verordnung lassen auch den Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 unberührt und sollten nicht so verstanden werden, dass vernetzte Produkte und verbundene Dienste derart konzipiert werden müssen, dass damit auch andere als die für die Zwecke ihrer Verarbeitung erforderlichen personenbezogenen Daten gespeichert oder anderweitig verarbeitet werden. Es könnte Unionsrecht oder nationales Recht eingeführt werden, um weitere Besonderheiten festzulegen, wie etwa die Produktdaten, die über vernetzte Produkte oder verbundene Dienste zugänglich sein sollten, da diese Daten für den effizienten Betrieb, die Reparatur oder die Wartung dieser vernetzten Produkte oder verbundenen Dienste von wesentlicher Bedeutung sein können. Führen spätere Aktualisierungen oder Änderungen eines vernetzten Produkts oder eines verbundenen Dienstes durch den Hersteller oder eine andere Partei zu zusätzlichen zugänglichen Daten oder zu einer Einschränkung ursprünglich zugänglicher Daten, so sollten diese Änderungen dem Nutzer im Rahmen der Aktualisierung oder Änderung mitgeteilt werden.

18. "**Geschäftsgeheimnis**" ein Geschäftsgeheimnis im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2016/943;
19. "**Inhaber eines Geschäftsgeheimnisses**" den Inhaber eines Geschäftsgeheimnisses im Sinne von Artikel 2 Nummer 2 der Richtlinie (EU) 2016/943;
20. "**Profiling**" Profiling im Sinne des Artikels 4 Absatz 4 der Verordnung (EU) 2016/679;
21. "**Bereitstellung auf dem Markt**" jede entgeltliche oder unentgeltliche Abgabe eines vernetzten Produkts zum Vertrieb, Verbrauch oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;
22. "**Inverkehrbringen**" die erstmalige Bereitstellung eines vernetzten Produkts auf dem Unionsmarkt;

23. **“Verbraucher”** jede natürliche Person, die zu Zwecken handelt, die außerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen;
24. **“Unternehmen”** eine natürliche oder juristische Person, die in Bezug auf von dieser Verordnung erfasste Verträge und Vorgehensweisen zu Zwecken im Zusammenhang mit ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt;
25. **“Kleinunternehmen”** ein Kleinunternehmen im Sinne des Artikels 2 Absatz 2 des Anhangs der Empfehlung 2003/361/;
26. **“Kleinstunternehmen”** ein Kleinstunternehmen im Sinne des Artikels 2 Absatz 3 des Anhangs der Empfehlung 2003/361/;
27. **“Einrichtungen der Union”** die Einrichtungen, Stellen und Agenturen der Union, die gemäß Rechtsakten eingerichtet wurden, die auf der Grundlage des Vertrags über die Europäische Union, des AEUV oder des Vertrags zur Gründung der Europäischen Atomgemeinschaft angenommen wurden;
28. **“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;
29. **“öffentlicher Notstand”** eine zeitlich begrenzte Ausnahmesituation – wie etwa 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 oder eines Mitgliedstaats bzw. 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 unmittelbaren Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem betroffenen Mitgliedstaat birgt und die nach den einschlägigen Verfahren des Unionsrechts oder des nationalen Rechts festgestellt und amtlich ausgerufen wurde;
30. **“Kunde”** eine natürliche oder juristische Person, die mit einem Anbieter von Datenverarbeitungsdiensten eine vertragliche Beziehung eingegangen ist, um einen oder mehrere Datenverarbeitungsdienste in Anspruch zu nehmen;
31. **“virtuelle Assistenten”** Software, die Aufträge, Aufgaben oder Fragen verarbeiten kann, auch aufgrund von Eingaben in Ton- und Schriftform, mit Gesten oder Bewegungen, und die auf der Grundlage dieser Aufträge, Aufgaben oder Fragen den Zugang zu anderen Diensten gewährt oder die Funktionen von vernetzten Produkten steuert;
32. **“digitale Vermögenswerte”** Elemente in digitaler Form – einschließlich Anwendungen -, für die der Kunde ein Nutzungsrecht hat, unabhängig von der vertraglichen Beziehung mit dem Datenverarbeitungsdienst, den er wechseln möchte;

(83) Digitale Vermögenswerte beziehen sich auf Elemente in digitaler Form, für die der Kunde das Nutzungsrecht hat, einschließlich Anwendungen und Metadaten im Zusammenhang mit der Konfiguration von Einstellungen, der Sicherheit und der Verwaltung von Zugangs- und Kontrollrechten, sowie andere Elemente wie Darstellungen von Virtualisierungstechnologien, einschließlich virtueller Maschinen und Container. Digitale Vermögenswerte können übertragen werden, sofern der Kunde ein Nutzungsrecht hat, das unabhängig von der vertraglichen Beziehung mit dem Datenverarbeitungsdienst, den er wechseln möchte, besteht. Die vorstehend genannten

anderen Elemente sind die Voraussetzung dafür, dass der Kunde seine Daten und Anwendungen im Umfeld des übernehmenden Anbieters von Datenverarbeitungsdiensten effektiv nutzen kann.

33. **“IKT-Infrastruktur in eigenen Räumlichkeiten”** IKT-Infrastruktur und Rechenressourcen, die im Eigentum des Kunden stehen oder vom Kunden gemietet oder geleast werden und die sich im Rechenzentrum des Kunden befinden und von ihm oder einem Dritten betrieben wird bzw. werden;
34. **“Wechsel”** den Prozess, an dem ein Quellenanbieter von Datenverarbeitungsdiensten, ein Kunde eines Datenverarbeitungsdienstes und gegebenenfalls ein übernehmender Anbieter von Datenverarbeitungsdiensten beteiligt sind und bei dem der Kunde eines Datenverarbeitungsdienstes von der Nutzung eines Datenverarbeitungsdienstes zur Nutzung eines anderen Datenverarbeitungsdienstes der gleichen Dienstart oder eines anderen Dienstes, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird oder der einem einer IKT-Infrastruktur in eigenen Räumlichkeiten angeboten wird, auch durch Extraktion, Umwandlung und Hochladen der Daten, wechselt;

(85) Der Wechsel ist ein Vorgang, der vom Kunden ausgeht und aus mehreren Schritten – einschließlich Datenextraktion – besteht, was das Herunterladen der Daten aus dem Ökosystem des ursprünglichen Anbieters von Datenverarbeitungsdiensten bezeichnet, die Umwandlung der Daten, wenn diese so strukturiert sind, dass sie nicht in das Schema des Zielspeicherorts passen, sowie das Hochladen der Daten in einen neuen Zielspeicherort. In bestimmten, in dieser Verordnung beschriebenen Situationen sollte es auch als Wechsel gelten, wenn ein bestimmter Dienst aus dem Vertrag herausgelöst und zu einem anderen Anbieter verlegt wird. Der Wechsel wird manchmal von einem Dritten im Namen des Kunden vollzogen. 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 auch für den betreffenden Dritten gelten. Anbieter von Datenverarbeitungsdiensten und Kunden tragen in Abhängigkeit vom Verfahrensschritt ein unterschiedliches Maß an Verantwortung. So ist beispielsweise der ursprüngliche Anbieter von Datenverarbeitungsdiensten dafür verantwortlich, die Daten in ein maschinenlesbares Format zu extrahieren, während der Kunde und der übernehmende Anbieter von Datenverarbeitungsdiensten die Daten in die neue Umgebung hochladen müssen, sofern kein spezieller professioneller Übergangsdienst in Anspruch genommen wird. Ein Kunde, der beabsichtigt, die in dieser Verordnung vorgesehenen Rechte im Zusammenhang mit dem Wechsel auszuüben, sollte den ursprünglichen Anbieter von Datenverarbeitungsdiensten von der Entscheidung, entweder zu einem anderen Anbieter von Datenverarbeitungsdiensten oder zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu wechseln oder die Vermögenswerte und exportierbaren Daten des Kunden zu löschen, in Kenntnis setzen.

35. **“Datenextraktionsentgelte”** Datenübertragungsentgelte, die den Kunden dafür in Rechnung gestellt werden, dass ihre Daten über das Netz aus der IKT-Infrastruktur eines Anbieters von Datenverarbeitungsdiensten in die Systeme anderer Anbieter oder in IKT-Infrastruktur in eigenen Räumlichkeiten extrahiert werden;
36. **“Wechselentgelte”** andere Entgelte als Standarddienstentgelte oder Sanktionen bei vorzeitiger Kündigung, die ein Anbieter von Datenverarbeitungsdiensten bei einem Kunden für die Handlungen erhebt, die in dieser Verordnung für den Wechsel zu den Systemen eines anderen Anbieters oder IKT-Infrastruktur in eigenen Räumlichkeiten vorgeschrieben sind, einschließlich Datenextraktionsentgelten;

(88) Wechselentgelte sind Entgelte, die Anbieter von Datenverarbeitungsdiensten bei ihren Kunden für den Vollzug des Wechsels erheben. Üblicherweise sollen mit diesen Entgelten die Kosten, die dem ursprünglichen Anbieter von Datenverarbeitungsdiensten durch den Wechsel entstehen können, an den Kunden, der den Wechsel wünscht, weitergegeben werden. Gängige Beispiele für Wechselentgelte sind mit der Datenübertragung von einem Anbieter von Datenverarbeitungsdiensten zu einem anderen oder von einem Anbieter zu einer IKT-Infrastruktur in den eigenen Räumlichkeiten verbundene Kosten (“Datenextraktionsentgelte”) oder durch spezifische Unterstützungstätigkeiten während des Vollzugs des Wechsels anfallende Kosten. Unangemessen hohe Datenextraktionsentgelte und andere ungerechtfertigte Entgelte, die in keinem Zusammenhang mit den tatsächlichen Kosten des Wechsels stehen, behindern Anbieterwechsel seitens des Kunden, schränken den freien Datenfluss ein, können den Wettbewerb einschränken und zu Abhängigkeitsverhältnissen des Kunden in Bezug auf einen bestimmten Dienst führen, da Anreize, sich für einen anderen oder weiteren Diensteanbieter zu entscheiden, verringert werden. Daher sollten Wechselentgelte nach drei Jahren nach dem Tag des Inkrafttretens dieser Verordnung abgeschafft werden. Anbieter von Datenverarbeitungsdiensten sollten bis zu diesem Zeitpunkt ermäßigte Wechselentgelte erheben können.

37. **“Funktionsäquivalenz”** die Wiederherstellung – auf der Grundlage der exportierbaren Daten und digitalen Vermögenswerte des Kunden – eines Mindestmaßes an Funktionalität in der Umgebung eines neuen Datenverarbeitungsdienstes der gleichen Dienstart nach dem Wechsel, wenn der übernehmende Datenverarbeitungsdienst als Reaktion auf dieselbe Eingabe für gemeinsame Funktionen, die dem Kunden im Rahmen des Vertrags bereitgestellt werden, ein materiell vergleichbares Ergebnis erbringt;

(86) Funktionsäquivalenz bedeutet, dass nach einem Wechsel ein Mindestfunktionsumfang auf der Grundlage der exportierbaren Daten und digitalen Vermögenswerte des Kunden in der Umgebung des neuen Datenverarbeitungsdienstes der gleichen Dienstart wiederhergestellt wird, wobei der übernehmende Datenverarbeitungsdienst bei gemeinsam genutzten Funktionen, die dem Kunden im Rahmen des Vertrags bereitgestellt werden, ein im Wesentlichen vergleichbares Ergebnis liefert. Von Anbietern von Datenverarbeitungsdiensten kann nur erwartet werden, dass sie die Funktionsäquivalenz in Bezug auf die Funktionen ermöglichen, die sowohl vom ursprünglichen als auch vom übernehmenden Datenverarbeitungsdienst unabhängig voneinander angeboten werden. Anbieter von Datenverarbeitungsdiensten sind nach der vorliegenden Verordnung nur zur Erleichterung der Funktionsäquivalenz verpflichtet, wenn sie Dienste des Bereitstellungsmodells IaaS anbieten.

38. **“exportierbare Daten”** für die Zwecke von den Artikeln 23 bis 31 und Artikel 35 die Eingabe- und Ausgabedaten einschließlich Metadaten, die unmittelbar oder mittelbar durch die Nutzung des Datenverarbeitungsdienstes durch den Kunden oder gemeinsam generiert werden, mit Ausnahme der Vermögenswerte oder Daten eines Anbieters von Datenverarbeitungsdiensten oder Dritter, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis darstellen;
39. **“intelligenter Vertrag”** ein Computerprogramm, das für die automatisierte Ausführung einer Vereinbarung oder eines Teils davon verwendet wird, wobei eine Abfolge elektronischer Datensätze verwendet wird und die Integrität dieser Datensätze sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet werden;
40. **“Interoperabilität”** die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, vernetzten Produkten, Anwendungen, Datenverarbeitungsdiensten oder Komponenten, Daten auszutauschen und zu nutzen, um ihre Funktionen auszuführen;

41. “**offene Interoperabilitätsspezifikationen**” eine technische Spezifikation im Bereich der Informations- und Kommunikationstechnologie, die leistungsbezogen darauf ausgerichtet sind, die Interoperabilität zwischen Datenverarbeitungsdiensten herzustellen;
42. “**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;
43. “**harmonisierte Norm**” eine harmonisierte Norm im Sinne des Artikels 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012.

## Kapitel II Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

### Artikel 3 Pflicht der Zugänglichmachung von Produktdaten und verbundenen Dienstdaten für den Nutzer

- (1) Vernetzte Produkte werden so konzipiert und hergestellt und verbundene Dienste werden so konzipiert und erbracht, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.
- (2) Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein vernetztes Produkt werden dem Nutzer vom Verkäufer, Vermieter oder Leasinggeber – wobei es sich auch um den Hersteller handeln kann – mindestens folgende Informationen in klarer und verständlicher Art und Weise bereitgestellt:
  - a) die Art, das Format und der geschätzte Umfang der Produktdaten, die das vernetzte Produkt generieren kann;
  - b) die Angabe, ob das vernetzte Produkt in der Lage ist, Daten kontinuierlich und in Echtzeit zu generieren;
  - c) die Angabe, ob das vernetzte Produkt in der Lage ist, Daten auf einem Gerät oder einem entfernten Server zu speichern, gegebenenfalls einschließlich der vorgesehenen Speicherdauer;
  - d) die Angabe, wie der Nutzer auf die Daten zugreifen, sie abrufen oder gegebenenfalls löschen kann, einschließlich der technischen Mittel hierfür sowie die betreffenden Nutzungsbedingungen und die betreffende Dienstqualität.

(24) Vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein vernetztes Produkt sollte der Verkäufer, Vermieter oder Leasinggeber – bei dem es sich auch um den Hersteller handeln kann – dem Nutzer Informationen zu den Produktdaten die das vernetzte Produkt generieren kann, einschließlich der Art, des Formats und der geschätzten Datenmenge, auf klare und verständliche Weise bereitstellen. Dies könnte,

soweit verfügbar, Informationen über Datenstrukturen, Datenformate, Vokabulare, Klassifizierungssysteme, Taxonomien und Codelisten sowie klare und ausreichende Informationen einschließen, die für die Ausübung der Nutzerrechte relevant sind, und darüber, wie die Daten gespeichert oder abgerufen werden können oder wie auf sie zugegriffen werden kann, einschließlich der Nutzungsbedingungen und der Dienstqualität von Anwendungsprogrammierschnittstellen oder gegebenenfalls der Bereitstellung von Software Development Kits. Diese Pflicht sorgt für Transparenz in Bezug auf die generierten Produktdaten und vereinfacht den Zugang für den Nutzer. Der Informationspflicht könnte beispielsweise dadurch nachgekommen werden, dass eine stabile URL-Adresse im Internet unterhalten wird, die als Weblink oder QR-Code verbreitet werden kann und zu den einschlägigen Informationen führt, die der Verkäufer, der Vermieter oder der Leasinggeber – bei dem es sich auch um den Hersteller handeln kann – dem Nutzer vor Abschluss eines Kauf-, Miet- oder Leasingvertrags für ein vernetztes Produkt bereitstellen könnte. 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. Zwar kann vom Dateninhaber nicht erwartet werden, dass er die Daten mit Blick auf die Bedürfnisse des Nutzers des vernetzten Produkts unbegrenzt speichert, jedoch sollte er eine angemessene Regelung in Bezug auf die Dauer der Datenspeicherung anwenden, gegebenenfalls im Einklang mit dem Grundsatz der Speicherbegrenzung nach Artikel 5 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679, die die wirksame Anwendung der Datenzugangsrechte gemäß dieser Verordnung ermöglicht. Die Informationspflicht berührt nicht die Pflicht des Verantwortlichen, der betroffenen Person Informationen gemäß den Artikeln 12, 13 und 14 der Verordnung (EU) 2016/679 zu übermitteln. Die Pflicht, vor Abschluss eines Vertrags über die Erbringung eines verbundenen Dienstes die entsprechenden Informationen bereitzustellen, sollte beim potenziellen Dateninhaber liegen, unabhängig davon, ob der Dateninhaber einen Kauf-, Miet- oder Leasingvertrag für ein vernetztes Produkt abschließt. Ändern sich die Informationen während der Lebensdauer des vernetzten Produkts oder der Vertragslaufzeit für den verbundenen Dienst, einschließlich wenn sich der Zweck, zu dem diese Daten verwendet werden sollen, gegenüber dem ursprünglich vorgesehenen Zweck ändert, so sollten diesbezügliche Informationen auch dem Nutzer bereitgestellt werden.

- (3) Vor Abschluss eines Vertrags für die Erbringung eines verbundenen Dienstes stellt der Anbieter eines solchen verbundenen Dienstes dem Nutzer mindestens folgende Informationen in einer klaren und verständlichen Art und Weise bereit:
- a) die Art, der geschätzte Umfang und die Häufigkeit der Erhebung der Produktdaten, die der potenzielle Dateninhaber voraussichtlich erhalten wird, und gegebenenfalls die Modalitäten, nach denen der Nutzer auf diese Daten zugreifen oder sie abrufen kann, einschließlich der Modalitäten des künftigen Dateninhabers in Bezug auf die Speicherung und der Dauer der Aufbewahrung von Daten;
  - b) die Art und der geschätzte Umfang der zu generierenden verbundenen Dienstdaten sowie die Modalitäten, nach denen der Nutzer auf diese Daten zugreifen oder sie abrufen kann, einschließlich der Modalitäten des künftigen Dateninhabers in Bezug auf die Speicherung und der Dauer der Aufbewahrung von Daten;
  - c) die Angabe, ob der potenzielle Dateninhaber erwartet, ohne Weiteres verfügbare Daten selbst zu verwenden, und die Zwecke, zu denen diese Daten verwendet werden sollen, und ob er beabsichtigt, einem oder mehreren Dritten zu gestatten, die Daten zu mit dem Nutzer vereinbarten Zwecken zu verwenden;

- d) die Identität des potenziellen Dateninhabers, z. B. sein Handelsname und die Anschrift des Ortes, an dem er niedergelassen ist, sowie gegebenenfalls anderer Datenverarbeitungsparteien;
- e) die Kommunikationsmittel, über die der potenzielle Dateninhaber schnell kontaktiert und effizient mit ihm kommuniziert werden kann;
- f) die Angabe, wie der Nutzer darum ersuchen kann, dass die Daten an einen Dritten weitergegeben werden, und wie er die Datenweitergabe gegebenenfalls beenden kann;
- g) das Recht des Nutzers, bei der in Artikel 37 genannten zuständigen Behörde Beschwerde wegen eines Verstoßes gegen eine der Bestimmungen dieses Kapitels einzulegen;
- h) die Angabe, ob ein potenzieller Dateninhaber Inhaber von Geschäftsgeheimnissen ist, die in den Daten enthalten sind, die über das vernetzte Produkt zugänglich sind oder die bei der Erbringung eines verbundenen Dienstes generiert werden, und, wenn der potenzielle Dateninhaber nicht Inhaber von Geschäftsgeheimnissen ist, die Identität des Inhabers des Geschäftsgeheimnisses;
- i) die Dauer des Vertrags zwischen dem Nutzer und dem potenziellen Dateninhaber sowie die Ausgestaltung für die vorzeitige Beendigung eines solchen Vertrags.

#### **Artikel 4 Rechte und Pflichten von Nutzern und Dateninhabern in Bezug auf den Zugang zu sowie die Nutzung und die Bereitstellung von Produktdaten und verbundenen Dienstdaten**

(27) In konzentrierten Sektoren, in denen die Endnutzer durch eine kleine Zahl von Herstellern mit vernetzten Produkten versorgt werden, stehen den Nutzern unter Umständen nur begrenzte Möglichkeiten für den Datenzugang, die Datennutzung und die Weitergabe von Daten zur Verfügung. Unter diesen Umständen reichen vertragliche Vereinbarungen möglicherweise nicht aus, um das Ziel der Stärkung der Handlungsfähigkeit der Nutzer zu erreichen, was es den Nutzern erschwert, aus den Daten, die mit den von ihnen gekauften, gemieteten oder geleasten vernetzten Produkten generiert werden, Wert zu schöpfen. Folglich ist das Potenzial für innovative kleinere Unternehmen, datengestützte Lösungen auf wettbewerbsfähige Weise anzubieten, und für eine vielfältige Datenwirtschaft in der Union begrenzt. Diese Verordnung sollte daher auf den jüngsten Entwicklungen in bestimmten Sektoren aufbauen, wie dem Verhaltenskodex für die Weitergabe von Agrardaten im Wege eines Vertrags. Unionsrecht oder nationales Recht kann erlassen werden, um sektorspezifischen Bedürfnissen und Zielen Rechnung zu tragen. Darüber hinaus sollten Dateninhaber ohne Weiteres verfügbare Daten, bei denen es sich um nicht-personenbezogene Daten handelt, nicht verwenden, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte oder die Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer auf jegliche andere Art zu erlangen, die die gewerbliche Position dieses Nutzers auf den Märkten, auf denen dieser tätig ist, untergraben könnte. Dazu könnte gehören, 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 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 bereitge-

stellt werden, vorzugsweise mit fein abgestuften Berechtigungsoptionen (z. B. "Zugriff einmalig zulassen" oder "Zugriff nur während der Nutzung der App oder des Dienstes zulassen"), einschließlich der Möglichkeit, solche Berechtigungen zu widerrufen.

- (1) Soweit der Nutzer nicht direkt vom vernetzten Produkt oder verbundenen Dienst aus auf die Daten zugreifen kann, stellen die Dateninhaber dem Nutzer ohne Weiteres verfügbare Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit bereit. Dies geschieht auf einfaches Verlangen auf elektronischem Wege, soweit dies technisch durchführbar ist.
- (2) Nutzer und Dateninhaber können den Zugang zu sowie die Nutzung oder die erneute Weitergabe von Daten vertraglich beschränken, wenn eine solche Verarbeitung die im Unionsrecht oder im nationalen Recht festgelegten Sicherheitsanforderungen des vernetzten Produkts beeinträchtigen und damit zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen könnte. Die für die betreffenden Sektoren zuständigen Behörden können den Nutzern und Dateninhabern in diesem Zusammenhang technisches Fachwissen bereitstellen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Artikel, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.
- (3) Unbeschadet des Rechts des Nutzers, jederzeit vor einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen, kann der Nutzer im Zusammenhang mit einer Streitigkeit mit dem Dateninhaber in Bezug auf die in Absatz 2 genannten vertraglichen Beschränkungen oder Verbote
  - a) gemäß Artikel 37 Absatz 5 Buchstabe b eine Beschwerde bei der zuständigen Behörde einlegen oder
  - b) mit dem Dateninhaber vereinbaren, gemäß Artikel 10 Absatz 1 eine Streitbeilegungsstelle mit der Angelegenheit zu befassen.
- (4) Die Dateninhaber dürfen die Ausübung der Wahlmöglichkeiten oder Rechte durch den Nutzer nach diesem Artikel nicht unangemessen erschweren, auch nicht dadurch, dass sie dem Nutzer in nicht neutraler Weise Wahlmöglichkeiten anbieten oder die Autonomie, die Entscheidungsfreiheit oder die Wahlfreiheit des Nutzers durch die Struktur, die Gestaltung, die Funktion oder die Funktionsweise einer digitalen Benutzerschnittstelle oder eines Teils davon unterlaufen oder beeinträchtigen.
- (5) Um zu überprüfen, ob eine natürliche oder juristische Person als Nutzer für die Zwecke von Absatz 1 einzustufen ist, verlangt der Dateninhaber von dieser Person keine Informationen, die über das erforderliche Maß hinausgehen. Dateninhaber bewahren keine Informationen über den Zugang des Nutzers zu den verlangten Daten – insbesondere keine Protokolldaten – auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Nutzers und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist.

(29) Dateninhaber können eine geeignete Nutzeridentifizierung verlangen, um die Berechtigung eines Nutzers auf Zugang zu den Daten zu überprüfen. Im Falle perso-

nenbezogener Daten, die von einem Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet werden, sollten die Dateninhaber sicherstellen, dass das Zugangsverlangen vom Auftragsverarbeiter entgegengenommen und bearbeitet wird.

- (6) Geschäftsgeheimnisse werden gewahrt und nur offengelegt, wenn vom Dateninhaber und vom Nutzer vor der Offenlegung alle Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren. Der Dateninhaber oder, wenn sie nicht dieselbe Person sind, der Inhaber des Geschäftsgeheimnisses ermittelt, auch in den relevanten Metadaten, die als Geschäftsgeheimnisse geschützten Daten und vereinbart mit dem Nutzer angemessene technische und organisatorische Maßnahmen, die erforderlich sind, um die Vertraulichkeit der weitergegebenen Daten, insbesondere gegenüber Dritten, zu wahren; dies gilt etwa für Mustervertragsklauseln, Vertraulichkeitsvereinbarungen, strenge Zugangsprotokolle, technische Normen und die Anwendung von Verhaltenskodizes.

(31) Nach der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates (23) gilt der Erwerb, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses unter anderem dann als rechtmäßig, wenn der betreffende Erwerb oder die betreffende Nutzung oder Offenlegung nach Unionsrecht oder nationalem Recht vorgeschrieben oder zulässig ist. Nach dieser Verordnung sind Dateninhaber zwar dazu verpflichtet, bestimmte Daten gegenüber Nutzern oder vom Nutzer ausgewählten Dritten offenzulegen, selbst wenn diese Daten unter den Schutz des Geschäftsgeheimnisses fallen, doch sollte dies so ausgelegt werden, dass der Schutz von Geschäftsgeheimnissen nach Maßgabe der Richtlinie (EU) 2016/943 gewahrt wird. In diesem Zusammenhang sollten Dateninhaber dem Nutzer oder vom Nutzer ausgewählten Dritten die Wahrung der Vertraulichkeit von Daten, die als Geschäftsgeheimnisse gelten, vorschreiben können. Daher sollten Dateninhaber die Geschäftsgeheimnisse vor deren Offenlegung ermitteln und die Möglichkeit haben, mit Nutzern oder vom Nutzer ausgewählten Dritten notwendige Maßnahmen zur Wahrung ihrer Vertraulichkeit zu vereinbaren, unter anderem durch die Verwendung von Mustervertragsklauseln, Vertraulichkeitsvereinbarungen, strengen Zugangsprotokollen, technischen Standards und die Anwendung von Verhaltenskodizes. Neben der Verwendung der von der Kommission zu entwickelnden und zu empfehlenden Mustervertragsklauseln könnte auch die Festlegung von Verhaltenskodizes und technischen Standards in Bezug auf den Schutz von Geschäftsgeheimnissen bei der Verarbeitung der Daten dazu beitragen, das Ziel dieser Verordnung zu erreichen, und sollte daher vorangetrieben werden. Besteht keine Vereinbarung über die notwendigen Maßnahmen oder setzt ein Nutzer oder ein vom Nutzer ausgewählter Dritter diese vereinbarten Maßnahmen nicht um oder verstößt gegen die Vertraulichkeit von Geschäftsgeheimnissen, so sollte es dem Dateninhaber möglich sein, die Weitergabe der als Geschäftsgeheimnisse eingestufteten Daten zu verweigern oder auszusetzen. In solchen Fällen sollte der Dateninhaber dem Nutzer oder dem Dritten seine Entscheidung unverzüglich schriftlich mitteilen und die nationale zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, davon unterrichten, dass er die Weitergabe von Daten verweigert oder ausgesetzt hat, und angeben, welche Maßnahmen nicht vereinbart oder umgesetzt wurden und – sofern relevant – bei welchen Geschäftsgeheimnissen die Vertraulichkeit verletzt wurde. Grundsätzlich können Dateninhaber ein Datenzugangsverlangen gemäß dieser Verordnung nicht allein aufgrund dessen ablehnen, dass bestimmte Daten als Geschäftsgeheimnisse gelten, da dies die beabsichtigte Wirkung dieser Verordnung untergraben würde. In Ausnahmefällen sollte es einem Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, jedoch möglich sein, im Einzelfall ein Datenzugangsverlangen für die betreffenden spezifischen Daten abzulehnen, wenn er gegenüber dem Nutzer oder dem Dritten nachweisen kann, dass durch die Offenlegung dieses Geschäftsgeheimnisses trotz von dem Nutzer oder dem Dritten vorgenommener technischer und organisatorischer Maßnahmen mit hoher

Wahrscheinlichkeit ein schwerer wirtschaftlicher Schaden entsteht. Ein schwerer wirtschaftlicher Schaden geht mit schweren irreparablen wirtschaftlichen Verlusten einher. Der Dateninhaber sollte seine Weigerung gegenüber dem Nutzer oder dem Dritten unverzüglich in schriftlicher Form ordnungsgemäß begründen und die zuständige Behörde hiervon in Kenntnis setzen. Eine solche Begründung sollte sich auf objektive Fakten stützen, aus denen hervorgeht, dass durch die Offenlegung bestimmter Daten die konkrete Gefahr eines schweren wirtschaftlichen Schadens zu erwarten ist, und weshalb die zum Schutz der verlangten Daten ergriffenen Maßnahmen als nicht ausreichend erachtet werden. In diesem Zusammenhang kann etwaigen negativen Auswirkungen auf die Cybersicherheit Rechnung getragen werden. Unbeschadet des Rechts, vor einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen, kann der Nutzer oder der Dritte, der die Entscheidung des Dateninhabers, die Weitergabe von Daten abzuweisen oder zu verweigern oder auszusetzen, anfechten möchte, bei der zuständigen Behörde Beschwerde einlegen, die sodann unverzüglich entscheiden sollte, ob und unter welchen Bedingungen die Weitergabe der Daten beginnen oder wieder aufgenommen werden sollte, oder der Nutzer oder der Dritte kann mit dem Dateninhaber vereinbaren, eine Streitbelegungsstelle mit der Angelegenheit zu befassen. Die in dieser Verordnung vorgesehenen Ausnahmen von den Datenzugangsrechten sollten in keiner Weise die Rechte der betroffenen Personen auf Zugang und Datenübertragbarkeit gemäß der Verordnung (EU) 2016/679 beschränken.

- (7) Wenn keine Einigung über die in Absatz 6 genannten erforderlichen Maßnahmen erzielt wird oder wenn vom Nutzer die gemäß Absatz 6 vereinbarten Maßnahmen nicht umgesetzt werden oder die Vertraulichkeit der Geschäftsgeheimnisse verletzt wird, kann der Dateninhaber die Weitergabe von Daten, die als Geschäftsgeheimnisse eingestuft wurden, verweigern oder gegebenenfalls aussetzen. Die Entscheidung des Dateninhabers ist ordnungsgemäß zu begründen und dem Nutzer unverzüglich schriftlich mitzuteilen. In solchen Fällen teilt der Dateninhaber der gemäß Artikel 37 benannten zuständigen Behörde mit, dass er die Weitergabe von Daten verweigert oder ausgesetzt hat, und gibt an, welche Maßnahmen nicht vereinbart oder umgesetzt wurden und bei welchen Geschäftsgeheimnissen die Vertraulichkeit untergraben wurde.
- (8) Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Nutzer gemäß Absatz 6 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch die Offenlegung von Geschäftsgeheimnissen erleiden wird, kann er ein Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, insbesondere der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen und dem Nutzer unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß vorliegendem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.

(57) Dateninhaber können geeignete technische Schutzmaßnahmen anwenden, um die unrechtmäßige Offenlegung von oder den unrechtmäßigen Zugang zu Daten zu verhindern. Diese Maßnahmen sollten jedoch weder zwischen Datenempfängern unterscheiden noch den Zugang zu Daten und deren Nutzung für Nutzer oder Datenempfänger beeinträchtigen. Im Falle missbräuchlicher Praktiken eines Datenempfängers, wie Irreführung des Dateninhabers durch Bereitstellung falscher Informationen in der Absicht, die Daten für unrechtmäßige Zwecke zu nutzen, einschließlich der

Entwicklung eines konkurrierenden vernetzten Produkts auf der Grundlage der Daten, kann der Dateninhaber und gegebenenfalls, falls es sich nicht um die gleiche Person handelt, der Inhaber eines Geschäftsgeheimnisses oder der Nutzer den Dritten oder den Datenempfänger auffordern, unverzüglich Korrektur- oder Abhilfemaßnahmen zu ergreifen. Derartige Aufforderungen, insbesondere Aufforderungen zur Einstellung der Herstellung, des Angebots oder des Inverkehrbringens von Waren, abgeleiteten Daten oder Dienstleistungen sowie Aufforderungen zur Beendigung der Einfuhr, Ausfuhr und Lagerung rechtsverletzender Waren bzw. zu deren Vernichtung, sollten im Hinblick darauf bewertet werden, ob sie in Bezug auf die Interessen des Dateninhabers, des Inhabers des Geschäftsgeheimnisses oder des Nutzers verhältnismäßig sind.

- (9) Unbeschadet des Rechts eines Nutzers, jederzeit vor einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen, kann die Entscheidung eines Dateninhabers, die Weitergabe von Daten gemäß den Absätzen 7 und 8 abzulehnen, zu verweigern oder auszusetzen, von einem Nutzer angefochten werden, indem er
- a) gemäß Artikel 37 Absatz 5 Buchstabe b eine Beschwerde bei der zuständigen Behörde einreicht, die unverzüglich entscheidet, ob und unter welchen Bedingungen die Weitergabe der Daten beginnt oder wieder aufgenommen wird, oder
  - b) mit dem Dateninhaber vereinbart, gemäß Artikel 10 Absatz 1 eine Streitbeilegungsstelle mit der Angelegenheit zu befassen.
- (10) Der Nutzer darf die aufgrund eines Verlangens nach Absatz 1 erlangten Daten weder zur Entwicklung eines vernetzten Produkts nutzen, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht, noch darf er diese Daten mit dieser Absicht an einen Dritten weitergeben oder nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Herstellers oder gegebenenfalls des Dateninhabers zu erlangen.

(32) Das Ziel dieser Verordnung besteht nicht nur darin, die Entwicklung neuer, innovativer vernetzter Produkte oder verbundener Dienste zu fördern und Innovationen auf den Folgemärkten voranzutreiben, sondern auch darin, die Entwicklung völlig neuartiger Dienste unter Nutzung der betreffenden Daten anzuregen, auch auf der Grundlage von Daten aus einer Vielzahl von vernetzten Produkten oder verbundenen Diensten. Gleichzeitig soll mit der vorliegenden Verordnung verhindert werden, dass die Anreize für Investitionen in die Art vernetzter Produkte, von denen die Daten erlangt werden, verloren gehen, etwa wenn Daten zur Entwicklung eines konkurrierenden vernetzten Produkts genutzt werden, das insbesondere aufgrund seiner Merkmale, seines Preises und seines Verwendungszwecks von den Nutzern als austauschbar oder ersetzbar betrachtet wird. Diese Verordnung sieht kein Verbot der Entwicklung eines verbundenen Dienstes unter Nutzung der im Rahmen dieser Verordnung erlangten Daten vor, da dies eine unerwünschte abschreckende Wirkung auf Innovationen hätte. Die Innovationsanstrengungen der Dateninhaber werden durch das Verbot geschützt, Daten, zu denen im Rahmen dieser Verordnung Zugang besteht, für die Entwicklung eines vernetzten Konkurrenzprodukts zu nutzen. Ob ein vernetztes Produkt mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht, hängt davon ab, ob die beiden vernetzten Produkte auf demselben Produktmarkt miteinander konkurrieren. Dies ist auf der Grundlage der bewährten Grundsätze des Wettbewerbsrechts der Union zur Bestimmung des einschlägigen Produktmarkts zu entscheiden. Allerdings könnte ein rechtmäßiger Zweck der Nutzung der Daten, soweit die Anforderungen der vorliegenden Verordnung, des Unionsrechts oder des nationalen Rechts dabei erfüllt sind, Reverse Engineering (Nachkonstruktion) umfassen. Dabei kann es sich um Zwecke der Reparatur oder der

Verlängerung der Lebensdauer eines vernetzten Produkts oder der Erbringung von Folgemarkt-Diensten für vernetzte Produkte handeln.

- (11) Der Nutzer darf keine Zwangsmittel einsetzen oder Lücken in der zum Schutz der Daten bestehenden technischen Infrastruktur eines Dateninhabers ausnutzen, um Zugang zu Daten zu erlangen.
- (12) Handelt es sich bei dem Nutzer nicht um die betroffene Person, deren personenbezogene Daten verlangt werden, so darf der Dateninhaber personenbezogene Daten, die bei der Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert werden, dem Nutzer nur dann bereitstellen, wenn es für die Verarbeitung eine gültige Rechtsgrundlage gemäß Artikel 6 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 jener Verordnung sowie des Artikels 5 Absatz 3 der Richtlinie 2002/58/ erfüllt sind.

(34) Bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes können, insbesondere wenn es sich bei dem Nutzer um eine natürliche Person handelt, Daten generiert werden, die sich auf eine 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. Die betroffene Person kann der Nutzer oder eine andere natürliche Person sein. Zugang zu personenbezogenen Daten darf nur von einem Verantwortlichen oder einer betroffenen Person verlangt werden. Der Nutzer, der die betroffene Person ist, ist unter bestimmten Umständen gemäß der Verordnung (EU) 2016/679 berechtigt, auf die jenen Nutzer betreffenden personenbezogenen Daten zuzugreifen; diese Rechte bleiben von der vorliegenden Verordnung unberührt. Nach der vorliegenden Verordnung hat ein Nutzer, der eine natürliche Person ist, ferner das Recht auf Zugang zu allen durch die Nutzung eines vernetzten Produkts generierten Daten, ob personenbezogen oder nicht-personenbezogen. 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 gilt der Nutzer als Verantwortlicher. Dementsprechend benötigt ein Nutzer, der als Verantwortlicher Zugang zu personenbezogenen Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert werden, zu verlangen beabsichtigt, für die Verarbeitung der Daten eine Rechtsgrundlage gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679, wie etwa die Einwilligung der betroffenen Person oder die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist. Dieser Nutzer sollte sicherstellen, dass die betroffene Person angemessen über die spezifischen, 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 die einschlägigen Pflichten zur Einhaltung der genannten Verordnung erfüllt. Es sollte davon ausgegangen werden, dass ein solcher Nutzer, sobald Daten bereitgestellt wurden, seinerseits Dateninhaber werden kann, wenn jener Nutzer die Kriterien dieser Verordnung erfüllt, und damit seinerseits den Pflichten zur Bereitstellung von Daten im Rahmen dieser Verordnung unterliegen kann.

- (13) Der Dateninhaber darf ohne Weiteres verfügbare Daten, bei denen es sich um nicht-personenbezogene Daten handelt, nur auf der Grundlage eines Vertrags mit dem Nutzer nutzen. Der Dateninhaber darf solche Daten nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers

oder in die Nutzung durch den Nutzer auf jegliche andere Art, die die gewerbliche Position dieses Nutzers auf Märkten, auf denen dieser tätig ist, untergraben könnte, zu erlangen.

(36) Der Zugang zu auf Endgeräten gespeicherten von über Endgeräte zugänglichen Daten unterliegt der Richtlinie 2002/58/ und erfordert die Einwilligung des Teilnehmers oder Nutzers im Sinne der genannten Richtlinie, es sei denn, der Datenzugang ist unbedingt für die Bereitstellung eines vom Nutzer oder vom Teilnehmer ausdrücklich verlangten Dienstes der Informationsgesellschaft oder zum alleinigen Zweck der Übertragung einer Nachricht erforderlich. Die Richtlinie 2002/58/ schützt die Integrität der Endgeräte eines 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.

(14) Dateninhaber dürfen nicht-personenbezogene Produktdaten Dritten zu keinen anderen kommerziellen oder nichtkommerziellen Zwecken als zur Erfüllung ihres Vertrags mit dem Nutzer bereitstellen. Gegebenenfalls werden Dritte von Dateninhabern vertraglich verpflichtet, die von ihnen erhaltenen Daten nicht erneut weiterzugeben.

(25) Diese Verordnung sollte nicht so verstanden werden, dass sie Dateninhabern ein neues Recht auf die Nutzung von Produktdaten oder verbundener Dienstdaten verleiht. Ist der Hersteller eines vernetzten Produkts der Dateninhaber, so sollte ein Vertrag zwischen dem Hersteller und dem Nutzer die Grundlage für die Nutzung nicht-personenbezogener Daten durch den Hersteller bilden. Ein solcher Vertrag könnte Teil einer Vereinbarung über die Erbringung des verbundenen Dienstes sein, die zusammen mit dem Kauf-, Miet- oder Leasingvertrag für das vernetzte Produkt getroffen werden kann. Jede Vertragsklausel, nach der der Dateninhaber die Produktdaten oder verbundenen Dienstdaten nutzen darf, sollte für den Nutzer transparent sein, auch in Bezug auf die Zwecke, zu denen der Dateninhaber die Daten zu verwenden beabsichtigt. Zu diesen Verwendungszwecken könnten die Verbesserung der Funktionsweise des vernetzten Produkts oder verbundener Dienste, die Entwicklung neuer Produkte oder Dienste oder die Aggregation von Daten mit dem Ziel, die sich daraus ergebenden abgeleiteten Daten Dritten bereitzustellen, gehören, sofern diese abgeleiteten Daten es nicht ermöglichen, einzelne Daten zu ermitteln, die von dem vernetzten Produkt an den Dateninhaber übermittelt wurden, und es Dritten nicht ermöglichen, diese Daten aus dem Datensatz abzurufen. Jede Vertragsänderung sollte der fundierten Zustimmung des Nutzers bedürfen. Diese Verordnung hindert die Parteien nicht daran, Vertragsklauseln zu vereinbaren, die bewirken, dass die Nutzung von nicht-personenbezogenen Daten oder bestimmten Kategorien nicht-personenbezogener Daten durch einen Dateninhaber ausgeschlossen oder eingeschränkt wird. Sie hindert die Parteien auch nicht daran, zu vereinbaren, dass Produktdaten oder verbundene Dienstdaten Dritten direkt oder indirekt, einschließlich sofern einschlägig über einen anderen Dateninhaber, bereitgestellt werden können. Darüber hinaus steht diese Verordnung auch sektorspezifischen Regulierungsanforderungen nach Unionsrecht oder nach mit dem Unionsrecht im Einklang stehendem nationalen Recht nicht entgegen, die die Nutzung bestimmter Daten durch den Dateninhaber aus genau festgelegten Gründen der öffentlichen Ordnung ausschließen oder einschränken würden. Ferner steht diese Verordnung dem nicht entgegen, dass Nutzer im Falle von Geschäftsbeziehungen zwischen Unternehmen Dritten oder Dateninhabern unter jeglichen rechtmäßigen Vertragsklauseln Daten bereitstellen, unter anderem indem sie vereinbaren, eine erneute Weitergabe dieser Daten zu begrenzen oder einzuschränken, oder dass Nutzer beispielsweise für den Verzicht auf ihr Recht, diese Daten zu verwenden oder weiterzugeben, eine angemessene Gegenleistung erhalten. Obwohl der Begriff "Dateninhaber" öffentliche Stellen im Allgemeinen nicht einschließt, kann er jedoch öffentliche Unternehmen einschließen.

## Artikel 5 Recht des Nutzers auf Weitergabe von Daten an Dritte

(26) Um das Entstehen liquider, fairer und effizienter Märkte für nicht-personenbezogene Daten zu fördern, sollten die Nutzer vernetzter Produkte Daten mit minimalem rechtllichem und technischem Aufwand, auch für kommerzielle Zwecke, an andere weitergeben können. Für Unternehmen ist es derzeit oft schwierig, die Personal- oder EDV-Kosten zu rechtfertigen, die anfallen, um nicht-personenbezogene Datensätze oder Datenprodukte aufzubereiten und sie potenziellen Gegenparteien über Datenvermittlungsdienste, einschließlich Datenmarktplätze, anzubieten. 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, faire und effiziente Märkte für nicht-personenbezogene Daten entstehen können, muss geklärt werden, welche Partei das Recht hat, solche Daten auf einem Markt anzubieten. Nutzer sollten daher das Recht haben, nicht-personenbezogene Daten zu kommerziellen und nichtkommerziellen Zwecken an Datenempfänger weiterzugeben. Eine solche Datenweitergabe könnte direkt durch den Nutzer, auf Verlangen des Nutzers über einen Dateninhaber oder durch Datenvermittlungsdienste erfolgen. Datenvermittlungsdienste im Sinne der Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates (22) könnten der Datenwirtschaft dienen, indem sie Geschäftsbeziehungen zwischen Nutzern, Datenempfängern und Dritten herstellen und die Nutzer bei der Ausübung ihres Datennutzungsrechts unterstützen, etwa indem sie die Anonymisierung der personenbezogenen Daten oder die Aggregation des Zugangs zu Daten von einer Vielzahl einzelner Nutzer sicherstellen. Sind Daten von der Verpflichtung eines Dateninhabers, sie Nutzern oder Dritten bereitzustellen, ausgenommen, so könnte der Umfang dieser Daten in dem zwischen dem Nutzer und dem Dateninhaber geschlossenen Vertrag über die Erbringung eines verbundenen Dienstes festgelegt werden, sodass die Nutzer leicht feststellen können, welche Daten ihnen für die Weitergabe an Datenempfänger oder Dritte bereitstehen. Dateninhaber sollten Dritten nicht-personenbezogene Produktdaten weder zu kommerziellen noch zu nichtkommerziellen Zwecken bereitstellen, außer es geht um die Erfüllung ihres Vertrags mit dem Nutzer; dies sollte die rechtlichen Anforderungen nach dem Unionsrecht oder dem nationalen Recht an einen Dateninhaber für die Bereitstellung von Daten unberührt lassen. Gegebenenfalls sollten Dateninhaber Dritte vertraglich dazu verpflichten, die von ihnen erhaltenen Daten nicht erneut weiterzugeben.

(30) Dem Nutzer sollte es freistehen, die Daten zu jedem rechtmäßigen Zweck zu verwenden. Dazu gehören die Bereitstellung der Daten, die der Nutzer im Rahmen der Ausübung seiner Rechte nach dieser Verordnung erhalten hat, für einen Dritten, der einen Folgemarkt-Dienst anbietet, der möglicherweise mit einem von einem Dateninhaber bereitgestellten Dienst im Wettbewerb steht, oder die Anweisung hierzu an den Dateninhaber. Das Zugangsverlangen sollte vom Nutzer oder von einem bevollmächtigten Dritten gestellt werden, der im Namen eines Nutzers handelt, einschließlich von einem Erbringer eines Datenvermittlungsdienstes. Dateninhaber sollten sicherstellen, dass die einem Dritten bereitgestellten Daten so genau, vollständig, zuverlässig, relevant und aktuell sind wie die bei der Nutzung des vernetzten Produkts oder verbundenen Dienstes generierten Daten, auf die der Dateninhaber selbst zugreifen kann oder darf. Rechte des geistigen Eigentums sollten bei der Verarbeitung der Daten gewahrt werden. Es ist wichtig, dass weitere Anreize für Investitionen in Produkte bestehen, deren Funktionen auf der Nutzung der Daten von in diese Produkte eingebauten Sensoren basieren.

(35) Produktdaten oder verbundene Dienstdaten sollten Dritten nur auf Verlangen des Nutzers bereitgestellt werden. Dementsprechend ergänzt die vorliegende Verordnung das in Artikel 20 der Verordnung (EU) 2016/679 verankerte Recht einer betroffenen Person, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie auch einem anderen Verantwortlichen zu übertragen, wenn diese Daten mithilfe automatisierter Verfahren 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 der genannten Verordnung 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 der Verordnung (EU) 2016/679 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 in Fällen gilt, in denen ein vernetztes Produkt oder verbundener Dienst durch seine Konzeption das Verhalten einer betroffenen Person oder andere Informationen in Bezug auf eine betroffene Person passiv erfasst. Die in dieser Verordnung enthaltenen Rechte ergänzen das Recht, personenbezogene Daten gemäß Artikel 20 der Verordnung (EU) 2016/679 auf verschiedene Weise zu erhalten und zu übertragen. Die vorliegende Verordnung gewährt Nutzern das Recht auf Zugang und darauf, einem Dritten alle Produktdaten oder verbundenen Dienstdaten bereitzustellen, unabhängig davon, ob es sich um personenbezogene Daten handelt, sowie unabhängig von der Unterscheidung zwischen aktiv bereitgestellten oder passiv erfassten Daten und von der Rechtsgrundlage für die Verarbeitung. Im Gegensatz zu Artikel 20 der Verordnung (EU) 2016/679 wird mit der vorliegenden Verordnung die technische Machbarkeit des Zugangs Dritter zu allen Arten von Daten, die in ihren Anwendungsbereich fallen – ob personenbezogen oder nicht-personenbezogen –, vorgeschrieben und gewährleistet, womit sichergestellt wird, dass technische Hindernisse den Zugang zu diesen Daten nicht mehr behindern oder verhindern. Außerdem ermöglicht sie es Dateninhabern, eine angemessene Gegenleistung für Kosten festlegen, die durch die Bereitstellung des direkten Zugangs zu den vom vernetzten Produkt des Nutzers generierten Daten entstehen, die von Dritten, nicht aber vom Nutzer zu tragen ist. Wenn ein Dateninhaber und ein Dritter nicht in der Lage sind, Bedingungen für einen solchen direkten Zugang zu vereinbaren, sollte die betroffene Person in keiner Weise daran gehindert werden, die in der Verordnung (EU) 2016/679 festgelegten 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 einen Vertrag nicht die Verarbeitung besonderer Kategorien personenbezogener Daten durch den Dateninhaber oder den Dritten gestattet werden kann.

- (1) Auf Verlangen eines Nutzers oder einer im Namen eines Nutzers handelnden Partei stellt der Dateninhaber einem Dritten ohne Weiteres verfügbare Daten sowie die für die Auslegung und Nutzung dieser Daten erforderlichen Metadaten unverzüglich, für den Nutzer unentgeltlich, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einfach, sicher, für den Nutzer unentgeltlich, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit bereit. Die Daten werden durch den Dateninhaber für den Dritten gemäß den Artikeln 8 und 9 bereitgestellt.
- (2) Absatz 1 gilt nicht für ohne Weiteres verfügbare Daten im Zusammenhang mit der Prüfung neuer vernetzter Produkte, Stoffe oder Verfahren, die noch nicht in Verkehr gebracht werden, es sei denn, ihre Verwendung durch Dritte ist vertraglich genehmigt.
- (3) Ein Unternehmen, das gemäß Artikel 3 der Verordnung (EU) 2022/1925 als Torwächter benannt wurde, gilt nicht als im Sinne des vorliegenden Artikels zugelassener Dritter und ist daher nicht berechtigt,
  - a) einen Nutzer dazu aufzufordern oder durch geschäftliche Anreize in irgendeiner Weise, auch durch eine finanzielle oder sonstige Gegenleistung, dafür zu gewinnen, Daten, die vom Nutzer aufgrund eines Verlangens nach Artikel 4 Absatz 1 erlangt wurden, für einen seiner Dienste bereitzustellen;

- b) einen Nutzer dazu aufzufordern oder durch geschäftliche Anreize dafür zu gewinnen, vom Dateninhaber zu verlangen, gemäß Absatz 1 dieses Artikels Daten für einen seiner Dienste bereitzustellen;
  - c) von einem Nutzer Daten zu erhalten, die der Nutzer aufgrund eines Verlangens nach Artikel 4 Absatz 1 erlangt hat.
- (4) Für die Zwecke der Überprüfung, ob eine natürliche oder juristische Person für die Zwecke von Absatz 1 als Nutzer oder als Dritter einzustufen ist, werden vom Dateninhaber oder Dritten keine Informationen verlangt, die über das erforderliche Maß hinausgehen. Die Dateninhaber bewahren keine Informationen über den Zugang des Dritten zu den verlangten Daten auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Dritten und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist.
- (5) Der Dritte darf keine Zwangsmittel verwenden oder Lücken in der zum Schutz der Daten bestehenden technischen Infrastruktur des Dateninhabers ausnutzen, um Zugang zu Daten zu erlangen.
- (6) Der Dateninhaber darf ohne Weiteres verfügbare Daten nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Dritten oder in die Nutzung durch den Dritten auf jegliche andere Art, die die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte, zu erlangen, es sei denn, der Dritte hat eine solche Nutzung genehmigt und hat die technische Möglichkeit, diese Genehmigung jederzeit einfach zu widerrufen.

(33) Ein Dritter, dem Daten bereitgestellt werden, kann eine natürliche oder juristische Person, wie etwa ein Verbraucher, ein Unternehmen, eine Forschungseinrichtung, eine gemeinnützige Organisation oder ein in beruflicher Eigenschaft handelnder Rechtsträger, sein. Wenn ein Dateninhaber dem Dritten die Daten bereitstellt, sollte er seine Position nicht missbrauchen, um einen Wettbewerbsvorteil auf Märkten zu erlangen, auf denen der Dateninhaber und der Dritte möglicherweise in direktem Wettbewerb stehen. Der Dateninhaber sollte ohne Weiteres verfügbare Daten daher nicht dazu nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte oder Produktionsmethoden des Dritten oder die Nutzung durch den Dritten auf jegliche andere Weise zu erlangen, die die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte. Der Nutzer sollte in der Lage sein, nicht-personenbezogene Daten zu kommerziellen Zwecken an Dritte weiterzugeben. Nach Zustimmung des Nutzers und vorbehaltlich der Bestimmungen dieser Verordnung sollten Dritte die vom Nutzer eingeräumten Datenzugangsrechte auf andere Dritte übertragen können, auch gegen Entgelt. Datenmittler zwischen Unternehmen und Personal Information Management Systemen (personal information management systems, PIMS), die in der Verordnung (EU) 2022/868 als Datenvermittlungsdienste bezeichnet werden, können Nutzer oder Dritte bei der Aufnahme von Geschäftsbeziehungen mit einer unbestimmten Zahl potenzieller Gegenparteien zu jedem in den Anwendungsbereich dieser Verordnung fallenden rechtmäßigen Zweck unterstützen. Sie könnten eine entscheidende Rolle bei der Aggregation des Zugangs zu Daten spielen, sodass Big-Data-Analysen oder maschinelles Lernen erleichtert werden können, vorausgesetzt dass die Nutzer die volle Kontrolle darüber behalten, ob sie ihre Daten zu einer solchen Aggregation bereitstellen und unter welchen kommerziellen Bedingungen ihre Daten zu nutzen sind.

- (7) Handelt es sich bei dem Nutzer nicht um die betroffene Person, deren personenbezogene Daten verlangt werden, so dürfen personenbezogene Daten, die bei der Nutzung eines vernetzten Produktes oder verbundenen Dienstes generiert werden, nur dann

vom Dateninhaber dem Dritten bereitgestellt werden, wenn es für die Verarbeitung eine gültige Rechtsgrundlage gemäß Artikel 6 der Verordnung (EU) 2016/679 gibt und gegebenenfalls die Bedingungen des Artikels 9 jener Verordnung sowie des Artikels 5 Absatz 3 der Richtlinie 2002/58/ erfüllt sind.

- (8) Die Ausübung der Rechte der betroffenen Person gemäß der Verordnung (EU) 2016/679 und insbesondere des Rechts auf Datenübertragbarkeit gemäß Artikel 20 jener Verordnung darf durch Versäumnisse seitens des Dateninhabers oder des Dritten, Vorkehrungen für die Übermittlung der Daten zu treffen, nicht behindert, verhindert oder beeinträchtigt werden.
- (9) Geschäftsgeheimnisse werden gewahrt und Dritten gegenüber nur insoweit offengelegt, als diese Offenlegung für den zwischen dem Nutzer und dem Dritten vereinbarten Zweck unbedingt erforderlich ist. Der Dateninhaber oder, wenn sie nicht dieselbe Person sind, der Inhaber des Geschäftsgeheimnisses ermittelt, auch in den relevanten Metadaten, die als Geschäftsgeheimnisse geschützten Daten und vereinbart mit dem Dritten alle angemessenen technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Vertraulichkeit der weitergegebenen Daten zu wahren; dies gilt etwa für Mustervertragsklauseln, Vertraulichkeitsvereinbarungen, strenge Zugangsprotokolle, technische Normen und die Anwendung von Verhaltenskodizes.
- (10) Wenn keine Einigung über die in Absatz 9 des vorliegenden Artikels genannten erforderlichen Maßnahmen erzielt wird oder wenn von dem Dritten die gemäß Absatz 9 des vorliegenden Artikels vereinbarten Maßnahmen nicht umgesetzt werden oder die Vertraulichkeit der Geschäftsgeheimnisse verletzt wird, kann der Dateninhaber die Weitergabe von Daten, die als Geschäftsgeheimnisse ermittelt wurden, verweigern oder gegebenenfalls aussetzen. Die Entscheidung des Dateninhabers ist ordnungsgemäß zu begründen und dem Dritten unverzüglich schriftlich mitzuteilen. In solchen Fällen teilt der Dateninhaber der gemäß Artikel 37 benannten zuständigen Behörde mit, dass er die Weitergabe von Daten verweigert oder ausgesetzt hat, und gibt an, welche Maßnahmen nicht vereinbart oder umgesetzt wurden und bei welchen Geschäftsgeheimnissen die Vertraulichkeit verletzt wurde.
- (11) Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Dritten gemäß Absatz 9 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird, kann er das Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, insbesondere der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Grads der Vertraulichkeit der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen und Dritten unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.
- (12) Unbeschadet des Rechts Dritter, jederzeit vor einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen, kann ein Dritter, der eine Entscheidung des Dateninhabers, die Weitergabe von Daten gemäß den Absätzen 10 und 11 abzulehnen, zu verweigern oder auszusetzen, anfechten möchte:

- a) gemäß Artikel 37 Absatz 5 Buchstabe b eine Beschwerde bei der zuständigen Behörde einreichen, die unverzüglich entscheidet, ob und unter welchen Bedingungen die Weitergabe der Daten beginnt oder wieder aufgenommen wird, oder
- b) mit dem Dateninhaber vereinbaren, gemäß Artikel 10 Absatz 1 eine Streitbeilegungsstelle mit der Angelegenheit zu befassen.

(13) Das Recht gemäß Absatz 1 darf die Rechte betroffener Personen gemäß dem geltenden Unionsrecht und nationalen Recht über den Schutz personenbezogener Daten nicht beeinträchtigen.

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

(1) Ein Dritter verarbeitet die ihm nach Artikel 5 bereitgestellten Daten nur zu den Zwecken und unter den Bedingungen, die er mit dem Nutzer vereinbart hat und gemäß dem geltenden Unionsrecht und nationalen Recht über den Schutz personenbezogener Daten, einschließlich der Rechte der betroffenen Person, soweit personenbezogene Daten betroffen sind. Der Dritte löscht die Daten, sobald sie für den vereinbarten Zweck nicht mehr benötigt werden, sofern mit dem Nutzer in Bezug auf nicht-personenbezogene Daten nichts anderes vereinbart wurde.

(37) Um zu verhindern, dass Nutzer ausgenutzt werden, sollten Dritte, denen die Daten auf Verlangen des Nutzers bereitgestellt wurden, diese Daten nur zu den mit dem Nutzer vereinbarten Zwecken verarbeiten und sie nur an andere Dritte weitergeben, wenn der Nutzer seine Einwilligung zu dieser Datenweitergabe gegeben hat.

(2) Dem Dritten ist untersagt,

(38) Im Einklang mit dem Grundsatz der Datenminimierung sollten Dritte nur auf solche Informationen zugreifen, die für die Erbringung des vom Nutzer verlangten Dienstes erforderlich sind. Nachdem der Dritte Zugang zu den Daten erhalten hat, sollte er diese zu den mit dem Nutzer vereinbarten Zwecken verarbeiten, ohne dass der Dateninhaber eingreift. Es sollte für den Nutzer genauso einfach sein, den Zugang Dritter zu den Daten zu verweigern oder zu beenden, wie es für ihn ist, den Zugang zu den Daten zu gestatten. Weder Dritte noch Dateninhaber sollten die Ausübung der Wahlmöglichkeiten oder Rechte der Nutzer unangemessen erschweren, auch nicht, indem sie ihnen Wahlmöglichkeiten auf nicht neutrale Weise anbieten, oder den Nutzer zwingen, täuschen oder manipulieren, oder indem sie – auch mittels einer digitalen Benutzerschnittstelle oder eines Teils davon –, die Autonomie, Entscheidungsfähigkeit oder freie Wahlmöglichkeiten des Nutzers untergraben oder beeinträchtigen. 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, 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 unerwünschtem Verhalten zu bewegen und zu täuschen, indem sie zu Entscheidungen über die Datenoffenlegung angeregt werden, sowie um die Entscheidungsfindung der Nutzer des Dienstes unverhältnismäßig in einer Weise zu beeinflussen, die ihre Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten untergräbt oder beeinträchtigt. Übliche und rechtmäßige Geschäftspraktiken, die mit dem Unionsrecht im Einklang stehen, sollten an sich nicht als “Dark Patterns” angesehen werden. Dritte und Dateninhaber sollten ihren Pflichten nach dem ein-

schlägigen Unionsrecht nachkommen, insbesondere den Anforderungen der Richtlinien 98/6/ (24) und 2000/31/ (25) des Europäischen Parlaments und des Rates sowie der Richtlinien 2005/29/ und 2011/83/EU.

- a) den Nutzern die Ausübung ihrer Wahlmöglichkeiten oder ihrer Rechte gemäß Artikel 5 und dem vorliegenden Artikel übermäßig zu erschweren, auch nicht, indem er den Nutzern Wahlmöglichkeiten auf nicht neutrale Weise anbietet, oder die Nutzer in irgendeiner Weise zwingt, täuscht oder manipuliert oder – auch mittels einer digitalen Benutzerschnittstelle oder eines Teils davon – die Autonomie, Entscheidungsfähigkeit oder Wahlmöglichkeiten des Nutzers zu untergraben oder zu beeinträchtigen;
- b) unbeschadet des Artikels 22 Absatz 2 Buchstaben a und c der Verordnung (EU) 2016/679, die erhaltenen Daten für das Profiling zu nutzen, es sei denn, dies ist erforderlich, um den vom Nutzer gewünschten Dienst zu erbringen;

(39) Dritte sollten auch davon absehen, Daten, die in den Anwendungsbereich dieser Verordnung fallen, für das Profiling einer Person zu verwenden, es sei denn, solche Verarbeitungstätigkeiten sind unbedingt erforderlich, um den vom Nutzer verlangten Dienst zu erbringen, einschliesslich im Kontext der automatisierten Entscheidungsfindung. Die Anforderung, Daten zu löschen, wenn diese für den mit dem Nutzer vereinbarten Zweck nicht mehr erforderlich sind, ergänzt – sofern in Bezug nicht-personenbezogene Daten nichts anderes vereinbart wurde – das Recht der betroffenen Person auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679. Wenn ein Dritter ein Anbieter eines Datenvermittlungsdienstes ist, gelten die in der Verordnung (EU) 2022/868 für die betroffene Person vorgesehenen Schutzvorkehrungen. Der Dritte kann die Daten für die Entwicklung eines neuen und innovativen vernetzten Produkts oder verbundenen Dienstes, nicht aber für die Entwicklung eines konkurrierenden vernetzten Produkts verwenden.

- c) die erhaltenen Daten einem anderen Dritten bereitzustellen, es sei denn, die Daten werden auf der Grundlage eines Vertrags mit dem Nutzer bereitgestellt, und vorausgesetzt, der andere Dritte trifft alle zwischen dem Dateninhaber und dem Dritten vereinbarten Maßnahmen, die erforderlich sind, um die Vertraulichkeit von Geschäftsgeheimnissen zu wahren;
- d) die erhaltenen Daten einem Unternehmen, das gemäß Artikel 3 der Verordnung (EU) 2022/1925 als Torwächter benannt wurde, bereitzustellen;
- e) die erhaltenen Daten zu nutzen, um ein Produkt zu entwickeln, das mit dem vernetzten Produkt, von dem die Daten stammen, im Wettbewerb steht, oder die Daten zu diesem Zweck an einen anderen Dritten weiterzugeben. Dritten ist ferner untersagt, ihnen bereitgestellte nicht-personenbezogene Produktdaten oder verbundene Dienstdaten zu nutzen, um Einblicke in die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Dateninhabers oder die Nutzung durch den Dateninhaber zu gewinnen;
- f) die erhaltenen Daten in einer Weise zu verwenden, die nachteilige Auswirkungen auf die Sicherheit des vernetzten Produkts oder des verbundenen Dienstes haben;
- g) die mit dem Dateninhaber oder dem Inhaber der Geschäftsgeheimnisse gemäß Artikel 5 Absatz 9 vereinbarten Maßnahmen zu missachten und die Vertraulichkeit von Geschäftsgeheimnissen zu untergraben;

- h) den Nutzer, bei dem es sich um einen Verbraucher handelt, daran zu hindern – einschließlich auf der Grundlage eines Vertrags -, die erhaltenen Daten anderen Parteien bereitzustellen.

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

- (1) Die Pflichten nach diesem Kapitel gelten nicht für Daten, die bei der Nutzung von vernetzten Produkten generiert werden, die von einem Kleinstunternehmen oder einem Kleinunternehmen hergestellt oder konzipiert werden oder die bei der Nutzung von verbundenen Diensten generiert werden, die von einem solchen Unternehmen erbracht werden, sofern dieses Unternehmen kein Partnerunternehmen oder kein verbundenes Unternehmen im Sinne des Artikels 3 des Anhangs der Empfehlung 2003/361/ hat, das nicht als Kleinstunternehmen oder Kleinunternehmen gilt, und sofern das Kleinstunternehmen oder Kleinunternehmen nicht als Unterauftragnehmer mit der Herstellung oder der Konzeption eines vernetzten Produkts oder der Erbringung eines verbundenen Dienstes beauftragt wurde.

Das Gleiche gilt für Daten, die durch die Nutzung von vernetzten Produkten generiert werden, die von einem Unternehmen hergestellt werden, das seit weniger als einem Jahr als mittleres Unternehmen Sinne des Artikels 2 des Anhangs der Empfehlung 2003/361/ eingestuft ist, oder für verbundene Dienste, die von einem solchen Unternehmen erbracht werden, und für vernetzten Produkte für ein Jahr nach dem Zeitpunkt ihres Inverkehrbringens durch ein mittleres Unternehmen.

(40) Start-ups, kleine Unternehmen und Unternehmen, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/ als mittlere Unternehmen einzustufen sind, sowie Unternehmen aus traditionellen Branchen mit weniger entwickelten digitalen Fähigkeiten haben Schwierigkeiten, Zugang zu einschlägigen Daten zu erlangen. Ziel dieser Verordnung ist es, diesen Rechtsträgern den Zugang zu Daten zu erleichtern und gleichzeitig sicherzustellen, dass die entsprechenden Pflichten so verhältnismäßig wie möglich sind, um eine Übervorteilung zu vermeiden. Durch die Anhäufung und Aggregation gewaltiger Datenmengen und die technologische Infrastruktur für ihre Monetarisierung ist in der digitalen Wirtschaft gleichzeitig eine kleine Zahl sehr großer Unternehmen mit beträchtlicher wirtschaftlicher Macht entstanden. Zu diesen sehr großen Unternehmen gehören Betreiber zentraler Plattformdienste, 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 (26) zielt darauf ab, diese Ineffizienzen und Ungleichgewichte zu beheben, indem die Kommission ein Unternehmen als "Torwächter" benennen kann und diesen Torwächtern eine Reihe von Pflichten auferlegt wird, darunter das Verbot, bestimmte Daten ohne Einwilligung zusammenzuführen, und die Pflicht, wirksames Rechte auf Datenübertragbarkeit gemäß Artikel 20 der Verordnung (EU) 2016/679 zu gewährleisten. Gemäß der Verordnung (EU) 2022/1925 und angesichts der einzigartigen Fähigkeit dieser Unternehmen, Daten zu erwerben, ist es zur Erreichung des Ziels der vorliegenden Verordnung nicht erforderlich und somit in Bezug auf die den entsprechenden Pflichten unterliegenden Dateninhaber unverhältnismäßig, solchen Torwächtern ein Datenzugangsrecht einzuräumen. Ihre Einbeziehung dürfte auch die Vorteile einschränken, die die vorliegende Verordnung im Zusammenhang mit der gerechten Verteilung der Datenwertschöpfung unter den Marktteilnehmern für KMU bewirken kann. Dies bedeutet, dass ein als Torwächter

benanntes Unternehmen, das zentrale Plattformdienste betreibt, auf der Grundlage der vorliegenden Verordnung keinen Zugang zu Nutzerdaten verlangen oder erhalten kann, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes oder eines virtuellen Assistenten generiert werden. Darüber hinaus dürfen Dritte, denen Daten auf Verlangen des Nutzers bereitgestellt werden, die Daten keinem 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 Torwächter angeboten werden. Außerdem hindert es diese Unternehmen nicht daran, dieselben Daten auf andere rechtmäßige Weise zu erlangen und zu nutzen. Die Zugangsrechte gemäß der vorliegenden Verordnung tragen zu einer größeren Auswahl an Dienstleistungen für die Verbraucher bei. Da freiwillige Vereinbarungen zwischen Torwächtern und Dateninhabern hiervon unberührt bleiben, würde eine Beschränkung der Zugangsgewährung für Torwächter diese nicht vom Markt ausschließen oder daran hindern, ihre Dienste anzubieten.

(41) Angesicht des derzeitigen Stands der Technik wäre es zu aufwendig, Kleinstunternehmen und Kleinunternehmen weitere Konzeptionspflichten für vernetzte Produkte, die von ihnen hergestellt oder konzipiert, oder verbundene Dienste, die von ihnen erbracht werden, aufzuerlegen. Dies ist jedoch nicht der Fall, wenn ein Kleinstunternehmen oder Kleinunternehmen ein Partnerunternehmen oder ein verbundenes Unternehmen im Sinne von Artikel 3 des Anhangs der Empfehlung 2003/361/ hat, das nicht als Kleinstunternehmen oder Kleinunternehmen gilt, und das mit der Herstellung oder Konzeption eines vernetzten Produkts oder mit der Erbringung eines verbundenen Dienstes beauftragt wird. In solchen Fällen ist das Unternehmen, das einem Kleinstunternehmen oder Kleinunternehmen den Herstellungs- oder Konzeptionsauftrag erteilt hat, in der Lage, dem Auftragnehmer angemessenen zu entschädigen. Ein Kleinstunternehmen oder Kleinunternehmen kann jedoch als Dateninhaber den Anforderungen dieser Verordnung unterliegen, wenn es nicht der Hersteller des vernetzten Produkts oder ein Erbringer verbundener Dienste ist. Für ein Unternehmen, das seit weniger als einem Jahr als mittleres Unternehmen eingestuft ist, sowie für von einem mittleren Unternehmen vor weniger als einem Jahr auf den Markt gebrachte vernetzte Produkte sollte eine Übergangszeit gelten. Dieser Zeitraum von einem Jahr erlaubt es einem mittleren Unternehmen, sich anzupassen und vorzubereiten, bevor es auf dem Dienstleistungsmarkt für die von ihm hergestellten vernetzten Produkte auf Grundlage der Zugangsrechte gemäß dieser Verordnung dem Wettbewerb ausgesetzt ist. Diese Übergangszeit gilt nicht, wenn ein solches mittleres Unternehmen ein Partnerunternehmen oder ein verbundenes Unternehmen hat, das nicht als Kleinstunternehmen oder Kleinunternehmen gilt, oder wenn ein solches mittleres Unternehmen mit der Herstellung oder Konzeption eines vernetzten Produkts oder der Erbringung eines verbundenen Dienstes beauftragt wurde.

- (2) Vertragsklauseln, die zum Nachteil des Nutzers die Anwendung der Rechte des Nutzers nach diesem Kapitel ausschließen, davon abweichen oder die Wirkung dieser Rechte abändern, sind für den Nutzer nicht bindend.

## **Kapitel III Pflichten der Dateninhaber, die gemäss dem Unionsrecht verpflichtet sind, Daten bereitzustellen**

## **Artikel 8 Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen**

- (1) Ist im Rahmen von Geschäftsbeziehungen zwischen Unternehmen ein Dateninhaber nach Artikel 5 oder nach anderem anwendbarem Unionsrecht oder nach im Einklang mit dem Unionsrecht erlassenen nationalen Recht verpflichtet, einem Datenempfänger Daten bereitzustellen, so vereinbart er mit einem Datenempfänger die Ausgestaltung für die Bereitstellung der Daten und stellt diese zu fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise im Einklang mit dem vorliegenden Kapitel und dem Kapitel IV bereit.

(42) Unter Berücksichtigung der Vielzahl von vernetzten Produkten, mit denen hinsichtlich Art, Umfang und Häufigkeit unterschiedliche Daten generiert werden, die mit unterschiedlichen Daten- und Cybersicherheitsrisiken einhergehen und wirtschaftliche Chancen von unterschiedlichem Wert bieten, und um die Kohärenz der Verfahren für die Datenweitergabe im Binnenmarkt, auch sektorübergreifend, sicherzustellen und faire Verfahren für die Datenweitergabe selbst in jenen Bereichen zu fördern und voranzubringen, in denen ein solches Recht auf Datenzugang nicht vorgesehen ist, enthält diese Verordnung horizontale Vorschriften über die Ausgestaltung des Datenzugangs in all jenen Fällen, in denen ein Dateninhaber nach dem Unionsrecht oder nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, verpflichtet ist, einem Datenempfänger Daten bereitzustellen. Ein solcher Zugang sollte auf fairen, angemessenen, nichtdiskriminierenden und transparenten Bedingungen beruhen. Diese allgemeinen Zugangsvorschriften gelten nicht für Datenbereitstellungspflichten gemäß der Verordnung (EU) 2016/679. Die freiwillige Datenweitergabe bleibt von diesen Vorschriften unberührt. Die unverbindlichen Mustervertragsklauseln für die Datenweitergabe zwischen Unternehmen, die die Kommission erarbeiten und empfehlen wird, können den Parteien dabei helfen, Verträge zu schließen, die faire, angemessene und nichtdiskriminierende Bedingungen enthalten und in transparenter Weise umgesetzt werden sollen. Der Abschluss von Verträgen, die die unverbindlichen Mustervertragsklauseln beinhalten können, sollte nicht bedeuten, dass das Recht auf Weitergabe von Daten an Dritte in irgendeiner Weise an das Bestehen eines solchen Vertrags geknüpft ist. Sollten die Parteien – auch mit Unterstützung von Streitbeilegungsstellen – nicht in der Lage sein, einen Vertrag über die Datenweitergabe zu schließen, so ist das Recht, Daten an Dritte weiterzugeben, vor nationalen Gerichten einklagbar.

(45) In Vereinbarungen über die Bereitstellung von Daten, die im Rahmen der Geschäftsbeziehungen zwischen Unternehmen abgeschlossen werden, sollte unabhängig davon, ob es sich um große Unternehmen oder KMU handelt, nicht zwischen vergleichbaren Kategorien von Datenempfängern unterschieden werden. Zum Ausgleich des Mangels an Informationen über die in verschiedenen Verträgen enthaltenen Bedingungen, der es dem Datenempfänger erschwert, zu beurteilen, ob die Bedingungen für die Bereitstellung der Daten nichtdiskriminierend sind, sollte es in der Verantwortung der Dateninhaber liegen, nachzuweisen, dass eine Vertragsklausel nichtdiskriminierend ist. Es liegt keine rechtswidrige Diskriminierung vor, wenn der Dateninhaber für die Bereitstellung von Daten unterschiedliche Vertragsklauseln vorsieht, sofern diese Unterschiede aus objektiven Gründen gerechtfertigt sind. Diese Pflichten gelten unbeschadet der Verordnung (EU) 2016/679.

- (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 eine missbräuchliche Vertragsklausel im Sinne des Artikels

13 darstellt oder wenn sie zum Nachteil des Nutzers die Ausübung der Rechte des Nutzers nach Kapitel II ausschließt, davon abweicht oder deren Wirkung abändert.

- (3) Ein Dateninhaber darf in Bezug auf die Modalitäten der Bereitstellung von Daten nicht zwischen vergleichbaren Kategorien von Datenempfängern, einschließlich Partnerunternehmen oder verbundenen Unternehmen, diskriminieren. Ist ein Datenempfänger der Ansicht, dass die Bedingungen, unter denen ihm Daten bereitgestellt werden, diskriminierend sind, so stellt der Dateninhaber dem Datenempfänger auf dessen begründetes Ersuchen unverzüglich Informationen bereit, aus denen hervorgeht, dass keine Diskriminierung vorliegt.
- (4) Daten dürfen einem Datenempfänger vom Dateninhaber – auch exklusiv – nur dann bereitgestellt werden, wenn der Nutzer dies gemäß Kapitel II verlangt hat.
- (5) Dateninhaber und Datenempfänger müssen keine Informationen herausgeben, die über das hinausgehen, was erforderlich ist, um die Einhaltung der für die Datenbereitstellung vereinbarten Mustervertragsklauseln oder die Erfüllung ihrer Pflichten aus dieser Verordnung oder aus anderem anwendbaren Unionsrecht oder aus im Einklang mit Unionsrecht erlassenen nationalen Recht zu überprüfen.
- (6) Eine Pflicht, einem Datenempfänger Daten bereitzustellen, verpflichtet nicht zur Offenlegung von Geschäftsgeheimnissen, es sei denn, im Unionsrecht, einschließlich des Artikels 4 Absatz 6 und des Artikels 5 Absatz 9 der vorliegenden Verordnung, oder in im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften ist etwas anderes vorgesehen.

## **Artikel 9 Gegenleistung für die Bereitstellung von Daten**

(46) Um weitere Investitionen in die Generierung und Bereitstellung wertvoller Daten zu fördern, einschließlich Investitionen in einschlägige technische Instrumente, zugleich aber unverhältnismäßige Belastungen bei Datenzugang und Datennutzung zu vermeiden, da die Datenweitergabe dadurch wirtschaftlich nicht mehr tragfähig wäre, enthält diese Verordnung den Grundsatz, dass Dateninhaber eine angemessene Gegenleistung verlangen können, wenn sie gemäß Unionsrecht oder nationalem Recht, das im Einklang mit Unionsrecht erlassen wurde, verpflichtet sind, einem Datenempfänger im Rahmen von Geschäftsbeziehungen zwischen Unternehmen Daten bereitzustellen. Diese Gegenleistung sollte nicht als Bezahlung für die Daten selbst verstanden werden. Die Kommission sollte Leitlinien erlassen, anhand derer eine angemessene Gegenleistung in der Datenwirtschaft berechnet werden kann.

(47) Erstens kann eine angemessene Gegenleistung für die Erfüllung der Verpflichtung gemäß Unionsrecht oder nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, einem Datenzugangsverlangen nachzukommen, einen Ausgleich für die Kosten umfassen, die mit der Bereitstellung der Daten verbunden sind. Dies können technische Kosten sein, beispielsweise Kosten, die für die Wiedergabe, die elektronische Verbreitung und die Speicherung von Daten erforderlich sind, nicht aber die Kosten der Datensammlung oder -produktion. Die technischen Kosten könnten ferner die Kosten für die Verarbeitung umfassen, die im Vorfeld der Bereitstellung der Daten erforderlich ist, einschließlich der mit der Formatierung der Daten verbundenen Kosten. Kosten im Zusammenhang mit der Bereitstellung der Daten können auch die Kosten für die Erleichterung konkreter Datenweitergabeverlangen umfassen. In Abhängigkeit von der Datenmenge sowie von den für die Bereitstellung der Daten getroffenen Vereinbarungen können diese Kosten zudem unterschiedlich hoch ausfallen. Durch langfristige Vereinbarungen zwischen

Dateninhabern und Datenempfängern, z. B. über ein Abonnementmodell oder die Verwendung von intelligenten Verträgen, können die Kosten im Rahmen regelmäßiger oder wiederholter Transaktionen in einer Geschäftsbeziehung niedriger sein. Kosten im Zusammenhang mit der Bereitstellung von Daten beziehen sich entweder auf ein bestimmtes Verlangen oder decken mehrere Verlangen ab. Im letzteren Fall sollten die Kosten für die Bereitstellung der Daten nicht von einem einzelnen Datenempfänger in voller Höhe getragen werden. Zweitens kann die angemessene Gegenleistung auch eine Marge umfassen, außer in Bezug auf KMU und gemeinnützige Forschungseinrichtungen. Die Marge kann in Abhängigkeit von den Faktoren, die mit den Daten selbst im Zusammenhang stehen, etwa Menge, Format oder Art der Daten, unterschiedlich bemessen sein. Sie kann die Kosten für die Erhebung der Daten berücksichtigen. Daher kann die Marge geringer ausfallen, wenn der Dateninhaber die Daten für sein eigenes Unternehmen erhoben hat, ohne wesentliche Investitionen zu tätigen, oder aber höher ausfallen, wenn in die Datenerhebung für die Zwecke des Unternehmens des Dateninhabers stark investiert werden muss. In Fällen, in denen sich die Nutzung der Daten durch den Datenempfänger nicht auf die eigenen Tätigkeiten des Dateninhabers auswirkt, kann die Marge begrenzt oder sogar ausgeschlossen werden. Außerdem könnte die Gegenleistung dadurch, dass die Daten von einem vernetzten Produkt, das Eigentum des Nutzers ist oder von ihm gemietet oder geleast wird, mitgeneriert werden, vergleichsweise niedriger ausfallen als in anderen Fällen, in denen die Daten, etwa bei der Erbringung eines verbundenen Dienstes, vom Dateninhaber generiert werden.

(48) Ein Eingreifen ist nicht erforderlich, wenn Daten zwischen großen Unternehmen weitergegeben werden oder wenn es sich beim Dateninhaber um ein kleines oder mittleres Unternehmen und beim Datenempfänger um ein großes Unternehmen handelt. In diesen Fällen wird davon ausgegangen, dass die Unternehmen in der Lage sind, innerhalb angemessener und nichtdiskriminierender Grenzen eine Gegenleistung auszuhandeln.

- (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, und darf eine Marge enthalten.
- (2) Bei der Einigung auf eine Gegenleistung berücksichtigen der Dateninhaber und der Datenempfänger insbesondere Folgendes:
  - a) angefallene Kosten für die Bereitstellung der Daten, einschließlich insbesondere der notwendigen Kosten für die Formatierung der Daten, die Verbreitung auf elektronischem Wege und die Speicherung;
  - b) gegebenenfalls Investitionen in die Erhebung und Generierung von Daten, wobei berücksichtigt wird, ob andere Parteien zur Beschaffung, Generierung oder Erhebung der betreffenden Daten beigetragen haben.
- (3) Die in Absatz 1 genannte Gegenleistung kann auch von Umfang, Format und Art der Daten abhängen.
- (4) Ist der Datenempfänger ein KMU oder eine gemeinnützige Forschungseinrichtung und hat der betreffende Datenempfänger keine Partnerunternehmen oder verbundenen Unternehmen, die nicht als KMU gelten, so darf eine Gegenleistung die in Absatz 2 Buchstabe a aufgeführten Kosten nicht übersteigen.

(49) Um KMU vor übermäßigen wirtschaftlichen Belastungen zu schützen, die ihnen die Entwicklung und den Betrieb innovativer Geschäftsmodelle übermäßig erschweren würden, sollte die von ihnen zu tragende angemessene Gegenleistung für die Be-

reistellung von Daten die mit der Bereitstellung der Daten direkt verbundenen Kosten nicht übersteigen. Mit der Bereitstellung direkt verbundene Kosten sind jene Kosten, die den einzelnen Datenzugangsverlangen zuzurechnen sind, wobei zu berücksichtigen ist, dass der Dateninhaber die erforderlichen technischen Schnittstellen oder die erforderliche Software und Netzanbindung dauerhaft einzurichten hat. Dieselbe Regelung sollte für gemeinnützige Forschungseinrichtungen gelten.

- (5) Die Kommission erlässt Leitlinien für die Berechnung einer angemessenen Gegenleistung unter Berücksichtigung des Rates des in Artikel 42 genannten Europäischen Dateninnovationsrates (EDIB).
- (6) Dieser Artikel steht dem nicht entgegen, dass Unionsrecht oder im Einklang mit Unionsrecht erlassene nationale Rechtsvorschriften eine Gegenleistung für die Bereitstellung von Daten ausschließen oder eine geringere Gegenleistung vorsehen.
- (7) Der Dateninhaber stellt dem Datenempfänger Informationen bereit, in denen die Grundlage für die Berechnung der Gegenleistung so detailliert dargelegt ist, dass der Datenempfänger beurteilen kann, ob die Anforderungen der Absätze 1 bis 4 erfüllt sind.

(51) 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 oder eine gemeinnützige Forschungseinrichtung handelt, dass die Gegenleistung nicht die Kosten übersteigt, die direkt mit der Bereitstellung der Daten für den Datenempfänger verbunden und jeweils dem einzelnen Verlangen zuzurechnen sind. Damit 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 bereitstellen.

## **Artikel 10 Streitbeilegung**

(52) 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 Datenweitergabe gestärkt wird. Falls 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. Während in dieser Verordnung nur die Bedingungen festgelegt sind, die Streitbeilegungsstellen erfüllen müssen, um zertifiziert zu werden, steht es den Mitgliedstaaten frei, spezifische Vorschriften für das Zertifizierungsverfahren, einschließlich des Ablaufs oder des Widerrufs der Zertifizierung, zu erlassen. Die in dieser Verordnung enthaltenen Bestimmungen über die Streitbeilegung sollten die Mitgliedstaaten nicht dazu verpflichten, Streitbeilegungsstellen einzurichten.

(55) Um die einheitliche Anwendung dieser Verordnung zu gewährleisten, sollten die Streitbeilegungsstellen die von der Kommission zu entwickelnden und zu empfehlenden unverbindlichen Mustervertragsklauseln sowie Unionsrecht oder nationales Recht zur Festlegung der Verpflichtungen zur Weitergabe von Daten oder Leitlinien der einschlägigen Fachbehörden für die Anwendung dieses Rechts berücksichtigen.

- (1) Nutzer, Dateninhaber und Datenempfänger haben Zugang zu einer gemäß Absatz 5 des vorliegenden Artikels zertifizierten Streitbeilegungsstelle für die Beilegung von Streitigkeiten nach Artikel 4 Absatz 3 und Absatz 9 und Artikel 5 Absatz 12 sowie

Streitigkeiten im Zusammenhang mit den fairen, angemessenen und nichtdiskriminierenden Bedingungen für die Bereitstellung von Daten und die transparente Art und Weise der Bereitstellung von Daten gemäß dem vorliegenden Kapitel und Kapitel IV.

(53) Das Streitbelegungsverfahren im Rahmen dieser Verordnung ist ein freiwilliges Verfahren, das es Nutzern, Dateninhabern und Datenempfängern ermöglicht, zu vereinbaren, Streitbelegungsstellen mit ihren Streitigkeiten zu befragen. Daher sollte es den Parteien freistehen, sich an eine Streitbelegungsstelle ihrer Wahl zu wenden, sei es innerhalb oder außerhalb der Mitgliedstaaten, in denen diese Parteien niedergelassen sind.

- (2) Die Streitbelegungsstellen teilen den betroffenen Parteien die Entgelte oder die zur Festsetzung der Entgelte verwendeten Methoden mit, bevor diese Parteien eine Entscheidung beantragen.
- (3) Bei Streitigkeiten, die einer Streitbelegungsstelle nach Artikel 4 Absatz 3 zugewiesen wurden, gilt, wenn die Streitbelegungsstelle eine Streitigkeit zugunsten des Nutzers oder Datenempfängers entscheidet, dass der Dateninhaber alle von der Streitbelegungsstelle erhobenen Gebühren trägt und dem betreffenden Nutzer oder Datenempfänger alle sonstigen angemessenen Ausgaben, die diesem im Zusammenhang mit der Streitbelegung entstanden sind, erstattet. Entscheidet die Streitbelegungsstelle eine Streitigkeit zugunsten des Dateninhabers, so ist der Nutzer oder der Datenempfänger nicht verpflichtet, Gebühren oder sonstige Kosten zu erstatten, die der Dateninhaber im Zusammenhang mit der Streitbelegung gezahlt hat oder zu zahlen hat, es sei denn, die Streitbelegungsstelle stellt fest, dass der Nutzer oder der Datenempfänger offensichtlich bösgläubig gehandelt hat.
- (4) Kunden und Anbieter von Datenverarbeitungsdiensten haben Zugang zu einer Streitbelegungsstelle, die gemäß Absatz 5 des vorliegenden Artikels zugelassen ist, um Streitigkeiten im Zusammenhang mit Verletzungen der Rechte der Kunden und der Pflichten der Anbieter von Datenverarbeitungsdiensten entsprechend Artikeln 23 bis 31 beizulegen.
- (5) Der Mitgliedstaat, in dem die Streitbelegungsstelle niedergelassen ist, lässt diese Stelle auf deren Antrag hin zu, nachdem sie nachgewiesen hat, dass sie alle folgenden Bedingungen erfüllt:
  - a) Sie ist unparteiisch und unabhängig und trifft ihre Entscheidungen nach klaren, diskriminierungsfreien und fairen Verfahrensregeln;
  - b) sie verfügt über das erforderliche Fachwissen, insbesondere in Bezug auf faire, angemessene und nichtdiskriminierende Bedingungen, einschließlich Gegenleistungen, über die transparente Bereitstellung von Daten, die es ihr ermöglicht, diese Bedingungen effektiv festzulegen;
  - c) sie ist über elektronische Kommunikationsmittel leicht erreichbar;
  - d) sie ist in der Lage, ihre Entscheidungen rasch, effizient und kostengünstig in mindestens einer Amtssprache der Union zu erlassen.
- (6) Die Mitgliedstaaten teilen der Kommission die nach Absatz 5 zugelassenen Streitbelegungsstellen mit. Die Kommission veröffentlicht auf einer eigens hierfür eingerichteten Website eine Liste dieser Stellen und hält diese auf dem neuesten Stand.

(7) Eine Streitbelegungsstelle verweigert die Bearbeitung eines Streitbelegungsantrags, der bereits bei einer anderen Streitbelegungsstelle oder einem Gericht eines Mitgliedstaats eingereicht wurde.

(54) Um zu vermeiden, dass – insbesondere in einer grenzüberschreitenden Situation – zwei oder mehr Streitbelegungsstellen mit derselben Streitigkeit befasst werden, sollte ein Ersuchen zur Streitbelegung von einer Streitbelegungsstelle abgelehnt werden können, wenn es bereits bei einer anderen Streitbelegungsstelle oder einem Gericht eines Mitgliedstaats eingereicht wurde.

(8) Eine Streitbelegungsstelle bietet den Parteien die Möglichkeit, sich innerhalb einer angemessenen Frist zu den Angelegenheiten zu äußern, in denen sich diese Parteien an die betreffende Stelle gewandt haben. In diesem Zusammenhang werden jeder Partei die Schriftsätze der anderen Partei und etwaige Erklärungen von Sachverständigen bereitgestellt. Den Parteien wird die Möglichkeit geboten, zu diesen Schriftsätzen und Erklärungen Stellung zu nehmen.

(9) Eine Streitbelegungsstelle entscheidet in einer Angelegenheit, die ihr vorgelegt wird, spätestens 90 Tage nach Erhalt eines Antrags gemäß den Absätzen 1 bis 4. Diese Entscheidung erfolgt schriftlich oder auf einem dauerhaften Datenträger und wird mit einer Begründung versehen.

(10) Die Streitbelegungsstellen erstellen und veröffentlichen jährliche Tätigkeitsberichte. Diese Jahresberichte müssen insbesondere die folgenden allgemeinen Angaben umfassen:

- a) eine Zusammenstellung der Ergebnisse von Streitigkeiten;
- b) den durchschnittlichen Zeitaufwand für die Lösung von Streitigkeiten;
- c) die häufigsten Gründe für Streitigkeiten.

(11) Um den Austausch von Informationen und bewährten Verfahren zu erleichtern, kann eine Streitbelegungsstelle beschließen, in den in Absatz 10 genannten Bericht Empfehlungen dazu aufzunehmen, wie Probleme zu vermeiden oder zu beheben sind.

(12) Die Entscheidung einer Streitbelegungsstelle ist für die Parteien nur dann bindend, wenn die Parteien vor Beginn des Streitbelegungsverfahrens dem bindenden Charakter ausdrücklich zugestimmt haben.

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

(56) Die Parteien eines Streitbelegungsverfahrens sollten nicht daran gehindert werden, ihre Grundrechte auf einen wirksamen Rechtsbehelf und ein faires Verfahren auszuüben. Daher sollte die Entscheidung, eine Streitbelegungsstelle mit einer Streitigkeit zu beauftragen, diesen Parteien nicht das Recht nehmen, bei einem Gericht eines Mitgliedstaats Rechtsmittel einzulegen. Die Streitbelegungsstellen sollten jährliche Tätigkeitsberichte öffentlich verfügbar machen.

## Artikel 11 Technische Schutzmaßnahmen über die unbefugte Nutzung oder Offenlegung von Daten

- (1) Ein Dateninhaber kann geeignete technische Schutzmaßnahmen, einschließlich intelligenter Verträge und Verschlüsselung, anwenden, um den unbefugten Zugang zu Daten, einschließlich Metadaten, zu verhindern und die Einhaltung der Artikel 5, 6, 8 und 9 sowie der für die Datenbereitstellung vereinbarten Mustervertragsklauseln sicherzustellen. Bei solchen technischen Schutzmaßnahmen dürfen weder Datenempfänger unterschiedlich behandelt werden noch dürfen Nutzer an der Ausübung ihres Rechts, eine Kopie der Daten zu erhalten, Daten abzurufen, zu verwenden oder auf diese zuzugreifen oder Dritten nach Artikel 5 Daten bereitzustellen, oder Dritte an der Ausübung ihrer Rechte nach dem Unionsrecht oder den nationalen Rechtsvorschriften, die im Einklang mit dem Unionsrecht angenommen wurden, gehindert werden. Nutzer, Dritte und Datenempfänger dürfen solche technischen Schutzmaßnahmen nur ändern oder aufheben, wenn der Dateninhaber dem zugestimmt hat.
- (2) Unter den in Absatz 3 genannten Umständen kommt der Dritte oder der Datenempfänger den Aufforderungen des Dateninhabers und gegebenenfalls des Inhabers des Geschäftsgeheimnisses – wenn es sich nicht um dieselbe Person handelt – oder des Nutzers unverzüglich nach:
  - a) die vom Dateninhaber bereitgestellten Daten und alle etwaigen Kopien davon zu 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 einzustellen und alle rechtsverletzenden Waren zu vernichten, wenn die ernsthafte Gefahr besteht, dass die unrechtmäßige Verwendung dieser Daten dem Dateninhaber, dem Inhaber des Geschäftsgeheimnisses oder dem Nutzer einen erheblichen Schaden zufügt, bzw. sofern eine solche Maßnahme im Hinblick auf die Interessen des Dateninhabers, des Inhabers des Geschäftsgeheimnisses oder des Nutzers nicht unverhältnismäßig wäre;
  - c) den Nutzer über die unbefugte Nutzung oder Offenlegung der Daten und über die Maßnahmen, die ergriffen wurden, um die unbefugte Nutzung oder Offenlegung der Daten zu unterbinden, zu unterrichten;
  - d) die Partei, die durch den Missbrauch oder die Offenlegung dieser unrechtmäßig abgerufenen oder genutzten Daten geschädigt wurde, zu entschädigen.
- (3) Absatz 2 findet Anwendung, wenn ein Dritter oder ein Datenempfänger
  - a) zwecks Erlangung der Daten einem Dateninhaber falsche Informationen gegeben, Täuschungs- oder Zwangsmittel eingesetzt oder Lücken in der zum Schutz der Daten bestehenden technischen Infrastruktur der Daten missbraucht hat,
  - b) die bereitgestellten Daten für nicht genehmigte Zwecke, einschließlich der Entwicklung eines konkurrierenden vernetzten Produkts im Sinne von Artikel 6 Absatz 2 Buchstabe e, genutzt hat,
  - c) unrechtmäßig Daten an eine andere Partei weitergegeben hat,

- d) die gemäß Artikel 5 Absatz 9 vereinbarten technischen und organisatorischen Maßnahmen nicht aufrechterhalten hat oder
  - e) die vom Dateninhaber gemäß Absatz 1 des vorliegenden Artikels angewandten technischen Schutzmaßnahmen ohne Zustimmung des Dateninhabers verändert oder aufgehoben hat.
- (4) Absatz 2 gilt ebenfalls, wenn ein Nutzer die vom Dateninhaber angewandten technischen Schutzmaßnahmen ändert oder aufhebt oder die vom Nutzer im Einvernehmen mit dem Dateninhaber oder, wenn sie nicht dieselbe Person sind, dem Inhaber des Geschäftsgeheimnisses getroffenen technischen und organisatorischen Maßnahmen zur Wahrung von Geschäftsgeheimnissen nicht aufrechterhält, sowie für jede andere Partei, die die Daten von dem Nutzer unter Verstoß gegen diese Verordnung erhält.
- (5) Hat der Datenempfänger gegen Artikel 6 Absatz 2 Buchstabe a oder b verstoßen, so haben die Nutzer dieselben Rechte wie Dateninhaber gemäß Absatz 2 des vorliegenden Artikels.

### **Artikel 12 Umfang der Pflichten der Dateninhaber, die nach dem Unionsrecht verpflichtet sind, Daten bereitzustellen**

- (1) Dieses Kapitel gilt, wenn ein Dateninhaber im Rahmen von Geschäftsbeziehungen zwischen Unternehmen nach Artikel 5 oder nach geltendem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften verpflichtet ist, einem Datenempfänger Daten bereitzustellen.
- (2) Eine Vertragsklausel in einer Datenweitergabevereinbarung, die zum Nachteil einer Partei oder gegebenenfalls zum Nachteil des Nutzers die Anwendung dieses Kapitels ausschließt, davon abweicht oder seine Wirkung abändert, ist für diese Partei nicht bindend.

## **Kapitel IV Missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen**

### **Artikel 13 Missbräuchliche Vertragsklauseln, die einem anderen Unternehmen einseitig auferlegt werden**

(28) Bei Verträgen zwischen einem Dateninhaber und einem Verbraucher als Nutzer eines vernetzten Produkts oder verbundenen Dienstes, das bzw. der Daten generiert, gilt das Verbraucherrecht der Union, insbesondere die Richtlinien 93/13/EWG und 2005/29/, damit ein Verbraucher keinen missbräuchlichen Vertragsklauseln unterliegt. Für die Zwecke dieser Verordnung sollten missbräuchliche Vertragsklauseln, die einem Unternehmen einseitig auferlegt werden, für das betreffende Unternehmen nicht verbindlich sein.

(43) Auf der Grundlage des Grundsatzes der Vertragsfreiheit sollte es den Parteien freistehen, in ihren Verträgen im Rahmen der allgemeinen Zugangsvorschriften für die Bereitstellung von Daten die genauen Bedingungen für die Bereitstellung von Daten auszuhandeln. Die Bedingungen solcher Verträge könnten sich auch auf technische und organisatorische Maßnahmen, auch in Bezug auf die Datensicherheit, erstrecken.

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

(58) 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 könnte, mit dem Ergebnis, dass der Zugang zu Daten wirtschaftlich weniger tragfähig und bisweilen untragbar ist. Solche vertraglichen Ungleichgewichte schaden allen Unternehmen, die nicht wirklich in der Lage sind, die Bedingungen für den Zugang zu Daten auszuhandeln, und die unter Umständen keine andere Wahl haben, als nicht verhandelbare Vertragsklauseln 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 Unternehmen nicht bindend sein, wenn diese Bedingungen diesen Unternehmen einseitig auferlegt wurden.

**(1) Vertragsklauseln 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, sind für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich sind.**

(59) Bei den Vorschriften über Vertragsklauseln sollte der Grundsatz der Vertragsfreiheit als wesentliches Konzept in den Geschäftsbeziehungen zwischen Unternehmen berücksichtigt werden. Daher sollten nicht alle Vertragsklauseln einer Missbräuchlichkeitsprüfung unterzogen werden, sondern nur jene Klauseln, die einseitig auferlegt 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. Vertragsklauseln, die lediglich von einer Partei eingebracht und von dem anderen Unternehmen akzeptiert werden, oder Klauseln, die zwischen den Vertragsparteien ausgehandelt und anschließend in geänderter Form vereinbart werden, sollten nicht als einseitig auferlegt gelten.

(60) 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.

(61) Kriterien für die Ermittlung missbräuchlicher Vertragsklauseln sollten nur auf überzogene Vertragsklauseln angewandt werden, bei denen eine stärkere Verhandlungsposition missbraucht wurde. Die überwiegende Mehrheit der Vertragsklauseln, 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. Für die Zwecke dieser Verordnung würde eine grobe Abweichung von der guten Geschäftspraxis unter anderem bedeuten, dass die Partei, der die Bedingung einseitig auferlegt wurde, in

ihrer Fähigkeit, ihr berechtigtes geschäftliches Interesse an den betreffenden Daten zu schützen, objektiv beeinträchtigt wird.

- (2) Wenn Vertragsklauseln zwingenden Bestimmungen des Unionsrechts oder bei Fehlen von Vertragsklauseln zur Regelung der Angelegenheit geltenden Bestimmungen des Unionsrechts entsprechen, gelten sie nicht als missbräuchlich.
- (3) Vertragsklauseln sind missbräuchlich, wenn ihre Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt.
- (4) Eine Vertragsklausel gilt insbesondere dann als missbräuchlich im Sinne des Absatzes 3, wenn sie Folgendes bezweckt oder bewirkt:

(62) Um für Rechtssicherheit zu sorgen, wird in dieser Verordnung eine Liste von Klauseln festgelegt, die stets als missbräuchlich gelten und eine Liste von Klauseln, bei denen davon ausgegangen wird, dass sie missbräuchlich sind. Im letzteren Fall sollte das Unternehmen, das die Vertragsklausel vorschreibt, in der Lage sein, die Vermutung der Missbräuchlichkeit zu widerlegen, indem es nachweist, dass eine in dieser Verordnung aufgeführte Vertragsklausel im konkreten Fall nicht missbräuchlich ist. Ist eine Vertragsklausel 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 in dieser Verordnung als missbräuchlich aufgeführten Vertragsklauseln als Maßstab für die Auslegung der allgemeinen Missbräuchlichkeitsbestimmung dienen. Schließlich können von der Kommission erstellte und empfohlene unverbindliche Mustervertragsklauseln für Verträge über die Datenweitergabe zwischen Unternehmen für Wirtschaftsunternehmen auch bei der Aushandlung von Verträgen hilfreich sein. Wird eine Vertragsklausel für missbräuchlich erklärt, so sollte der betreffende Vertrag ohne diese Klausel weiterhin gelten, es sei denn, die missbräuchliche Klausel ist nicht von den übrigen Vertragsklauseln abtrennbar.

- 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 dieser Pflichten;
  - c) das ausschließliche Recht der Partei, die die Klausel einseitig auferlegt hat, zu bestimmen, ob die gelieferten Daten vertragsgemäß sind, oder Vertragsklauseln auszulegen.
- (5) Eine Vertragsklausel gilt als missbräuchlich im Sinne des Absatzes 3, wenn sie Folgendes bezweckt oder bewirkt:
    - a) eine unangemessene Beschränkung der Rechtsmittel bei Nichterfüllung von Vertragspflichten oder der Haftung bei einer Verletzung dieser Pflichten oder eine Erweiterung der Haftung des Unternehmens, dem die Klausel einseitig auferlegt wurde;
    - b) das 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, insbesondere, wenn

diese Daten sensible Geschäftsdaten enthalten oder durch das Geschäftsgeheimnis oder durch Rechte des geistigen Eigentums geschützt sind;

- c) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, die von ihr während der Vertragslaufzeit bereitgestellten oder generierten Daten zu nutzen, oder eine Beschränkung der Nutzung dieser Daten insofern, als diese Partei nicht berechtigt ist, diese Daten in angemessener Weise zu nutzen, zu erfassen, darauf zuzugreifen oder sie zu kontrollieren oder zu verwerten;
- d) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, die Vereinbarung innerhalb einer angemessenen Frist zu kündigen;
- e) die Hinderung der Partei, der die Klausel einseitig auferlegt wurde, daran, während der Vertragslaufzeit oder innerhalb einer angemessenen Frist nach Kündigung des Vertrags eine Kopie der von ihr bereitgestellten oder generierten Daten zu erhalten;
- f) die Möglichkeit, dass die Partei, die die Klausel einseitig auferlegt hat, den Vertrag mit unangemessen kurzer Frist kündigen darf, und zwar unter Berücksichtigung jeglicher realistischer Möglichkeit für die andere Vertragspartei, zu einem anderen, vergleichbaren Dienst zu wechseln, und des durch die Kündigung verursachten finanziellen Nachteils, außer bei Vorliegen schwerwiegender Gründe;
- g) die Möglichkeit, dass die Partei, die die Klausel einseitig auferlegt hat, den vertraglich vereinbarten Preis oder eine andere wesentliche Bedingung in Bezug auf Art, Format, Qualität oder Menge der weiterzugebenden Daten ohne eine im Vertrag spezifizierte stichhaltige Begründung wesentlich abändert, ohne dass der anderen Partei das Recht eingeräumt wird, den Vertrag im Falle einer solchen Abänderung zu kündigen.

Unterabsatz 1 Buchstabe g berührt nicht Klauseln, nach denen sich die Partei, die die Klausel einseitig auferlegt hat, das Recht vorbehält, die Bedingungen eines unbefristeten Vertrags einseitig zu ändern, sofern eine in diesem Vertrag spezifizierte stichhaltige Begründung vorliegt, wonach die Partei, die die Klausel einseitig auferlegt hat, verpflichtet ist, die andere Vertragspartei innerhalb einer angemessenen Frist von solch einer beabsichtigten Änderung in Kenntnis zu setzen, und es der anderen Vertragspartei freisteht, den Vertrag im Falle einer solchen Änderung unentgeltlich zu kündigen.

- (6) Vertragsklauseln gelten im Sinne dieses Artikels als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht werden und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann. Die Vertragspartei, die die Vertragsklausel eingebracht hat, trägt die Beweislast dafür, dass diese Klausel nicht einseitig auferlegt wurde. Die Vertragspartei, die die beanstandete Klausel eingebracht hat, kann sich nicht darauf berufen, dass es sich um eine missbräuchliche Vertragsklausel handelt.
- (7) Ist die missbräuchliche Vertragsklausel von den übrigen Bedingungen des Vertrags abtrennbar, so bleiben die übrigen Vertragsklauseln bindend.
- (8) Dieser Artikel gilt weder für Vertragsklauseln, in denen der Hauptgegenstand des Vertrags festgelegt wird, noch für die Angemessenheit des Preises für die als Gegenleistung weitergegebenen Daten.

- (9) Die Parteien eines unter Absatz 1 fallenden Vertrags dürfen die Anwendung dieses Artikels nicht ausschließen, nicht davon abweichen und dessen Wirkungen nicht abändern.

## **Kapitel V Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen aussergewöhnlicher Notwendigkeit**

(63) Im Falle außergewöhnlicher Notwendigkeit kann es erforderlich sein, dass öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union bei der Wahrnehmung ihrer gesetzlichen Pflichten im öffentlichen Interesse vorhandene Daten, gegebenenfalls einschließlich beigefügter Metadaten, die von einem Unternehmen gehalten werden, nutzen, um auf öffentliche Notlagen oder andere Ausnahmesituationen zu reagieren. Unter einer außergewöhnlichen Notwendigkeit sind – im Gegensatz zu sonstigen Umständen, die möglicherweise geplant oder terminiert sind oder regelmäßig oder häufig eintreten, – Umstände zu verstehen, die nicht vorhersehbar und zeitlich begrenzt sind. Während der Begriff “Dateninhaber” öffentliche Stellen im Allgemeinen nicht einschließt, kann er öffentliche Unternehmen umfassen. Forschungseinrichtungen und Forschungsförderungseinrichtungen könnten auch als öffentliche Stellen oder Einrichtungen des öffentlichen Rechts eingerichtet sein. Um die Belastung der Unternehmen zu begrenzen, sollten Kleinstunternehmen und Kleinunternehmen nur dann verpflichtet sein, öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union Daten bereitzustellen, wenn solche Daten in Fällen außergewöhnlicher Notwendigkeit erforderlich sind, um auf einen öffentlichen Notstand zu reagieren und öffentliche Stellen, die Kommission, die Europäische Zentralbank oder die Einrichtungen der Union solche Daten unter gleichwertigen Bedingungen auf andere Weise nicht rechtzeitig und wirksam beschaffen können.

### **Artikel 14 Pflicht zur Bereitstellung von Daten wegen außergewöhnlicher Notwendigkeit**

Wenn eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union den Nachweis dafür erbringt, dass im Hinblick auf die Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse die außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen betreffenden Metadaten – gemäß Artikel 15 besteht, stellen die Dateninhaber, bei denen sich diese Daten befinden und bei denen es sich um andere juristische Personen als öffentliche Stellen handelt, diese Daten auf ordnungsgemäß begründeten Antrag bereit.

(64) Bei öffentlichen Notständen wie Notlagen im Bereich der öffentlichen Gesundheit, Notlagen aufgrund von Naturkatastrophen, einschließlich solcher, die durch den Klimawandel und die Umweltzerstörung noch verschärft werden, sowie von Menschen verursachter schwerer Katastrophen, wie großen Cybersicherheitsvorfällen, wird das öffentliche

Interesse an der Verwendung der Daten schwerer wiegen als das Interesse der Dateninhaber, frei über die von ihnen gehaltenen Daten zu verfügen. In einem solchen Fall sollten die Dateninhaber verpflichtet werden, die Daten öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union auf deren Verlangen bereitzustellen. Das Vorliegen eines öffentlichen Notstands sollte in Übereinstimmung mit dem Unionsrecht oder nationalen Recht und auf der Grundlage der jeweils einschlägigen Verfahren, einschließlich der Verfahren der einschlägigen internationalen Organisationen festgestellt oder erklärt werden. In solchen Fällen sollte die öffentliche Stelle nachweisen, dass die Daten, die Gegenstand des Verlangens sind, nicht auf andere Weise rechtzeitig und wirksam und unter gleichwertigen Bedingungen erlangt werden konnten, beispielsweise durch die freiwillige Bereitstellung von Daten durch ein anderes Unternehmen oder Abfragen einer öffentlichen Datenbank.

## **Artikel 15 Außergewöhnliche Notwendigkeit der Datennutzung**

(65) Eine außergewöhnliche Notwendigkeit kann sich auch aus Situationen ergeben, die keinen Notstand darstellen. In solchen Fällen sollte es einer öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union nur gestattet sein, nicht-personenbezogene Daten zu verlangen. Die öffentliche Stelle sollte nachweisen, dass die Daten erforderlich sind, um eine bestimmte Aufgabe im öffentlichen Interesse zu erfüllen, die gesetzlich ausdrücklich vorgesehen ist, etwa die Erstellung amtlicher Statistiken oder die Eindämmung oder Überwindung eines öffentlichen Notstands. Darüber hinaus kann ein solches Verlangen nur gestellt werden, wenn die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union spezifische Daten ermittelt hat, die sie auf andere Weise nicht rechtzeitig und wirksam und unter gleichwertigen Bedingungen erlangen könnte, und nur, wenn sie alle anderen zur Verfügung stehenden Mittel ausgeschöpft hat, um diese Daten zu erlangen, wie etwa die Beschaffung der Daten über freiwillige Vereinbarungen, einschließlich des Erwerbs von nicht-personenbezogenen Daten auf dem Markt, wobei der jeweilige Marktkurs geboten wird, oder durch Rückgriff auf bestehende Verpflichtungen zur Bereitstellung von Daten oder den Erlass neuer Rechtsvorschriften, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnten. Ferner sollten die Bedingungen und Grundsätze für Verlangen etwa in Bezug auf Zweckbindung, Verhältnismäßigkeit, Transparenz und Befristung gelten. Werden Daten verlangt, die für die Erstellung amtlicher Statistiken erforderlich sind, so sollte die anfragende öffentliche Stelle auch nachweisen, ob sie nach nationalem Recht befugt ist, nicht-personenbezogene Daten auf dem Markt zu erwerben.

- (1)** Die außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten im Sinne dieses Kapitels ist zeitlich befristet und im Umfang begrenzt und gilt nur unter einem der folgenden Umstände als gegeben, wenn:
  - a)* die verlangten Daten zur Bewältigung eines öffentlichen Notstands erforderlich sind und die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union diese Daten unter gleichwertigen Bedingungen auf andere Weise nicht rechtzeitig und wirksam beschaffen kann;
  - b)* nicht von Buchstabe a erfassten Umstände vorliegen, und nur soweit nicht-personenbezogene Daten betroffen sind, wenn
    - (i)* eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union auf der Grundlage des Unionsrechts oder des nationalen Rechts tätig wird und spezifische Daten ermittelt hat, deren Fehlen sie daran hindert, eine bestimmte im öffentlichen Interesse ausgeübte

Aufgabe zu erfüllen, die rechtlich ausdrücklich vorgesehen ist, wie etwa amtliche Statistiken zu erstellen oder einen öffentlichen Notstand einzudämmen oder zu überwinden, und

- (ii) die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union alle anderen ihr zur Verfügung stehenden Mittel ausgeschöpft hat, um solche Daten zu erlangen, darunter der Erwerb von nicht-personenbezogenen Daten auf dem Markt durch Angebot von Markttarifen oder die Inanspruchnahme bestehender Verpflichtungen zur Bereitstellung von Daten oder der Erlass neuer Rechtsvorschriften, die die rechtzeitige Verfügbarkeit der Daten gewährleisten könnten.
- (2) Absatz 1 Buchstabe b dieses Artikels gilt nicht für Kleinunternehmen und Kleinstunternehmen.
- (3) Die Verpflichtung, nachzuweisen, dass die öffentliche Stelle nicht in der Lage war, nicht-personenbezogene Daten durch den Erwerb auf dem Markt zu erhalten, gilt nicht, wenn die spezifische Aufgabe, die im öffentlichen Interesse ausgeübt wird, in der Erstellung amtlicher Statistiken besteht und der Erwerb solcher Daten nach nationalem Recht nicht zulässig ist.

### **Artikel 16 Verhältnis zu anderen Pflichten zur Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union**

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

(66) Diese Verordnung sollte weder für freiwillige Vereinbarungen über den Datenaustausch zwischen privaten und öffentlichen Stellen, einschließlich der Bereitstellung von Daten durch KMU, gelten noch diesen vorgehen, und sie lässt Rechtsakte der Union unberührt, die verbindliche Auskunftersuchen öffentlicher Stellen an private Einrichtungen vorsehen. Die den Dateninhabern auferlegten Pflichten zur Bereitstellung von Daten, die nicht auf einer außergewöhnlichen Notwendigkeit beruhen, insbesondere wenn die Datengrundlage und die Dateninhaber bekannt sind oder die Daten regelmäßig genutzt werden können, wie im Falle von Berichtspflichten und sich aus dem Binnenmarkt ergebenden Pflichten, sollten von dieser Verordnung nicht berührt werden. Datenzugangsanforderungen, die dazu dienen, die Einhaltung der geltenden Vorschriften zu überprüfen, sollten von dieser Verordnung ebenfalls nicht berührt werden, auch in Fällen, in denen öffentliche Stellen die Aufgabe der Überprüfung der Einhaltung der Vorschriften anderen als öffentlichen Stellen übertragen.

- (2) Dieses Kapitel gilt nicht für öffentliche Stellen, die Kommission, die Europäische Zentralbank und die Einrichtungen der Union, die Tätigkeiten zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung durchführen, oder für die Zoll- oder Steuerverwaltung. Dieses Kapitel berührt nicht das anwendbare Unionsrecht und das anwendbare nationale Recht 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.

(68) Bei der Wahrnehmung ihrer Aufgaben in den Bereichen Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Vollstreckung strafrechtlicher und verwaltungsrechtlicher Sanktionen sowie der Erhebung von Daten für Steuer- oder Zollzwecke sollten sich öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union auf ihre Befugnisse im Rahmen des Unionsrechts oder des nationalen Rechts stützen. Diese Verordnung berührt daher nicht die Gesetzgebungsakte für die Datenweitergabe, den Datenzugang und die Datennutzung in diesen Bereichen.

## Artikel 17 Datenbereitstellungsverlangen

- (1) Öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union müssen in ihren Datenverlangen nach Artikel 14
- a) angeben, welche Daten, einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten, benötigt werden;
  - b) nachweisen, dass die für das Bestehen einer außergewöhnlichen Notwendigkeit erforderlichen Bedingungen gemäß Artikel 15 für die Zwecke, für die die Daten verlangt werden, erfüllt sind;
  - c) den Zweck des Verlangens, die beabsichtigte Nutzung der verlangten Daten gegebenenfalls auch durch einen Dritten gemäß Absatz 4, und die Dauer dieser Nutzung sowie gegebenenfalls die Art und Weise erläutern, wie die Verarbeitung personenbezogener Daten der außergewöhnlichen Notwendigkeit abhelfen soll;
  - d) nach Möglichkeit angeben, wann die Daten von allen Parteien, die Zugang zu den Daten haben, voraussichtlich gelöscht sein werden;
  - e) die Wahl des Dateninhabers, an den das Verlangen gerichtet ist, begründen;
  - f) alle anderen öffentlichen Stellen oder die Kommission, die Europäische Zentralbank oder Einrichtungen der Union und Dritte angeben, an die die verlangten Daten voraussichtlich weitergegeben werden;
  - g) – falls personenbezogene Daten verlangt werden – alle technischen und organisatorischen Maßnahmen angeben, die zur Umsetzung der Datenschutzgrundsätze und erforderlichen Garantien erforderlich und verhältnismäßig sind, wie etwa die Pseudonymisierung, und ob der Dateninhaber vor der Bereitstellung der Daten eine Anonymisierung vornehmen kann;

(72) Im Falle einer außergewöhnlichen Notwendigkeit im Zusammenhang mit öffentlichen Notstandsmaßnahmen sollten öffentliche Stellen nach Möglichkeit nicht-personenbezogene Daten verwenden. Im Falle von Verlangens, die auf einer außergewöhnlichen Notwendigkeit beruhen, die nicht im Zusammenhang mit einem öffentlichen Notstand steht, können keine personenbezogenen Daten verlangt werden. Wenn personenbezogene Daten Gegenstand des Verlangens sind, sollte der Dateninhaber die Daten stets anonymisieren. Ist es unbedingt erforderlich, mit den Daten für eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union auch personenbezogene Daten bereitzustellen oder erweist sich eine Anonymisierung als unmöglich, so sollte die Stelle, die die Daten verlangt, die strikte Notwendigkeit und die besonderen und begrenzten Zwecke der Verarbeitung nachweisen. Die geltenden Vorschriften über den Schutz personenbezogener Daten sollten eingehalten werden. Die Bereitstellung der Daten und ihre anschließende Nutzung sollten mit Schutzvorkehrungen für die Rechte und Interessen der von diesen Daten betroffenen Personen einhergehen.

- h)* die Rechtsvorschrift angeben, durch die der anfragenden öffentlichen Stelle, der Kommission, der Europäischen Union oder der Einrichtung der Union die für das Datenverlangen relevante spezifische im öffentlichen Interesse ausgeübte Aufgabe übertragen wird;
- i)* die Frist angeben, innerhalb deren die Daten bereitzustellen sind und die Frist gemäß Artikel 18 Absatz 2, innerhalb deren der Dateninhaber das Verlangen ablehnen oder dessen Änderung beantragen kann;
- j)* sich nach besten Kräften darum bemühen, zu vermeiden, dass die Erfüllung des Datenverlangens zur Haftung des Dateninhabers für Verstöße gegen das Unionsrecht oder nationales Recht führt.

(2) Ein Datenverlangen nach Absatz 1 dieses Artikels muss

- a)* schriftlich und in klarer, prägnanter, einfacher und für den Dateninhaber verständlicher Sprache abgefasst sein,
- b)* genaue Angaben zur Art der verlangten Daten enthalten und sich auf die Daten beziehen, über die der Dateninhaber zum Zeitpunkt des Verlangens Kontrolle hat;
- c)* im Hinblick auf die Detailstufe und den Umfang der verlangten Daten sowie die Häufigkeit des Zugangs zu den verlangten Daten in einem angemessenen Verhältnis zu der außergewöhnlichen Notwendigkeit stehen und ausreichend begründet sein;
- d)* die rechtmäßigen Ziele des Dateninhabers unter Zusage der Gewährleistung der Wahrung von Geschäftsgeheimnissen gemäß Artikel 19 Absatz 3 und unter Berücksichtigung der Kosten und des nötigen Aufwands für die Bereitstellung der Daten achten;
- e)* nicht-personenbezogene Daten betreffen, und nur dann, wenn sich erweist, dass dies nicht ausreicht, um auf die außergewöhnliche Notwendigkeit der Nutzung von Daten gemäß Artikel 15 Absatz 1 Buchstabe a zu reagieren, personenbezogene Daten in pseudonymisierter Form verlangen und die technischen und organisatorischen Maßnahmen festlegen, die zum Schutz der Daten ergriffen werden;
- f)* dem Dateninhaber Aufschluss über die Sanktionen geben, die nach Artikel 40 von der nach Artikel 37 benannten zuständigen Behörde verhängt werden, wenn er dem Verlangen nicht nachkommt;
- g)* sofern das Verlangen durch eine öffentliche Stelle erfolgt, dem in Artikel 37 genannten Datenkoordinator des Mitgliedstaats, in dem die anfragende öffentliche Stelle niedergelassen ist, übermittelt werden, der das Verlangen unverzüglich online öffentlich verfügbar macht, es sei denn, die öffentliche Stelle ist der Auffassung, dass diese Veröffentlichung eine Gefahr für die öffentliche Sicherheit darstellen würde;
- h)* sofern das Verlangen durch die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union erfolgt, unverzüglich online verfügbar gemacht werden;
- i)* – falls personenbezogene Daten verlangt werden – der für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörde im

Mitgliedstaat, in dem die öffentliche Stelle niedergelassen ist, unverzüglich gemeldet werden.

Die Europäische Zentralbank und die Einrichtungen der Union informieren die Kommission über ihre Verlangen.

(69) Im Einklang mit Artikel 6 Absätze 1 und 3 der Verordnung (EU) 2016/679 ist ein verhältnismäßiger, begrenzter und vorhersehbarer Rahmen auf Unionsebene erforderlich, wenn es um die Wahl der Rechtsgrundlage für die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen, die Kommission, die Europäische Zentralbank und die Einrichtungen der Union im Fall außergewöhnlicher Notwendigkeit geht, um sowohl Rechtssicherheit zu gewährleisten als auch den Verwaltungsaufwand für Unternehmen so gering wie möglich zu halten. Zu diesem Zweck sollten Datenverlangen öffentlicher Stellen, der Kommission, der Europäischen Zentralbank oder der Einrichtungen der Union an Dateninhaber hinsichtlich ihres Umfangs und ihrer Detailstufe spezifisch, transparent und verhältnismäßig sein. Der Zweck des Verlangens und die beabsichtigte Nutzung der verlangten Daten sollten konkret und eindeutig erläutert werden, wobei der anfragenden Stelle eine angemessene Flexibilität bei der Wahrnehmung ihrer Aufgaben im öffentlichen Interesse einzuräumen ist. Das Verlangen sollte auch den berechtigten Interessen der Dateninhaber, an die es gerichtet wird, Rechnung tragen. Der Aufwand für die Dateninhaber sollte so gering wie möglich gehalten werden, indem die anfragenden Stellen verpflichtet werden, den Einmaligkeitsgrundsatz einzuhalten, der verhindert, dass dieselben Daten mehrmals oder von mehreren öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder den Einrichtungen der Union verlangt werden. Zur Gewährleistung der Transparenz sollten Datenverlangen, die von der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union gestellt werden, unverzüglich von der die Daten verlangenden Stelle veröffentlicht werden. Die Europäische Zentralbank und die Einrichtungen der Union sollten die Kommission über ihre Verlangen unterrichten. Wenn das Datenverlangen von einer öffentlichen Stelle gestellt wurde, sollte diese Stelle auch den Datenkoordinator des Mitgliedstaats, in dem die öffentliche Stelle niedergelassen ist, unterrichten. Es sollte sichergestellt werden, dass alle Verlangen online öffentlich verfügbar sind. Nach einer solchen Unterrichtung über ein Datenverlangen kann die zuständige Behörde beschließen, die Rechtmäßigkeit des Verlangens zu bewerten, und ihre Aufgaben im Zusammenhang mit der Durchsetzung und Anwendung dieser Verordnung wahrnehmen. Der Datenkoordinator sollte sicherstellen, dass alle von öffentlichen Stellen gestellten Verlangen online öffentlich verfügbar sind.

- (3) Eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union dürfen nach diesem Kapitel erlangte Daten nicht zur Weiterverwendung im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2022/868 oder Artikel 2 Nummer 11 der Richtlinie (EU) 2019/1024 bereitstellen. Die Verordnung (EU) 2022/868 und die Richtlinie (EU) 2019/1024 finden keine Anwendung auf nach diesem Kapitel erlangte von öffentlichen Stellen gehaltene Daten.

(70) Mit der Datenbereitstellungspflicht soll sichergestellt werden, dass öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union über das erforderliche Wissen zur Bewältigung oder Verhinderung öffentlicher Notstände oder zu deren Überwindung 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 weder die Verordnung (EU) 2022/868 noch die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates (28) für Daten gelten, die im Rahmen der vorliegenden Verordnung bereitgestellt werden, und diese Daten 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 Weitergabe der Daten zu Forschungszwecken oder für die Entwicklung, Erstellung und Verbreitung amtlicher Statistiken unberührt lassen, sofern die in der vorliegenden Verordnung festgelegten Bedingungen erfüllt sind. Öffentliche Stellen sollten auch Daten, die sie gemäß der vorliegenden Verordnung erlangt haben, mit anderen öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union austauschen dürfen, um die außergewöhnliche Notwendigkeit auszuräumen, wegen der sie verlangt wurden.

- (4) Durch Absatz 3 dieses Artikels wird eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union nicht daran gehindert, nach diesem Kapitel erlangte Daten mit einer anderen öffentlichen Stelle oder mit der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union zwecks Wahrnehmung der in Artikel 15 genannten Aufgaben auszutauschen, wie in dem Verlangen gemäß Absatz 1 Buchstabe f des vorliegenden Artikels angegeben, oder die Daten einem Dritten bereitzustellen, wenn sie im Rahmen einer öffentlich verfügbaren Vereinbarung technische Inspektionen oder andere Aufgaben an diesen Dritten delegiert hat. Die Pflichten öffentlicher Stellen gemäß Artikel 19, insbesondere die Garantien zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen, gelten auch für diese Dritten. Wenn eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union Daten nach diesem Absatz übermittelt oder bereitstellt, teilt sie dies dem Dateninhaber, von dem sie die Daten erhalten hat, unverzüglich mit.
- (5) Ist der Dateninhaber der Ansicht, dass seine Rechte nach diesem Kapitel durch die Übermittlung oder Bereitstellung von Daten verletzt wurden, so kann er bei der nach Artikel 37 benannten zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, Beschwerde einlegen.
- (6) Die Kommission entwickelt ein Musterformular für Verlangen gemäß dem vorliegenden Artikel.

## **Artikel 18 Erfüllung von Datenverlangen**

- (1) Ein Dateninhaber, der ein Datenzugangsverlangen nach diesem Kapitel erhält, stellt der anfragenden öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union die Daten unverzüglich bereit, wobei die erforderlichen technischen, organisatorischen und rechtlichen Maßnahmen berücksichtigt werden.
- (2) Unbeschadet besonderer Erfordernisse bezüglich der Verfügbarkeit von Daten, die in Unionsrecht oder nationalem Recht festgelegt sind, kann ein Dateninhaber Datenzugangsverlangen im Sinne dieses Kapitels im Falle von Daten, die zur Bewältigung eines öffentlichen Notstands erforderlich sind, unverzüglich und in jedem Fall innerhalb von fünf Arbeitstagen nach Eingang des Datenverlangens sowie in anderen Fällen einer au-

ßergewöhnlichen Notwendigkeit unverzüglich und in jedem Fall innerhalb von 30 Arbeitstagen nach Eingang des betreffenden Datenverlangens aus einem der folgenden Gründe ablehnen oder deren Änderung beantragen:

(71) Dateninhaber sollten die Möglichkeit haben, je nach Art der in dem Verlangen geltend gemachten außergewöhnlichen Notwendigkeit unverzüglich und in jedem Fall spätestens innerhalb von fünf oder 30 Arbeitstagen entweder eine Änderung des Verlangens einer öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union abzulehnen oder dieses zu beantragen. Gegebenenfalls sollte der Dateninhaber diese Gelegenheit haben, wenn er keine Kontrolle über die verlangten Daten hat, d. h. wenn er keinen unmittelbaren Zugang zu den Daten hat und deren Verfügbarkeit nicht feststellen kann. Die Nichtbereitstellung der Daten sollte sich begründen lassen, wenn nachgewiesen werden kann, dass das Verlangen mit einem zuvor von einer anderen öffentlichen Stelle oder von der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union zu demselben Zweck eingereichten Verlangen vergleichbar ist und der Dateninhaber nicht über die Löschung der Daten gemäß dieser Verordnung informiert wurde. Wenn ein Dateninhaber das Verlangen ablehnt oder dessen Änderung beantragt, sollte er die Ablehnung gegenüber der öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der Einrichtung der Union, die das Verlangen gestellt hat, begründen. Wenn in Bezug auf die verlangten Datensätze die Datenbankrechte sui generis gemäß der Richtlinie 96/9/ des Europäischen Parlaments und des Rates (29) Anwendung finden, sollten die Dateninhaber ihre Rechte in einer Weise ausüben, die die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder Einrichtung der Union nicht daran hindert, die Daten im Einklang mit dieser Verordnung zu erlangen oder weiterzugeben.

- a) Der Dateninhaber hat keine Kontrolle über die verlangten Daten;
  - b) ein ähnliches Verlangen zu demselben Zweck wurde bereits von einer anderen öffentlichen Stelle oder von der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union gestellt, und der Dateninhaber wurde nicht gemäß Artikel 19 Absatz 1 Buchstabe c über das Löschen der Daten unterrichtet;
  - c) das Verlangen erfüllt nicht die Voraussetzungen nach Artikel 17 Absätze 1 und 2.
- (3) Wenn der Dateninhaber das Verlangen gemäß Absatz 2 Buchstabe b ablehnt oder dessen Änderung beantragt, nennt er die öffentliche Stelle oder die Kommission, die Europäische Zentralbank oder die Einrichtung der Union, die zuvor zu demselben Zweck Daten verlangt hatte.
- (4) Wenn die verlangten Daten auch personenbezogene Daten enthalten, werden diese vom Dateninhaber ordnungsgemäß anonymisiert, es sei denn, zur Erfüllung des Datenzugangsverlangens einer öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union ist die Offenlegung personenbezogener Daten erforderlich. In diesen Fällen muss der Dateninhaber die Daten pseudonymisieren.
- (5) Wenn die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union beabsichtigt, der Ablehnung des Datenverlangens eines Dateninhabers zu widersprechen, oder wenn der Dateninhaber Einspruch gegen das Verlangen einzulegen beabsichtigt und die Angelegenheit durch eine entsprechende Änderung des Verlangens nicht beigelegt werden kann, wird die nach Artikel 37 benannte zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, mit der Angelegenheit befasst.

## **Artikel 19 Pflichten öffentlicher Stellen, der Kommission, der Europäischen Zentralbank und der Einrichtungen der Union**

- (1) Eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union, die Daten aufgrund eines Verlangens nach Artikel 14 erhalten hat,
- a) darf die Daten nicht in einer Weise nutzen, die mit dem Zweck des Datenverlangens unvereinbar ist;
  - b) muss technische und organisatorische Maßnahmen getroffen haben, die die Vertraulichkeit und Integrität der verlangten Daten und die Sicherheit der Datenübermittlungen – insbesondere bei personenbezogenen Daten – wahren und die Rechte und Freiheiten der betroffenen Personen schützen;
  - c) muss die Daten löschen, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und dem Dateninhaber sowie den Einzelpersonen oder Organisationen, die die Daten gemäß Artikel 21 Absatz 1 erhalten haben, unverzüglich mitteilen, dass die Daten gelöscht worden sind, es sei denn, die Archivierung der Daten ist im Einklang mit Unionsrecht oder nationalem Recht über den Zugang der Öffentlichkeit zu Dokumenten im Rahmen der Transparenzverpflichtungen vorgeschrieben.

(73) Daten, die öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union wegen einer außergewöhnlichen Notwendigkeit bereitgestellt werden, sollten nur für die Zwecke des Datenverlangens genutzt werden, es sei denn, der Dateninhaber, der die Daten bereitgestellt hat, hat ausdrücklich zugestimmt, dass die Daten für andere Zwecke genutzt werden. Sofern nichts anderes vereinbart wurde, sollten die Daten gelöscht werden, sobald sie für den im Verlangen genannten Zweck nicht mehr erforderlich sind, und der Dateninhaber sollte davon in Kenntnis gesetzt werden. Diese Verordnung baut auf den bestehenden Zugangsregelungen der Union und der Mitgliedstaaten auf und bewirkt keine Änderung des nationalen Rechts für den Zugang der Öffentlichkeit zu Dokumenten im Zusammenhang mit Transparenzpflichten. Daten sollten gelöscht werden, sobald sie nicht mehr benötigt werden, um diesen Transparenzpflichten nachzukommen.

- (2) Eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union oder Dritte, die Daten gemäß diesem Kapitel erhalten, sind nicht berechtigt,
- a) die Daten oder Erkenntnisse über die wirtschaftliche Lage, die Vermögenswerte und Produktions- oder Betriebsmethoden des Dateninhabers zu nutzen, um ein vernetztes Produkt oder einen verbundenen Dienst zu entwickeln oder zu verbessern, das bzw. die mit dem vernetzten Produkt oder des verbundenen Dienstes des Dateninhabers im Wettbewerb steht;
  - b) die Daten für die unter Buchstabe a genannten Zwecke an einen anderen Dritten weiterzugeben.

(74) Bei der Weiterverwendung von Daten, die von Dateninhabern bereitgestellt werden, sollten öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union sowohl geltendes Unionsrecht oder nationales Recht als auch die vertraglichen Pflichten des Dateninhabers einhalten. Sie sollten sowohl davon absehen, ein vernetztes Produkt oder einen verbundenen Dienst zu entwickeln oder zu verbessern, das/die mit dem vernetzten Produkt oder des verbundenen Dienstes des Dateninhabers im Wettbewerb steht, als auch davon, die Daten zu diesen

Zwecken an Dritte weiterzugeben. Außerdem sollten sie einen Dateninhaber auf dessen Ersuchen hin öffentlich anerkennen und für die Gewährleistung der Sicherheit der erhaltenen Daten verantwortlich sein. Ist die Offenlegung von Geschäftsgeheimnissen des Dateninhabers gegenüber öffentlichen Stellen, der Kommission, der Europäischen Zentralbank oder Einrichtungen der Union unbedingt erforderlich, um den Zweck zu erfüllen, für den die Daten verlangt wurden, so sollte dem Dateninhaber die Vertraulichkeit dieser Daten vor deren Offenlegung zugesichert werden.

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

## **Artikel 20 Ausgleich im Falle einer außergewöhnlichen Notwendigkeit**

(75) Wenn es um den Schutz eines bedeutenden öffentlichen Gutes geht, wie etwa die Bewältigung öffentlicher Notstände, sollte von der öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der betreffenden Einrichtung der Union nicht erwartet werden, dass sie den Unternehmen für die erlangten Daten eine Gegenleistung gewähren. Öffentliche Notstände sind seltene Ereignisse, und nicht alle derartigen Notstände erfordern die Nutzung von Daten, die von Unternehmen gehalten werden. Gleichzeitig könnte die Verpflichtung zur Bereitstellung von Daten für Kleinunternehmen und Kleinunternehmen eine erhebliche Belastung darstellen. Diese Unternehmen sollten daher selbst im Kontext öffentlicher Notstandsmaßnahmen eine Gegenleistung verlangen können. Es ist nicht wahrscheinlich, dass die Geschäftstätigkeit der Dateninhaber durch die Inanspruchnahme dieser Verordnung durch öffentliche Stellen, die Kommission, die Europäische Zentralbank oder Einrichtungen der Union beeinträchtigt wird. Da Fälle einer außergewöhnlichen Notwendigkeit, bei denen es sich nicht um die Bewältigung eines öffentlichen Notstands handelt, jedoch unter Umständen häufiger sind, sollten Dateninhaber in diesen Fällen Anspruch auf eine angemessene Gegenleistung haben, die die mit der Erfüllung des Verlangens verbundenen technischen und organisatorischen Kosten nicht übersteigen sollte, sowie auf die angemessene Marge, die zur Bereitstellung der Daten für die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union erforderlich ist. Die Gegenleistung sollte nicht als Bezahlung für die Daten selbst und nicht als obligatorisch verstanden werden. Dateninhaber sollten keine Gegenleistung verlangen können, wenn die nationalen statistischen Ämter oder andere für die Erstellung von Statistiken zuständige nationale Behörden Dateninhabern aufgrund des nationalen Rechts keine Gegenleistung für die Bereitstellung von Daten gewähren dürfen. Die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die betreffende Einrichtung der Union sollte in der Lage sein, die Höhe der vom Dateninhaber geforderten Gegenleistung anzufechten, indem sie die zuständige Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, mit der Angelegenheit befasst.

- (1) Dateninhaber, bei denen es sich nicht um Kleinstunternehmen und Kleinunternehmen handelt, stellen die zur Bewältigung eines öffentlichen Notstands nach Artikel 15 Absatz 1 Buchstabe a erforderlichen Daten unentgeltlich bereit. Die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union, die die Daten erhalten haben, erkennen den Beitrag des Dateninhabers auf dessen Ersuchen hin öffentlich an.
- (2) Der Dateninhaber hat Anspruch auf eine faire Gegenleistung für die Bereitstellung von Daten im Einklang mit einem Verlangen gemäß Artikel 15 Absatz 1 Buchstabe b. Diese Gegenleistung deckt mindestens die technischen und organisatorischen Kosten, die durch die Erfüllung des Verlangens entstehen, gegebenenfalls einschließlich der Kosten einer Anonymisierung, Pseudonymisierung, Aggregation und technischen Anpassung, und einer angemessenen Marge. Auf Verlangen der öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der Einrichtung der Union übermittelt der Dateninhaber Informationen über die Grundlage der Kostenberechnung und die angemessene Marge.
- (3) Absatz 2 gilt auch, wenn Kleinstunternehmen und Kleinunternehmen für die Bereitstellung von Daten eine Gegenleistung beanspruchen.
- (4) Dateninhaber haben kein Recht auf Gegenleistung für die Bereitstellung von Daten zur Erfüllung eines Verlangens gemäß Artikel 15 Absatz 1 Buchstabe b, falls die besondere Aufgabe im öffentlichen Interesse in der Erstellung amtlicher Statistiken durchgeführt wird und der Erwerb von Daten nach nationalem Recht nicht zulässig ist. Die Mitgliedstaaten unterrichten die Kommission, wenn der Erwerb von Daten für die Erstellung amtlicher Statistiken nach nationalem Recht nicht zulässig ist.
- (5) Ist die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union mit der Höhe der vom Dateninhaber geforderten Gegenleistung nicht einverstanden, so kann sie bei der nach Artikel 37 benannten zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, Beschwerde einlegen.

### **Artikel 21 Weitergabe von im Zusammenhang mit außergewöhnlichen Notwendigkeiten erhaltenen Daten an Forschungseinrichtungen oder statistische Ämter**

- (1) Eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union ist berechtigt, die nach diesem Kapitel erhaltenen Daten weiterzugeben
  - a) an Einzelpersonen oder Organisationen im Hinblick auf die Durchführung wissenschaftlicher Forschungstätigkeiten oder Analysen, die mit dem Zweck des Datenverlangens vereinbar sind, oder
  - b) an nationale statistische Ämter oder an Eurostat zur Erstellung amtlicher Statistiken.
- (2) Personen oder Organisationen, die Daten nach Absatz 1 erhalten, müssen gemeinnützig oder im Rahmen einer nach Unionsrecht oder nach nationalem Recht anerkannten Aufgabe von öffentlichem Interesse handeln. Dies umfasst keine Organisationen, die in

erheblichem Maße dem Einfluss gewerblicher Unternehmen unterliegen, wodurch diese einen bevorzugten Zugang zu den Forschungsergebnissen erhalten könnten.

- (3) Einzelpersonen oder Organisationen, die Daten nach Absatz 1 des vorliegenden Artikels erhalten, müssen die gleichen Verpflichtungen erfüllen, die für öffentliche Stellen, die Kommission, die Europäische Zentralbank oder die Einrichtungen der Union nach Artikel 17 Absatz 3 und Artikel 19 gelten.
- (4) Unbeschadet des Artikels 19 Absatz 1 Buchstabe c können Einzelpersonen oder Organisationen, die Empfänger der Daten gemäß Absatz 1 dieses Artikels sind, die erhaltenen Daten, nachdem sie von den öffentlichen Stellen, der Kommission, der Europäischen Zentralbank und den Einrichtungen der Union gelöscht wurden, für einen Zeitraum von bis zu sechs Monaten für die Zwecke des Datenverlangens aufbewahren.
- (5) Beabsichtigt eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union, Daten gemäß Absatz 1 des vorliegenden Artikels zu übermitteln oder bereitzustellen, so teilt sie dies dem Dateninhaber, von dem die Daten empfangen wurden, unverzüglich mit, unter Angabe der Identität und der Kontaktdaten der die Daten empfangenden Organisation oder Einzelperson, des Zwecks der Übermittlung oder Bereitstellung der Daten, des Zeitraums, für den die Daten verwendet werden sollen, und der getroffenen technischen Schutzmaßnahmen und organisatorischen Maßnahmen, auch wenn personenbezogene Daten oder Geschäftsgeheimnisse betroffen sind. Ist der Dateninhaber mit der Übermittlung oder Bereitstellung von Daten nicht einverstanden, so kann er bei der nach Artikel 37 benannten zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, Beschwerde einlegen.

(76) Die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union sollte befugt sein, die Daten, die sie aufgrund des Verlangens erlangt hat, an andere Stellen oder Personen weiterzugeben, wenn dies zur Durchführung wissenschaftlicher oder analytischer Tätigkeiten erforderlich ist, die sie nicht selbst durchführen kann, sofern diese Tätigkeiten mit dem Zweck des Datenverlangens vereinbar sind. Sie sollte den Dateninhaber rechtzeitig über eine solche Weitergabe unterrichten. Die Daten können unter den gleichen Umständen auch zur Entwicklung, Erstellung und Verteilung amtlicher Statistiken an die nationalen statistischen Ämter und Eurostat weitergegeben werden. Die betreffenden Forschungstätigkeiten sollten jedoch mit dem Zweck des Datenverlangens vereinbar sein, 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. Organisationen sollten für die Zwecke dieser Verordnung nicht als Forschungsorganisationen gelten, wenn sie in erheblichem Maße dem Einfluss gewerblicher Unternehmen unterliegen, die aufgrund der strukturellen Gegebenheiten Kontrolle ausüben können und dadurch einen bevorzugten Zugang zu den Forschungsergebnissen erhalten könnten.

## **Artikel 22 Amtshilfe und grenzüberschreitende Zusammenarbeit**

- (1) Öffentliche Stellen, die Kommission, die Europäische Zentralbank und die Einrichtungen der Union arbeiten im Hinblick auf die kohärente Umsetzung dieses Kapitels zusammen und unterstützen sich diesbezüglich gegenseitig.

- (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 des Datenverlangens unvereinbar ist.
- (3) Beabsichtigt eine öffentliche Stelle, von einem Dateninhaber, der in einem anderen Mitgliedstaat niedergelassen ist, die Bereitstellung von Daten zu verlangen, so teilt sie diese Absicht zunächst der nach Artikel 37 benannten zuständigen Behörde jenes Mitgliedstaats mit. Diese Anforderung gilt auch für Zugangsverlangen der Kommission, der Europäischen Zentralbank sowie von Einrichtungen der Union. Das Verlangen wird von der zuständigen Behörde des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, geprüft.
- (4) Nach Prüfung des Verlangens im Lichte der in Artikel 17 festgelegten Anforderungen ergreift die jeweils zuständige Behörde unverzüglich eine der folgenden Maßnahmen:
  - a) Sie übermittelt das Verlangen an den Dateninhaber und weist die anfragende öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union gegebenenfalls darauf hin, dass sie mit öffentlichen Stellen des Mitgliedstaats, in dem der Dateninhaber niedergelassen ist, zusammenarbeiten muss, um den Verwaltungsaufwand für den Dateninhaber bei der Erfüllung des Verlangens zu verringern;
  - b) sie lehnt das Verlangen aus hinreichend begründeten Gründen im Einklang mit diesem Kapitel ab.

Die anfragende öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union trägt dem Hinweis der jeweils zuständigen Behörde sowie den von dieser genannten Gründen gemäß Unterabsatz 1 Rechnung, bevor sie, falls zutreffend, weitere Maßnahmen wie die erneute Einreichung des Verlangens ergreift.

(77) Zur Bewältigung eines grenzüberschreitenden öffentlichen Notstands oder einer anderen außergewöhnlichen Notwendigkeit können Datenverlangen an Dateninhaber in anderen Mitgliedstaaten als dem der anfragenden öffentlichen Stelle gerichtet werden. In diesem Fall sollte die anfragende öffentliche Stelle die zuständige Behörde des Mitgliedstaats unterrichten, in dem der Dateninhaber niedergelassen ist, damit diese das Verlangen anhand der in der vorliegenden Verordnung festgelegten Kriterien prüfen kann. Dies sollte auch für Verlangen der Kommission, der Europäischen Zentralbank oder einer Einrichtung der Union gelten. Falls personenbezogene Daten verlangt werden, sollte die öffentliche Stelle die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in dem Mitgliedstaat, in dem die öffentliche Stelle niedergelassen ist, informieren. Die betreffende zuständige Behörde sollte befugt sein, die öffentliche Stelle, die Kommission, die Europäische Zentralbank oder die Einrichtung der Union darauf hinzuweisen, dass sie mit den öffentlichen Stellen des Mitgliedstaats zusammenarbeiten muss, in dem der Dateninhaber niedergelassen ist, um den Verwaltungsaufwand für den Dateninhaber zu minimieren. Hat die zuständige Behörde hinsichtlich der Vereinbarkeit des Verlangens mit dieser Verordnung triftige Einwände, so sollte sie das Verlangen der öffentlichen Stelle, der Kommission, der Europäischen Zentralbank oder der Einrichtung der Union ablehnen, die diesen Einwänden ihrerseits Rechnung tragen sollte, bevor sie weitere Maßnahmen – einschließlich der erneuten Einreichung des Verlangens – ergreift.

# Kapitel VI Wechsel zwischen Datenverarbeitungsdiensten

## Artikel 23 Beseitigung von Hindernissen für einen wirksamen Wechsel

Anbieter von Datenverarbeitungsdiensten treffen die in den Artikeln 25, 26, 27, 29 und 30 vorgesehenen Maßnahmen, um es Kunden zu ermöglichen, zu einem Datenverarbeitungsdienst, der die gleiche Dienstleistung abdeckt, die von einem anderen Anbieter von Datenverarbeitungsdiensten erbracht wird, oder zu IKT-Infrastruktur in eigenen Räumlichkeiten zu wechseln oder gegebenenfalls mehrere Anbieter von Datenverarbeitungsdiensten gleichzeitig in Anspruch zu nehmen. Insbesondere dürfen Anbieter von Datenverarbeitungsdiensten keine vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse aufzwingen und müssen solche Hindernisse beseitigen, wenn sie die Kunden daran hindern,

- a) den Vertrag über den Datenverarbeitungsdienst nach der maximalen Kündigungsfrist und nachdem der Wechsel gemäß Artikel 25 erfolgreich vollzogen ist, zu kündigen;
- b) neue Verträge mit einem anderen Anbieter von Datenverarbeitungsdiensten für die gleiche Dienstleistung zu schließen;
- c) exportierbare Daten des Kunden und digitale Vermögenswerte zu einem anderen Anbieter von Datenverarbeitungsdiensten oder zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu übertragen, auch nach Inanspruchnahme eines unentgeltlichen Angebots;
- d) gemäß Artikel 24 die Funktionsäquivalenz bei der Nutzung des neuen Datenverarbeitungsdienstes in der IKT-Umgebung eines anderen Anbieters von Datenverarbeitungsdiensten, der die gleiche Dienstleistung abdeckt, zu erreichen;
- e) die in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienste von anderen von dem Anbieter von Datenverarbeitungsdiensten erbrachten Datenverarbeitungsdiensten zu trennen, soweit dies technisch durchführbar ist.

(78) Die Fähigkeit der Kunden von Datenverarbeitungsdiensten, einschließlich Cloud- und Edge-Diensten, von einem Datenverarbeitungsdienst unter Wahrung eines Mindestumfangs von Dienstfunktionen – und ohne dass es zu Ausfallzeiten kommt – zu einem anderen zu wechseln oder ohne unangemessene Erschwernisse und Datenübertragungskosten Dienste mehrerer Anbieter zu nutzen, ist eine wesentliche Voraussetzung für einen stärker wettbewerbsorientierten Markt mit geringeren Marktzutrittsschranken für neue Anbieter von Datenverarbeitungsdiensten sowie für die Sicherstellung einer besseren Resilienz der Nutzer dieser Dienste. Kunden, die von unentgeltlichen Angeboten profitieren, sollten auch von den in dieser Verordnung festgelegten Bestimmungen für den Wechsel profitieren, damit diese Angebote nicht zu einer Abhängigkeitssituation für die Kunden führen.

(79) Mit der Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates (30) werden Anbieter von Datenverarbeitungsdiensten angehalten, Verhaltensregeln für die Selbstregulierung zu entwickeln und wirksam umzusetzen, die bewährte Verfahren umfassen, unter anderem zur Erleichterung des Wechsels des Anbieters

von Datenverarbeitungsdiensten und der Übertragung von Daten. Da die Verbreitung daraufhin entwickelter Selbstregulierungsrahmen zurückhaltend ausfiel und es generell an offenen Standards und Schnittstellen mangelt, muss für Anbieter von Datenverarbeitungsdiensten eine Reihe regulatorischer Mindestverpflichtungen festgelegt werden, um jene vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse auszuräumen, die im Fall eines Anbieterwechsels des Kunden nicht nur zu einer geminderten Datenübertragungsgeschwindigkeit führen, sondern den effektiven Vollzug des Wechsels zwischen Datenverarbeitungsdiensten verhindern.

(82) Wenn der ursprüngliche Anbieter von Datenverarbeitungsdiensten die Extraktion der dem Kunden gehörenden exportierbaren Daten behindert, kann das die Wiederherstellung der Dienstfunktionen in der Infrastruktur des übernehmenden Anbieters von Datenverarbeitungsdiensten behindern. Um die Ausstiegsstrategie des Kunden zu erleichtern, unnötige und aufwändige Aufgaben zu vermeiden und sicherzustellen, dass der Kunde keine seiner Daten durch den Vollzug des Wechsels verliert, sollte der ursprüngliche Anbieter von Datenverarbeitungsdiensten den Kunden im Voraus über den Umfang der Daten unterrichten, die exportiert werden können, sobald dieser Kunde beschließt, zu einem anderen Dienst, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, oder zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu wechseln. Der Begriff "exportierbare Daten" sollte zumindest die Eingabe- und Ausgabedaten – einschließlich Metadaten –, die durch die Nutzung des Datenverarbeitungsdienstes durch den Kunden unmittelbar oder mittelbar generiert oder gemeinsam generiert werden, umfassen, mit Ausnahme der Vermögenswerte oder Daten von dem Anbieter von Datenverarbeitungsdiensten oder von einem Dritten. Vermögenswerte oder Daten von dem Anbieter von Datenverarbeitungsdiensten oder von einem Dritten, die durch Rechte des geistigen Eigentums geschützt sind oder Geschäftsgeheimnisse dieses Anbieters oder Dritten darstellen, oder Daten im Zusammenhang mit der Integrität und Sicherheit des Dienstes, bei denen der Anbieter von Datenverarbeitungsdiensten im Falle eines Exports Cybersicherheitsrisiken ausgesetzt ist, sollten von den exportierbaren Daten ausgenommen sein. Diese Ausnahmen sollten den Vollzug des Wechsels weder behindern noch verzögern.

(84) Ziel dieser Verordnung ist es, den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, wozu die Bedingungen und Maßnahmen gehören, die notwendig sind, damit ein Kunde in der Lage ist, einen Vertrag für einen Datenverarbeitungsdienst zu kündigen, einen oder mehrere neue Verträge mit verschiedenen Anbietern von Datenverarbeitungsdiensten zu schließen, seine exportierbaren Daten und digitalen Vermögenswerte zu übertragen und gegebenenfalls von Funktionsäquivalenz zu profitieren.

(91) Wenn Anbieter von Datenverarbeitungsdiensten ihrerseits Kunden von Datenverarbeitungsdiensten sind, die von einem Dritten erbracht werden, können sie selbst vom wirksameren Vollzug des Wechsels profitieren, während sie in Bezug auf eigene Dienstangebote weiter an die Pflichten nach dieser Verordnung gebunden bleiben.

(92) Anbieter von Datenverarbeitungsdiensten sollten verpflichtet sein, im Rahmen ihrer Fähigkeiten und in einem angemessenen Verhältnis zu ihren jeweiligen Verpflichtungen jede Hilfe und Unterstützung zu leisten, die erforderlich ist, um den Wechsel zum Dienst eines anderen Anbieters von Datenverarbeitungsdiensten erfolgreich, effektiv und sicher zu vollziehen. Diese Verordnung verpflichtet Anbieter von Datenverarbeitungsdiensten nicht dazu, neue Kategorien von Datenverarbeitungsdiensten, auch nicht innerhalb der IKT-Infrastruktur verschiedener Anbieter von Datenverarbeitungsdiensten oder auf deren Grundlage zu entwickeln, um die Funktionsäquivalenz in einer anderen als der eigenen Umgebung zu gewährleisten. Der ursprüngliche Anbieter von Datenverarbeitungsdiensten hat weder Zugang zur noch

Einblick in die Umgebung des übernehmenden Anbieters von Datenverarbeitungsdiensten. Funktionsäquivalenz sollte also nicht dahingehend verstanden werden, dass sie den ursprünglichen Anbieter von Datenverarbeitungsdiensten zur Wiederherstellung des betreffenden Dienstes innerhalb der Infrastruktur des übernehmenden Anbieters von Datenverarbeitungsdiensten verpflichtet. Der ursprüngliche Anbieter von Datenverarbeitungsdiensten sollte vielmehr im Rahmen seiner Befugnisse alle ihm vernünftigerweise zur Verfügung stehenden Maßnahmen ergreifen, um die Verwirklichung der Funktionsäquivalenz zu ermöglichen, indem er Kapazitäten, angemessene Informationen, Dokumentation, technische Unterstützung und gegebenenfalls die erforderlichen Instrumente bereitstellt.

(93) Anbieter von Datenverarbeitungsdiensten sollten zudem dazu verpflichtet werden, bestehende Hindernisse auszuräumen und keine neuen Hindernisse zu schaffen; dies gilt auch in Bezug auf Kunden, die zu einer IKT-Infrastruktur in eigenen Räumlichkeiten wechseln möchten. Hindernisse können unter anderem vorkommerzieller, gewerblicher, technischer, vertraglicher oder organisatorischer Art sein. Anbieter von Datenverarbeitungsdiensten sollten ferner dazu verpflichtet werden, Hindernisse für die Herauslösung eines bestimmten einzelnen Dienstes aus anderen, im Rahmen eines Vertrags erbrachten Datenverarbeitungsdiensten zu beseitigen und einen Wechsel für den betreffenden Dienst zu ermöglichen, wenn einer solchen Herauslösung keine größeren, nachweislichen technischen Hindernisse entgegenstehen.

## **Artikel 24 Tragweite der technischen Verpflichtungen**

Die Verantwortung von Anbietern von Datenverarbeitungsdiensten gemäß der Artikel 23, 25, 29, 30 und 34 gilt nur für die Dienste, Verträge oder Geschäftsgepflogenheiten, die vom ursprünglichen Anbieter der Datenverarbeitungsdienste angeboten wurden.

## **Artikel 25 Vertragsklauseln für den Wechsel**

(96) Um die Interoperabilität und den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, sollten Nutzer und Anbieter von Datenverarbeitungsdiensten die Verwendung von Instrumenten für die Umsetzung und die Einhaltung der Vorschriften in Erwägung ziehen, vor allem derjenigen, die von der Kommission in Form eines EU-Regelwerks für die Cloud sowie eines Leitfadens für die Vergabe öffentlicher Aufträge für Datenverarbeitungsdiensten veröffentlicht wurden. Insbesondere Standardvertragsklauseln sind geeignet, da sie das Vertrauen in Datenverarbeitungsdienste stärken, ein ausgewogeneres Verhältnis zwischen Nutzern und Anbietern von Datenverarbeitungsdiensten schaffen und die Rechtssicherheit in Bezug auf die Bedingungen für den Wechsel zu anderen Datenverarbeitungsdiensten erhöhen. In diesem Zusammenhang sollten Nutzer und Anbieter von Datenverarbeitungsdiensten die Verwendung der Standardvertragsklauseln oder anderer Instrumente für die Einhaltung von Vorschriften durch Selbstregulierung – sofern diese den Anforderungen dieser Verordnung entsprechen –, in Erwägung ziehen, die von einschlägigen Gremien oder Sachverständigengruppen, die nach Unionsrecht eingerichtet wurden, ausgearbeitet wurden.

- (1) Die Rechte des Kunden und die Pflichten des Anbieters von Datenverarbeitungsdiensten in Bezug auf den Wechsel zwischen Anbietern solcher Dienste oder gegebenenfalls zu einer IKT-Infrastruktur in eigenen Räumlichkeiten werden eindeutig in einem schriftlichen Vertrag festgelegt. Der Anbieter von Datenverarbeitungsdiensten stellt dem Kunden diesen Vertrag vor der Vertragsunterzeichnung so bereit, dass er den Vertrag speichern und reproduzieren kann.

- (2) Unbeschadet der Richtlinie (EU) 2019/770 enthält der in Absatz 1 dieses Artikels genannte Vertrag mindestens Folgendes:
- a) Klauseln, die es dem Kunden ermöglichen, auf Verlangen zu einem Datenverarbeitungsdienst zu wechseln, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, oder alle exportierbaren Daten und digitalen Vermögenswerte unverzüglich und in keinem Fall zu einem späteren Zeitpunkt als nach Ablauf der verbindlichen Übergangsfrist von höchstens 30 Kalendertagen ab Ablauf der in Buchstabe d genannten maximalen Kündigungsfrist auf eine IKT-Infrastruktur in eigenen Räumlichkeiten zu übertragen, wobei der Anbieter von Datenverarbeitungsdiensten in dieser Frist
    - (i) i) dem Kunden und von ihm autorisierten Dritten beim Vollzug des Wechsels angemessene Unterstützung leistet;
    - (ii) ii) mit der gebotenen Sorgfalt handelt, um die Kontinuität des Geschäftsbetriebs aufrechtzuerhalten und die Erbringung der vertragsmäßigen Funktionen oder Dienste fortzusetzen;
    - (iii) iii) eindeutig über bekannte Risiken für die unterbrechungsfreie Erbringung der Funktionen oder Dienste unterrichtet, die auf den ursprünglichen Anbieter der Datenverarbeitungsdienste zurückgehen;
    - (iv) iv) während der Wechsel vollzogen wird, für ein hohes Maß an Sicherheit sorgt; dies gilt insbesondere für die Sicherheit der Daten während ihrer Übertragung und die kontinuierliche Sicherheit der Daten während des in Buchstabe g genannten Abrufzeitraums im Einklang mit dem geltenden Unionsrecht oder dem nationalen Recht;
  - b) die Verpflichtung des Anbieters von Datenverarbeitungsdiensten, die für die vertraglich vereinbarten Dienste relevante Ausstiegsstrategie des Kunden zu unterstützen, unter anderem durch Bereitstellung aller einschlägigen Informationen;
  - c) eine Klausel, in der festgelegt ist, dass der Vertrag als beendet gilt und der Kunde über die Kündigung in einem der folgenden Fälle unterrichtet wird:
    - (i) i) gegebenenfalls, nachdem der Wechsel erfolgreich vollzogen ist;
    - (ii) ii) nach Ablauf der in Buchstabe d genannten maximalen Kündigungsfrist, wenn der Kunde nicht wechseln, sondern seine exportierbaren Daten und digitalen Vermögenswerte nach Beendigung des Dienstes löschen möchte,
  - d) eine maximale Kündigungsfrist für die Einleitung des Wechsels, die zwei Monate nicht überschreiten darf;
  - e) eine erschöpfende Auflistung aller Kategorien von Daten und digitalen Vermögenswerten, die während des Wechselvollzugs übertragen werden können, einschließlich mindestens aller exportierbaren Daten;
  - f) eine erschöpfende Liste der Datenkategorien, die für die interne Funktionsweise des Datenverarbeitungsdienstes des Anbieters spezifisch sind und von den exportierbaren Daten gemäß Buchstabe e des vorliegenden Absatzes ausgenommen werden, wenn die Gefahr einer Verletzung von Geschäftsgeheimnissen des Anbieters besteht, vorausgesetzt solche Ausnahmen behindern oder verzögern den Wechsel nach Artikel 23 Buchstabe c nicht;

- g) eine Mindestfrist für den Datenabruf von mindestens 30 Kalendertagen, der nach dem Ablauf des zwischen dem Kunden und dem Anbieter der Datenverarbeitungsdienste gemäß Buchstabe a des vorliegenden Absatzes und Absatz 4 vereinbarten Übergangszeitraums beginnt;
  - h) eine Klausel, die garantiert, dass alle exportierbaren Daten und digitalen Vermögenswerte, die direkt vom Kunden generiert werden oder sich direkt auf den Kunden beziehen, nach Ablauf des unter Buchstabe g genannten Abrufzeitraums oder nach Ablauf eines vereinbarten alternativen Zeitraums zu einem späteren Zeitpunkt als dem Ablaufdatum des in Buchstabe g genannten Abrufzeitraums vollständig gelöscht werden, sofern der Wechsel erfolgreich vollzogen ist;
  - i) Wechselentgelte, die von Anbietern von Datenverarbeitungsdiensten gemäß Artikel 29 erhoben werden können.
- (3) Der in Absatz 1 genannte Vertrag muss Klauseln enthalten, wonach der Kunde den Anbieter von Datenverarbeitungsdiensten nach Ablauf der maximalen Kündigungsfrist gemäß Absatz 2 Buchstabe d über seine Entscheidung unterrichten kann, eine oder mehrere der folgenden Maßnahmen durchzuführen:
- a) Wechsel zu einem anderen Anbieter von Datenverarbeitungsdiensten, wobei der Kunde in diesem Fall die erforderlichen Angaben zu diesem Anbieter macht;
  - b) Wechsel zu einer IKT-Infrastruktur in eigenen Räumlichkeiten;
  - c) Löschung seiner exportierbaren Daten und digitalen Vermögenswerte.
- (4) Ist der verbindliche maximale Übergangszeitraum nach Absatz 2 Buchstabe a technisch nicht durchführbar, so teilt der Anbieter von Datenverarbeitungsdiensten dies dem Kunden innerhalb von 14 Arbeitstagen nach der Beantragung des Wechsels mit und begründet ordnungsgemäß die technische Undurchführbarkeit und gibt einen alternativen Übergangszeitraum an, der sieben Monate nicht überschreiten darf. Im Einklang mit Absatz 1 wird die Kontinuität des Dienstes während des alternativen Übergangszeitraums gegebenenfalls sichergestellt.
- (87) Datenverarbeitungsdienste werden in verschiedenen Bereichen verwendet und weisen hinsichtlich ihrer Komplexität und der Dienstart Unterschiede auf. Dies ist insbesondere mit Blick auf den Übertragungsvorgang und den entsprechenden Zeitrahmen zu berücksichtigen. Eine Verlängerung des Übergangszeitraums geltend zu machen, wenn der Wechsel aus technischen Gründen nicht in der vorgesehenen Zeit abgeschlossen werden kann, sollte aber dessen ungeachtet nur in hinreichend begründeten Fällen geltend gemacht werden können. Die Beweislast sollte in dieser Hinsicht vollständig beim Anbieter des betreffenden Datenverarbeitungsdienstes liegen. Dies gilt unbeschadet des ausschließlichen Rechts des Kunden, den Übergangszeitraum einmal um einen Zeitraum zu verlängern, der seines Erachtens seinen eigenen Zwecken besser entspricht. Der Kunde kann sich vor oder während des Übergangszeitraums auf dieses Recht auf Verlängerung berufen, wobei zu berücksichtigen ist, dass der Vertrag während des Übergangszeitraums weiterhin gilt.
- (5) Unbeschadet des Absatzes 4 enthält der in Absatz 1 genannte Vertrag Klauseln, wonach der Kunde berechtigt ist, den Übergangszeitraum einmal um einen Zeitraum zu verlängern, den er für seine eigenen Zwecke für angemessener hält.

## **Artikel 26 Informationspflicht der Anbieter von Datenverarbeitungsdiensten**

Der Anbieter von Datenverarbeitungsdiensten stellt dem Kunden Folgendes bereit:

- a) Informationen über die verfügbaren Verfahren für den Wechsel und die Übertragung von Inhalten auf den Datenverarbeitungsdienst, einschließlich Informationen über verfügbare Wechsel- und Übertragungsmethoden und -formate sowie über Einschränkungen und technische Beschränkungen, die dem Anbieter von Datenverarbeitungsdiensten bekannt sind;
- b) einen Verweis auf ein aktuelles Online-Register der Anbieter von Datenverarbeitungsdiensten mit Einzelheiten zu allen Datenstrukturen und Datenformaten sowie zu den einschlägigen Normen und offenen Interoperabilitätsspezifikationen, in denen die in Artikel 25 Absatz 2 Buchstabe e beschriebenen exportierbaren Daten verfügbar sind.

(95) Die Informationen, die Anbieter von Datenverarbeitungsdiensten Kunden bereitstellen müssen, könnten die Ausstiegsstrategie der Kunden unterstützen. Die Informationen sollten Folgendes umfassen: Verfahren für die Einleitung des Wechsels vom Datenverarbeitungsdienst, die maschinenlesbaren Datenformate, in die die Nutzerdaten exportiert werden können, die Instrumente für den Datenexport – einschließlich offener Schnittstellen – und Informationen zur Kompatibilität mit harmonisierten Normen oder gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen, Informationen über bekannte technische Beschränkungen und Einschränkungen, die sich auf den Vollzug des Wechsels auswirken könnten, und die geschätzte Zeit, die erforderlich ist, um den Wechsel zu vollziehen.

## **Artikel 27 Verpflichtung zum Handeln nach Treu und Glauben**

Alle Beteiligten, einschließlich der übernehmenden Anbieter von Datenverarbeitungsdiensten, arbeiten nach Treu und Glauben zusammen, damit der Wechsel effektiv vollzogen wird, Daten rechtzeitig übertragen werden können und die Kontinuität des Datenverarbeitungsdienstes aufrechterhalten wird.

(97) Um den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern, sollten alle beteiligten Parteien, einschließlich des ursprünglichen und des übernehmenden Anbieters von Datenverarbeitungsdiensten, nach Treu und Glauben zusammenarbeiten, um den Vollzug des Wechsels wirksam zu gestalten, und die sichere und fristgemäße Übertragung der erforderlichen Daten in einem gängigen, maschinenlesbaren Format über eine offene Schnittstelle zu ermöglichen und dabei die Dienstkontinuität zu wahren.

## **Artikel 28 Vertragliche Transparenzpflichten in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld**

- (1) Anbieter von Datenverarbeitungsdiensten stellen auf ihren Websites folgende Informationen bereit und halten diese Informationen auf dem neuesten Stand:
  - a) die Gerichtsbarkeit, der die IKT-Infrastruktur unterliegt, die für die Datenverarbeitung der einzelnen Dienste der Anbieter errichtet wurde;
  - b) eine allgemeine Beschreibung der technischen, organisatorischen und vertraglichen Maßnahmen, die der Anbieter von Datenverarbeitungsdiensten getroffen hat, um einen internationalen staatlichen Zugang zu oder eine internationale

staatliche Übermittlung von in der Union gespeicherten nicht-personenbezogenen Daten zu verhindern, wenn ein entsprechender Zugang oder eine entsprechende Übermittlung im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünde.

- (2) Die in Absatz 1 genannten Websites werden in dem Vertrag für alle Datenverarbeitungsdienste, die von Anbietern von Datenverarbeitungsdiensten angeboten werden, aufgeführt.

## **Artikel 29 Schrittweise Abschaffung von Wechselentgelten**

- (1) Ab dem 12. Januar 2027 dürfen Anbieter von Datenverarbeitungsdiensten für den Vollzug des Anbieterwechsels keine Wechselentgelte mehr erheben.
- (2) Vom 11. Januar 2024 bis zum 12. Januar 2027 dürfen Anbieter von Datenverarbeitungsdiensten bei den Kunden für den Vollzug des Wechsels ermäßigte Wechselentgelte erheben.
- (3) Die in Absatz 2 genannten ermäßigten Wechselentgelte dürfen die Kosten, die dem Anbieter von Datenverarbeitungsdiensten im unmittelbaren Zusammenhang mit dem betreffenden Wechsel entstehen, nicht übersteigen.

(89) Der ursprüngliche Anbieter von Datenverarbeitungsdiensten sollte bestimmte Aufgaben auslagern und Dritten für die Erfüllung der in dieser Verordnung festgelegten Verpflichtungen eine Gegenleistung erbringen können. Die Kosten für die vom ursprünglichen Anbieter von Datenverarbeitungsdiensten beschlossene Auslagerung von Diensten während des Vollzugs des Wechsels sollte nicht der Kunde tragen, und diese Kosten sollten als ungerechtfertigt gelten, es sei denn, sie decken Leistungen, die der Anbieter von Datenverarbeitungsdiensten auf Bitte des Kunden um zusätzliche Unterstützung beim Wechsel hin erbringt, die über die in dieser Verordnung ausdrücklich festgelegten Pflichten des Anbieters beim Wechsel hinausgehen. Diese Verordnung hindert Kunden nicht daran, Dritten für die Unterstützung im Migrationsprozess eine Gegenleistung zu erbringen, bzw. sie hindert Parteien nicht daran, im Einklang mit dem Unionsrecht oder dem nationalen Recht Verträge über Datenverarbeitungsdienste mit fester Laufzeit zu vereinbaren, einschließlich verhältnismäßiger Sanktionen für die vorzeitige Kündigung dieser Verträge. Zur Förderung des Wettbewerbs sollte die schrittweise Abschaffung der mit dem Wechsel von Datenverarbeitungsdiensten verbundenen Entgelte insbesondere die Abschaffung der Datenextraktionsentgelte umfassen, die von einem Anbieter von Datenverarbeitungsdiensten beim Kunden erhoben werden. Standarddienstentgelte für die Erbringung der Datenverarbeitungsdienste selbst sind keine Wechselentgelte. Diese Standarddienstentgelte sind nicht widerrufsfähig und gelten, bis der Vertrag über die Erbringung des betreffenden Dienstes nicht mehr gilt. Kunden können nach dieser Verordnung die Erbringung zusätzlicher Dienste verlangen, die über die nach dieser Verordnung bestehenden Pflichten des Anbieters beim Wechsel hinausgehen. Diese zusätzlichen Dienste können vom Anbieter erbracht und in Rechnung gestellt werden, wenn sie auf Verlangen des Kunden erbracht werden und der Kunde dem Preis dieser Dienste im Voraus zustimmt.

- (4) Vor dem Abschluss eines Vertrags mit einem Kunden unterrichten Anbieter von Datenverarbeitungsdiensten den potenziellen Kunden eindeutig über die möglicherweise erhobenen Standarddienstentgelte und die bei vorzeitiger Kündigung möglicherweise auferlegten Sanktionen sowie über die ermäßigten Wechselentgelte, die während des in Absatz 2 genannten Zeitrahmens erhoben werden könnten.

- (5) Gegebenenfalls stellen Anbieter von Datenverarbeitungsdiensten einem Kunden Informationen über Datenverarbeitungsdienste bereit, durch die der Wechsel sehr kompliziert oder kostspielig wird oder ohne nennenswerte Eingriffe in die Daten, digitalen Vermögenswerte oder die Dienstarchitektur unmöglich ist.
- (6) Anbieter von Datenverarbeitungsdiensten veröffentlichen die in den Absätzen 4 und 5 genannten Informationen für Kunden gegebenenfalls auf einem gesonderten Abschnitt ihrer Website oder auf eine andere leicht zugängliche Weise.
- (7) Der Kommission wird die Befugnis übertragen, gemäß Artikel 45 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, indem ein Überwachungsmechanismus eingerichtet wird, mit dem die Kommission die von Anbietern von Datenverarbeitungsdiensten auf dem Markt verlangten Wechselentgelte überwachen kann, um sicherzustellen, dass die Wechselentgelte gemäß den Absätzen 1 und 2 des vorliegenden Artikels innerhalb der in diesen Absätzen festgelegten Fristen abgeschafft und verringert werden.

### **Artikel 30 Technische Aspekte des Wechsels**

(94) Während des gesamten Vollzugs des Wechsels sollte ein hohes Maß an Sicherheit gewahrt werden. Das bedeutet, dass der ursprüngliche Anbieter von Datenverarbeitungsdiensten das Sicherheitsniveau, zu dem er sich in Bezug auf den Dienst verpflichtet hat, auf alle technischen Modalitäten – wie Netzverbindungen oder physische Geräte – ausdehnen sollte, für die er während des Vollzugs des Wechsels verantwortlich ist. 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 (31) eingeführt wurden, sollten davon unberührt bleiben. Die vorliegende Verordnung darf nicht so verstanden werden, dass ein Anbieter von Datenverarbeitungsdiensten daran gehindert wird, Kunden neue und verbesserte Dienste, Merkmale und Funktionen anzubieten oder auf dieser Grundlage mit anderen Anbietern von Datenverarbeitungsdiensten in Wettbewerb zu treten.

- (1) Was Datenverarbeitungsdienste für skalierbare und elastische Rechenressourcen betrifft, die auf Infrastrukturelemente wie Server, Netze und die für den Betrieb der Infrastruktur erforderlichen virtuellen Ressourcen beschränkt sind, aber keinen Zugang zu den Betriebsdiensten, zur Software und zu den Anwendungen gewähren, die auf diesen Infrastrukturelementen gespeichert sind, anderweitig verarbeitet oder eingesetzt werden, ergreifen Anbieter im Einklang mit Artikel 27 alle ihnen zur Verfügung stehenden angemessenen Maßnahmen, um zu ermöglichen, dass der Kunde, nachdem er zu einem Dienst der gleichen Dienstart gewechselt ist, bei der Nutzung des übernehmenden Datenverarbeitungsdienstes Funktionsäquivalenz erreicht. Der ursprüngliche Anbieter von Datenverarbeitungsdiensten ermöglicht den Wechsel, indem er Kapazitäten, angemessene Informationen, Dokumentationsmaterial, technische Unterstützung und gegebenenfalls die erforderlichen Instrumente bereitstellt.
- (2) Andere als die in Absatz 1 genannten Anbieter von Datenverarbeitungsdiensten stellen allen ihren Kunden und den betreffenden übernehmenden Anbietern von Datenverarbeitungsdiensten unentgeltlich offene Schnittstellen bereit, um den Wechsel zu ermöglichen. Diese Schnittstellen müssen ausreichende Informationen über den betreffenden

Dienst enthalten, damit die Software entwickelt werden kann, die für die Kommunikation mit den Diensten zu Zwecken der Datenübertragbarkeit und der Interoperabilität erforderlich ist.

(90) Um einer Bindung an bestimmte Anbieter zu Lasten des Wettbewerbs und der Entwicklung neuer Dienste entgegenzuwirken, bedarf es eines ambitionierten und innovationsfördernden regulatorischen Konzepts für Interoperabilität. Die Interoperabilität zwischen Datenverarbeitungsdiensten erfordert mehrere Schnittstellen und Infrastrukturebenen sowie Software und beschränkt sich selten auf die einfache Frage, ob sie erreicht werden kann oder nicht. Der Aufbau der nötigen Interoperabilität ist vielmehr von einer Kosten-Nutzen-Analyse abhängig, mit der ermittelt wird, ob es sinnvoll ist, die vernunftgemäß vorhersehbaren Ergebnisse anzustreben. Die Norm ISO/IEC 19941:2017 ist eine wichtige internationale Norm, die einen wichtigen Bezugspunkt hinsichtlich der Verwirklichung der Ziele dieser Verordnung bildet, da sie technische Erwägungen zur Klärung der Komplexität eines solchen Verfahrens umfasst.

- (3) Bei anderen als den in Absatz 1 des vorliegenden Artikels genannten Datenverarbeitungsdiensten gewährleisteten Anbieter von Datenverarbeitungsdiensten die Kompatibilität mit gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen oder harmonisierter Interoperabilitätsnormen, und zwar mindestens zwölf Monate, nachdem die Bezugnahmen auf diese gemeinsamen Interoperabilitätsspezifikationen oder harmonisierten Normen für die Interoperabilität von Datenverarbeitungsdiensten – im Anschluss an die Veröffentlichung der zugrunde liegenden Durchführungsrechtsakte im Amtsblatt der Europäischen Union – in der zentralen Datenbank der Union für Normen für Datenverarbeitungsdienste im Einklang mit Artikel 35 Absatz 8 veröffentlicht wurden.
- (4) Anbieter von Datenverarbeitungsdiensten, die nicht in Absatz 1 dieses Artikels genannt sind, aktualisieren das in Artikel 26 Buchstabe b genannte Online-Register im Einklang mit ihren Verpflichtungen gemäß Absatz 3 des vorliegenden Artikels.
- (5) Im Falle eines Wechsels zwischen Diensten der gleichen Dienstart, für die in der zentralen Datenbank der Union für die Interoperabilität von Datenverarbeitungsdiensten gemäß Artikel 35 Absatz 8 keine gemeinsamen Spezifikationen oder die in Absatz 3 des vorliegenden Artikels genannten harmonisierten Normen für die Interoperabilität veröffentlicht wurden, exportiert der Anbieter der Datenverarbeitungsdienste auf Verlangen des Kunden alle exportierbaren Daten in einem strukturierten, gängigen und maschinenlesbaren Format.
- (6) Anbieter von Datenverarbeitungsdiensten sind nicht verpflichtet, neue Technologien oder Dienste zu entwickeln oder digitale Vermögenswerte, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis darstellen, gegenüber einem Kunden oder einem anderen Anbieter von Datenverarbeitungsdiensten offenzulegen oder die Sicherheit und Integrität des Kunden oder Anbieters zu beeinträchtigen.

### **Artikel 31 Spezifische Regelung für bestimmte Datenverarbeitungsdienste**

- (1) Die in Artikel 23 Buchstabe d, Artikel 29 und Artikel 30 Absätze 1 und 3 festgelegten Verpflichtungen gelten nicht für Datenverarbeitungsdienste, bei denen die meisten zentralen Funktionen auf die spezifischen Bedürfnisse eines einzelnen Kunden zuge-

schnitten wurden, oder wenn alle Komponenten für die Zwecke eines einzelnen Kunden entwickelt wurden und wenn diese Datenverarbeitungsdienste nicht im größeren kommerziellen Maßstab über den Dienstleistungskatalog der Anbieter von Datenverarbeitungsdiensten angeboten werden.

(98) Datenverarbeitungsdienste für Dienste, bei denen die meisten Hauptmerkmale speziell auf konkrete Vorgaben eines einzelnen Kunden zugeschnitten sind oder bei denen alle Komponenten für die Zwecke eines einzelnen Kunden entwickelt wurden, sollten von einigen der für den Wechsel zwischen Datenverarbeitungsdiensten geltenden Verpflichtungen ausgenommen werden. Dienste, die der Anbieter von Datenverarbeitungsdiensten über seinen Dienstleistungskatalog im großen kommerziellen Maßstab anbietet, sollten nicht dazu gehören. Es gehört zu den Verpflichtungen des Anbieters von Datenverarbeitungsdiensten, potenzielle Kunden solcher Dienste vor Abschluss eines Vertrags ordnungsgemäß über diejenigen in dieser Verordnung festgelegten Verpflichtungen zu informieren, die nicht für die betreffenden Dienste gelten. Der Anbieter von Datenverarbeitungsdiensten ist nicht daran gehindert, solche Dienste letztlich in großem Maßstab einzuführen; in diesem Fall müsste er jedoch alle in dieser Verordnung festgelegten Verpflichtungen für den Wechsel erfüllen.

- (2) Die in diesem Kapitel festgelegten Verpflichtungen gelten nicht für Datenverarbeitungsdienste, die nicht als Vollversion, sondern zu Test- und Bewertungszwecken und für einen begrenzten Zeitraum bereitgestellt werden.
- (3) Vor dem Abschluss eines Vertrags über die Erbringung der in diesem Artikel genannten Datenverarbeitungsdienste unterrichtet der Anbieter von Datenverarbeitungsdiensten den potenziellen Kunden über die Verpflichtungen aus diesem Kapitel, die nicht gelten.

## **Kapitel VII Unrechtmässiger staatlicher Zugang zu und unrechtmässige staatliche Übermittlung von nicht-personenbezogenen Daten im internationalen Umfeld**

### **Artikel 32 Staatlicher Zugang und staatliche Übermittlung im internationalen Umfeld**

- (1) Unbeschadet der Absätze 2 oder 3 treffen Anbieter von Datenverarbeitungsdiensten alle angemessenen technischen, organisatorischen und rechtlichen Maßnahmen, einschließlich Verträgen, um den staatlichen Zugang zu und die staatliche Übermittlung von in der Union gespeicherten nicht-personenbezogenen Daten im internationalen Umfeld und durch Drittländer zu verhindern, wenn dies im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stehen würde.
- (2) Für jegliche Entscheidung bzw. jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, die Anbieter von

Datenverarbeitungsdiensten auffordern, in den Anwendungsbereich dieser Verordnung fallende nicht-personenbezogene Daten zu übermitteln oder Zugang zu diesen Daten zu gewähren, gilt, dass sie unabhängig von der Art und Weise nur anerkannt werden bzw. vollstreckbar sind, wenn sie auf einer rechtskräftigen internationalen Übereinkunft, etwa auf einem Rechtshilfeabkommen zwischen dem anfragenden Drittland und der Union oder einer solcher Übereinkunft zwischen dem anfragenden Drittland und einem Mitgliedstaat, beruhen.

- (3) Wenn keine internationale Übereinkunft gemäß Absatz 2 besteht und an einen Anbieter von Datenverarbeitungsdiensten eine Entscheidung bzw. ein Urteil eines Gerichts eines Drittlands oder eine Entscheidung einer Verwaltungsbehörde eines Drittlands ergeht, wonach unter diese Verordnung fallende in der Union gespeicherte nicht-personenbezogene Daten zu übermitteln sind oder Zugang zu diesen Daten zu gewähren ist, und der Adressat eines solchen Urteils oder einer solchen Entscheidung im Falle der Folgeleistung gegen das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats verstoßen würde, erfolgt die Übermittlung von oder die Gewährung des Zugangs zu diesen Daten an bzw. für die betreffende Drittlandsbehörde nur, wenn
- a) das Rechtssystem des Drittlands vorschreibt, dass die Entscheidung oder das Urteil zu begründen ist und verhältnismäßig sein muss, und vorsieht, dass die Entscheidung oder das Urteil eine hinreichende Bestimmtheit aufweisen muss, indem darin z. B. eine hinreichende Bezugnahme auf bestimmte verdächtige Personen oder Rechtsverletzungen erfolgt,
  - b) der begründete Einwand des Adressaten von einem zuständigen Gericht des Drittlands überprüft wird und
  - c) das zuständige Gericht des Drittlands, das die Entscheidung oder das Urteil erlässt oder die Entscheidung einer Verwaltungsbehörde überprüft, nach dem Recht dieses Drittlands 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 oder des Urteils kann die Stellungnahme der zuständigen nationalen Stelle oder der für die internationale Zusammenarbeit in Rechtssachen zuständigen Behörde einholen, um festzustellen, ob die in Unterabsatz 1 festgelegten Bedingungen erfüllt sind, insbesondere wenn er der Auffassung ist, dass die Entscheidung möglicherweise Geschäftsgeheimnisse und andere sensible Geschäftsdaten sowie Inhalte, die durch Rechte des geistigen Eigentums geschützt sind, betrifft oder die Übermittlung eine Re-Identifikation ermöglichen könnte. Die zuständige nationale Stelle oder Behörde kann die Kommission konsultieren. Ist der Adressat der Auffassung, dass die Entscheidung oder das Urteil die nationale Sicherheit oder die Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten beeinträchtigen könnte, so holt er die Stellungnahme der einschlägigen nationalen Stellen oder Behörden ein, um festzustellen, ob die verlangten Daten die nationale Sicherheit oder die Verteidigungsinteressen der Union oder ihrer Mitgliedstaaten betreffen. Hat der Adressat binnen eines Monats keine Antwort erhalten oder gelangt eine solche Stelle oder Behörde in ihrer Stellungnahme zu dem Schluss, dass die in Unterabsatz 1 festgelegten Bedingungen nicht erfüllt sind, so kann der Adressat die Aufforderung zur Übermittlung von oder zum Zugang zu nicht-personenbezogenen Daten aus diesen Gründen ablehnen.

Der in Artikel 42 genannte EDIB berät und unterstützt die Kommission bei der Ausarbeitung von Leitlinien für die Bewertung, ob die in Unterabsatz 1 dieses Absatzes genannten Bedingungen erfüllt sind.

- (4) Sind die Voraussetzungen nach Absatz 2 oder Absatz 3 erfüllt, so stellt der Anbieter von Datenverarbeitungsdiensten die Mindestmenge an Daten bereit, die auf der Grundlage einer angemessenen Auslegung dieses Verlangens durch den Anbieter oder die in Absatz 3 Unterabsatz 2 genannte einschlägige nationale Stelle oder Behörde als Reaktion auf das Verlangen zulässig ist.
- (5) Der Anbieter von Datenverarbeitungsdiensten teilt dem Kunden mit, dass für seine Daten ein Datenzugangsverlangen einer Behörde eines Drittlands vorliegt, bevor er das Verlangen erfüllt, außer in Fällen, in denen das Verlangen Strafverfolgungszwecken dient und solange zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahmen erforderlich ist.

(101) Drittländer können Gesetze, Verordnungen und sonstige Rechtsakte erlassen, die darauf ausgerichtet sind, dass nicht-personenbezogene Daten, die – auch in der Union – außerhalb der Landesgrenzen gespeichert sind, übertragen werden können bzw. staatliche Stellen direkten Zugang zu solchen Daten haben. In Drittländern ergangene Gerichtsurteile oder Entscheidungen anderer Justiz- oder Verwaltungsbehörden, einschließlich Strafverfolgungsbehörden, mit denen eine solche Übertragung von oder ein solcher Zugang zu nicht-personenbezogenen Daten gefordert wird, sollten vollstreckbar sein, wenn sie sich auf eine internationale Vereinbarung, etwa ein Rechtshilfeabkommen, stützen, das zwischen dem anfragenden Drittland und der Union oder einem Mitgliedstaat besteht. Mitunter kann es auch dazu kommen, dass die sich aus dem Recht eines Drittlands ergebende Verpflichtung zur Übertragung von oder Gewährung des Zugangs zu nicht-personenbezogenen Daten einer nach Unionsrecht oder nach dem nationalen Recht des betreffenden Mitgliedstaats bestehenden Verpflichtung zum Schutz dieser Daten entgegensteht, insbesondere, was den Schutz der Grundrechte des Einzelnen, wie das Recht auf Sicherheit und das Recht auf einen wirksamen Rechtsbehelf, oder die grundlegenden Interessen eines Mitgliedstaats im Zusammenhang mit der nationalen Sicherheit oder Verteidigung sowie den Schutz sensibler Geschäftsdaten, einschließlich des Schutzes des Geschäftsgeheimnisses, und den Schutz von Rechten des geistigen Eigentums, darunter auch vertragliche Vertraulichkeitspflichten nach einem solchen Gesetz, betrifft. Besteht keine internationale Vereinbarung zur Regelung dieser Fragen, so sollte die Übertragung von oder der Zugang zu nicht-personenbezogenen Daten nur gestattet sein, wenn überprüft wurde, dass das Rechtssystem des betreffenden Drittlands die Begründung und die Verhältnismäßigkeit sowie die hinreichende Bestimmtheit der gerichtlichen Anordnung oder Entscheidung vorschreibt und dem Adressaten die Möglichkeit einräumt, dem zuständigen Gericht des Drittlands, das zur gebührenden Berücksichtigung der einschlägigen rechtlichen Interessen des Bereitstellers der Daten befugt ist, seinen begründeten Einwand zur Überprüfung vorzulegen. Nach Möglichkeit sollte der Anbieter von Datenverarbeitungsdiensten den Kunden, dessen Daten verlangt werden, im Rahmen des Datenzugangsverlangens der Behörde des Drittlands vor der Gewährung des Zugangs zu diesen Daten unterrichten können, um zu überprüfen, ob ein solcher Zugang möglicherweise gegen Unionsrecht oder nationales Recht verstößt, wie etwa ein solches über den Schutz sensibler Geschäftsdaten, einschließlich des Schutzes des Geschäftsgeheimnisses und der Rechte des geistigen Eigentums sowie vertraglicher Vertraulichkeitspflichten.

(102) Um das Vertrauen in Daten weiter zu stärken, ist es wichtig, dass Schutzvorkehrungen, die Unionsbürgern, der öffentlichen Hand und Unternehmen die Kontrolle über ihre Daten gewährleisten sollen, so weit wie möglich umgesetzt werden. Darüber

hinaus sollten das Recht, die Werte und die Standards der Union unter anderem in Bezug auf Sicherheit, Datenschutz und Privatsphäre sowie Verbraucherschutz gewahrt werden. Um einen unrechtmäßigen staatlichen Zugang der Behörden von Drittländern zu nicht-personenbezogenen Daten zu verhindern, sollten dieser Verordnung unterliegende Anbieter von Datenverarbeitungsdiensten wie Cloud- und Edge-Diensten alle zumutbaren Maßnahmen ergreifen, um den Zugang zu Systemen zu verhindern, in denen nicht-personenbezogenen Daten gespeichert werden, gegebenenfalls auch durch die Verschlüsselung von Daten, häufige Audits, die Überprüfung der Einhaltung der einschlägigen Systeme für die Sicherheitszertifizierung und die Änderung der Unternehmenspolitik.

## Kapitel VIII Interoperabilität

### **Artikel 33 Wesentliche Anforderungen an die Interoperabilität von Daten, von Mechanismen und Diensten für die Datenweitergabe sowie von gemeinsamen europäischen Datenräumen**

- (1) Teilnehmer an Datenräumen, die anderen Teilnehmern Daten oder Datendienste anbieten, müssen die folgenden wesentlichen Anforderungen zur Erleichterung der Interoperabilität von Daten, von Mechanismen und Diensten für die Datenweitergabe sowie von gemeinsamen europäischen Datenräumen erfüllen, bei denen es sich um zweck- oder sektorspezifische oder sektorübergreifende interoperable Rahmen für gemeinsame Normen und Verfahren für die Weitergabe oder die gemeinsame Verarbeitung von Daten – unter anderem für die Entwicklung neuer Produkte und Dienste, wissenschaftliche Forschung oder Initiativen der Zivilgesellschaft – handelt:
- a) Datensatzinhalte, Nutzungsbeschränkungen, Lizenzen, Datenerhebungsmethoden, Datenqualität und Unsicherheiten sind – gegebenenfalls 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, sofern verfügbar, werden in einer öffentlich verfügbaren und einheitlichen Weise beschrieben;
  - c) die technischen Mittel für den Datenzugang, wie etwa Anwendungsprogrammierschnittstellen, sowie ihre Nutzungsbedingungen und die Dienstqualität sind ausreichend beschrieben, um den automatischen Datenzugang und die automatische Datenübermittlung zwischen den Parteien, auch kontinuierlich, im Massendownload oder in Echtzeit in einem maschinenlesbaren Format zu ermöglichen, sofern dies technisch machbar ist und das reibungslose Funktionieren des vernetzten Produkts nicht beeinträchtigt;
  - d) es werden gegebenenfalls die Mittel bereitgestellt, mit denen die Interoperabilität von Tools für die Automatisierung der Ausführung von Verträgen über die Datenweitergabe, wie intelligenten Verträgen, ermöglicht wird.

Die Anforderungen können allgemeiner Art sein oder bestimmte Sektoren betreffen, müssen aber die Wechselwirkungen mit Anforderungen aus anderem Unionsrecht oder aus nationalem Recht in vollem Umfang berücksichtigen.

- (2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 45 dieser Verordnung delegierte Rechtsakte zur Ergänzung dieser Verordnung durch die nähere Bestimmung der in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen zu erlassen, und zwar in Bezug auf diejenigen Anforderungen, die naturgemäß nicht die beabsichtigte Wirkung entfalten können, sofern sie nicht in verbindlichen Rechtsakten der Union näher spezifiziert werden, und mit Ziel, den technologischen Entwicklungen und Marktentwicklungen angemessen Rechnung zu tragen.

Die Kommission berücksichtigt den Rat des EDIB gemäß Artikel 42 Buchstabe c, wenn sie delegierte Rechtsakte erlässt.

- (3) Bei Teilnehmern an Datenräumen, die Daten oder Datendienste für andere Teilnehmer an Datenräumen anbieten, die ganz oder teilweise den harmonisierten Normen entsprechen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht werden, wird die Konformität mit den in Absatz 1 festgelegten wesentlichen Anforderungen vermutet, soweit diese Anforderungen durch diese harmonisierten Normen oder Teile dieser harmonisierten Normen erfasst werden.
- (4) Die Kommission beauftragt gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit, Entwürfe für harmonisierte Normen zu erarbeiten, die den in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen genügen.
- (5) Die Kommission kann im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen erlassen, die einige oder alle in Absatz 1 festgelegten wesentlichen Anforderungen erfassen, sofern folgende Voraussetzungen erfüllt sind:
- a) Die Kommission hat gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragt, eine harmonisierte Norm zu erarbeiten, die den in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen genügt, und
- (i) i) der Auftrag wurde entweder nicht angenommen,
  - (ii) ii) die harmonisierten Normen für diesen Auftrag sind nicht innerhalb der gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 gesetzten Frist vorgelegt worden oder
  - (iii) iii) die harmonisierten Normen erfüllen den Auftrag nicht, und
- b) im Amtsblatt der Europäischen Union ist für die harmonisierten Normen, die die einschlägigen, in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen erfassen, keine Fundstelle gemäß der Verordnung (EU) Nr. 1025/2012 veröffentlicht, und wird eine solche Fundstelle voraussichtlich auch nicht innerhalb einer angemessenen Frist veröffentlicht werden.

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

- (6) Vor der Ausarbeitung eines Entwurfs des in Absatz 5 des vorliegenden Artikels genannten Durchführungsrechtsakts teilt die Kommission dem in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss mit, dass die Bedingungen von Absatz 5 des vorliegenden Artikels ihres Erachtens erfüllt sind.
- (7) Bei der Ausarbeitung des Entwurfs des in Absatz 5 genannten Durchführungsrechtsakts berücksichtigt die Kommission den Rat des EDIB und die Standpunkte anderer einschlägiger Gremien oder Expertengruppen und konsultiert ordnungsgemäß alle einschlägigen Interessenträger.
- (8) Bei Teilnehmern an Datenräumen, die Daten oder Datendienste für andere Teilnehmer an Datenräumen anbieten, die ganz oder teilweise den gemeinsamen Spezifikationen entsprechen, die gemäß den in Absatz 5 genannten Durchführungsrechtsakten festgelegt wurden, wird die Konformität mit den in Absatz 1 festgelegten wesentlichen Anforderungen vermutet, soweit diese Anforderungen ganz oder teilweise durch diese gemeinsamen Spezifikationen erfasst werden.
- (9) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission für die Zwecke der Veröffentlichung ihrer Fundstelle im Amtsblatt der Europäischen Union vorgeschlagen, so bewertet die Kommission die harmonisierte Norm gemäß der Verordnung (EU) Nr. 1025/2012. Wird die Fundstelle einer harmonisierten Norm im Amtsblatt der Europäischen Union veröffentlicht, so werden die in Absatz 5 des vorliegenden Artikels genannten Durchführungsrechtsakte, die dieselben wesentlichen Anforderungen erfassen, wie sie von dieser harmonisierten Norm erfasst sind, von der Kommission ganz oder teilweise aufgehoben.
- (10) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den in Absatz 1 festgelegten wesentlichen Anforderungen nicht vollständig entspricht, so setzt er die Kommission durch die Übermittlung einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die ausführliche Erläuterung und kann gegebenenfalls den Durchführungsrechtsakt ändern, durch den die fragliche gemeinsame Spezifikation festgelegt wurde.
- (11) Die Kommission kann unter Berücksichtigung des Vorschlags des EDIB gemäß Artikel 30 Buchstabe h der Verordnung (EU) 2022/868 zur Festlegung von interoperablen Rahmen für gemeinsame Normen und Verfahren für das Funktionieren gemeinsamer europäischer Datenräume Leitlinien annehmen.

(103) Normung und semantische Interoperabilität sollten eine wichtige Rolle bei der Bereitstellung technischer Lösungen zur Gewährleistung der Interoperabilität innerhalb von und zwischen gemeinsamen europäischen Datenräumen spielen, bei denen es sich um zweck- oder sektorspezifische oder sektorübergreifende interoperable Rahmen für gemeinsame Normen und Verfahren für die Weitergabe oder die gemeinsame Verarbeitung von Daten, unter anderem für die Entwicklung neuer Produkte und Dienste, wissenschaftliche Forschung oder zivilgesellschaftliche Initiativen, handelt. In dieser Verordnung sollten bestimmte wesentliche Interoperabilitätsanforderungen festgelegt werden. Teilnehmer an Datenräumen, die anderen Teilnehmern Daten oder Datendienste anbieten und bei denen es sich um Stellen handelt, die die Weitergabe von Daten innerhalb gemeinsamer europäischer Datenräume erleichtern oder daran beteiligt sind, einschließlich Dateninhaber, sollten diese Anforderungen erfüllen, soweit sie Elemente betreffen, die ihrer Kontrolle unterliegen. Die Einhaltung dieser Vorschriften kann durch die Einhaltung der in dieser Verordnung festgelegten wesentlichen Anforderungen gewährleistet oder aufgrund der Einhaltung von har-

monisierten Normen oder gemeinsamen Spezifikationen im Rahmen einer Konformitätsvermutung vermutet werden. Um die Konformität mit den Interoperabilitätsanforderungen zu erleichtern, muss eine Konformitätsvermutung für die Interoperabilitätslösungen vorgesehen werden, die ganz oder teilweise den harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 entsprechen, welche den Standardrahmen für die Erarbeitung der Normen, nach denen solche Konformitätsvermutungen vorgesehen werden, bildet. Die Kommission sollte die Hindernisse für die Interoperabilität bewerten und den Normungsbedarf priorisieren, sodass sie auf dieser Grundlage gemäß der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen kann, Entwürfe für harmonisierte Normen zu erarbeiten, die die in der vorliegenden Verordnung festgelegten wesentlichen Anforderungen erfüllen. Führen solche Aufträge nicht zu harmonisierten Normen oder reichen solche harmonisierten Normen nicht aus, um die Konformität mit den wesentlichen Anforderungen der vorliegenden Verordnung zu gewährleisten, so sollte die Kommission, sofern sie dabei die Rolle und die Funktionen der Normungsorganisationen gebührend achtet, in der Lage sein, gemeinsame Spezifikationen in den genannten Bereichen zu erlassen. Gemeinsame Spezifikationen sollten nur als außergewöhnliche Ausweichlösung erlassen werden, um die Einhaltung der wesentlichen Anforderungen dieser Verordnung zu erleichtern, oder wenn der Normungsprozess blockiert ist, oder bei Verzögerungen bei der Festlegung geeigneter harmonisierter Normen. Ist eine Verzögerung auf die technische Komplexität der betreffenden Norm zurückzuführen, so sollte die Kommission dies berücksichtigen, bevor sie die Festlegung gemeinsamer Spezifikationen in Erwägung zieht. Gemeinsame Spezifikationen sollten offen und inklusiv erarbeitet werden und gegebenenfalls dem Rat des gemäß der Verordnung (EU) 2022/868 eingerichteten Europäischen Dateninnovationsrates (EDIB) Rechnung tragen. Darüber hinaus könnten in den verschiedenen Sektoren – auf der Grundlage ihrer jeweiligen besonderen Bedürfnisse – auch gemeinsame Spezifikationen im Einklang mit Unionsrecht oder nationalem Recht erlassen werden. Darüber hinaus sollte die Kommission in die Lage versetzt werden, die Erarbeitung harmonisierter Normen für die Interoperabilität von Datenverarbeitungsdiensten in Auftrag zu geben.

## **Artikel 34 Interoperabilität zu Zwecken der parallelen Nutzung von Datenverarbeitungsdiensten**

- (1) Die in Artikel 23, Artikels 24, Artikels 25 Absatz 2 Buchstabe a Ziffern ii und iv und Buchstaben e und f sowie Artikel 30 Absätze 2, 3, 4 und 5 festgelegten Anforderungen gelten entsprechend auch für Anbieter von Datenverarbeitungsdiensten, um die Interoperabilität zu Zwecken der parallelen Nutzung von Datenverarbeitungsdiensten zu erleichtern.
- (2) Wenn ein Datenverarbeitungsdienst parallel mit einem anderen Datenverarbeitungsdienst genutzt wird, können die Anbieter von Datenverarbeitungsdiensten Datenextraktionsentgelte verlangen, aber nur zur Weitergabe der entstandenen Extraktionskosten, ohne diese Kosten zu übersteigen.

(99) Im Einklang mit der Mindestanforderung, den Wechsel von Anbietern von Datenverarbeitungsdiensten zu ermöglichen, zielt diese Verordnung auch darauf ab, die Interoperabilität für die parallele Nutzung mehrerer Datenverarbeitungsdienste durch ergänzende Funktionen zu verbessern. Dies betrifft Situationen, in denen Kunden einen Vertrag im Hinblick auf den Wechsel zu einem anderen Anbieter von Datenverarbeitungsdiensten nicht kündigen, sondern mehrere Dienste verschiedener Anbieter parallel und interoperabel genutzt werden, um die ergänzenden Funktionen der verschiedenen Dienste in der Systemkonfiguration des Kunden nutzen zu können. Im Gegensatz zu der einmaligen Extraktion, die beim Vollzug eines Wechsels erforder-

lich ist, kann die Datenextraktion von einem zu einem anderen Anbieter von Datenverarbeitungsdiensten mit dem Ziel, die parallele Nutzung von Diensten zu erleichtern, jedoch bekanntlich ein fortlaufender Vorgang sein. Anbieter von Datenverarbeitungsdiensten sollten daher für die Datenextraktion zu Zwecken der parallelen Nutzung nach drei Jahren nach dem Tag des Inkrafttretens der vorliegenden Verordnung weiterhin Datenextraktionsentgelte erheben können, die die anfallenden Kosten nicht übersteigen. Dies ist unter anderem für die erfolgreiche Einführung von Multi-Cloud-Strategien wichtig, die es Kunden ermöglichen, zukunftssichere IT-Strategien umzusetzen, und die Abhängigkeit von einzelnen Anbietern von Datenverarbeitungsdiensten verringern. Durch die Erleichterung eines Multi-Cloud-Ansatzes für Kunden von Datenverarbeitungsdiensten kann außerdem – wie in der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (32) in Bezug auf Anbieter von Finanzdienstleistungen festgestellt – dazu beigetragen werden, die Betriebsstabilität der digitalen Systeme der Kunden zu stärken.

## **Artikel 35 Interoperabilität von Datenverarbeitungsdiensten**

- (1) Offene Interoperabilitätsspezifikationen und harmonisierte Normen für die Interoperabilität von Datenverarbeitungsdiensten
  - a) bewirken, soweit dies technisch machbar ist, die Interoperabilität zwischen verschiedenen Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;
  - b) verbessern die Übertragbarkeit digitaler Vermögenswerte zwischen verschiedenen Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;
  - c) erleichtern, soweit dies technisch machbar ist, die Funktionsäquivalenz zwischen den in Artikel 30 Absatz 1 genannten Datenverarbeitungsdiensten, die die gleiche Dienstart abdecken;
  - d) beeinträchtigen Sicherheit und Integrität der Datenverarbeitungsdienste und Daten nicht;
  - e) sind für die Möglichkeit einer technischen Aufrüstung und die Einbindung neuer Funktionen und Innovationen in Datenverarbeitungsdiensten ausgelegt.
- (2) Offene Interoperabilitätsspezifikationen und harmonisierte Normen für die Interoperabilität von Datenverarbeitungsdiensten müssen Folgendes angemessen regeln:
  - a) die Aspekte der Cloud-Interoperabilität in Bezug auf die Transportinteroperabilität, die syntaktische Interoperabilität, die semantische Dateninteroperabilität, die verhaltensbezogene Interoperabilität und die Interoperabilität der Regeln und Vorgaben;
  - b) die Aspekte der Cloud-Datenübertragbarkeit in Bezug auf die syntaktische Datenübertragbarkeit, die semantische Datenübertragbarkeit und die Übertragbarkeit der Datenregeln;
  - c) die Aspekte der Cloud-Anwendungen in Bezug auf die syntaktische Übertragbarkeit von Anwendungen, die Übertragbarkeit von Anwendungsbefehlen, die Übertragbarkeit von Anwendungsmetadaten, die Übertragbarkeit des Anwendungsverhaltens und die Übertragbarkeit der Anwendungsregeln.
- (3) Offene Interoperabilitätsspezifikationen müssen Anhang II der Verordnung (EU) Nr. 1025/2012 entsprechen.

- (4) Nach Berücksichtigung einschlägiger internationaler und europäischer Normen und Selbstregulierungsinitiativen kann die Kommission gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragen, Entwürfe für harmonisierte Normen, die in den Absätzen 1 und 2 des vorliegenden Artikels festgelegten wesentlichen Anforderungen genügen, zu erarbeiten.
- (5) Die Kommission kann im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen festlegen, die alle in den Absätzen 1 und 2 des vorliegenden Artikels festgelegten wesentlichen Anforderungen erfassen.
- (6) Die Kommission berücksichtigt bei der Ausarbeitung des in Absatz 5 dieses Artikels genannten Entwurfs des Durchführungsrechtsakts die Standpunkte der in Artikel 37 Absatz 5 Buchstabe h genannten einschlägigen zuständigen Behörden sowie anderer einschlägiger Gremien oder Expertengruppen und konsultiert ordnungsgemäß alle einschlägigen Interessenträger.
- (7) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den wesentlichen Anforderungen gemäß den Absätzen 1 und 2 nicht vollständig entspricht, so setzt er die Kommission durch Übermittlung einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die ausführliche Erläuterung und kann gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde, ändern.
- (8) Für die Zwecke des Artikels 30 Absatz 3 veröffentlicht die Kommission im Wege von Durchführungsrechtsakten die Fundstellen harmonisierter Normen und gemeinsamer Spezifikationen für die Interoperabilität von Datenverarbeitungsdiensten in einer zentralen Datenbank der Union für Normen für die Interoperabilität von Datenverarbeitungsdiensten.
- (9) Die in diesem Artikel genannten Durchführungsrechtsakte werden gemäß dem in Artikel 46 Absatz 2 genannten Prüfverfahren erlassen.

(100) Offene Interoperabilitätsspezifikationen und -normen, die gemäß Anhang II der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates (33) im Bereich der Interoperabilität und Übertragbarkeit entwickelt wurden, werden voraussichtlich eine Cloud-Umgebung mit mehreren Anbietern ermöglichen, was eine wesentliche Voraussetzung für offene Innovation in der europäischen Datenwirtschaft ist. Da die Akzeptanz festgelegter Normen auf dem Markt im Rahmen der 2016 abgeschlossenen Initiative zur Koordinierung der Cloud-Normung (CSC) zurückhaltend ausfiel, muss sich die Kommission auch darauf verlassen, dass die Marktteilnehmer einschlägige offene Interoperabilitätsspezifikationen entwickeln, um mit dem raschen technologischen Fortschritt in dieser Branche Schritt zu halten. Solche offenen Interoperabilitätsspezifikationen können dann von der Kommission in Form gemeinsamer Spezifikationen erlassen werden. Wenn ferner nicht nachgewiesen wurde, dass gemeinsame Spezifikationen oder Normen, die eine wirksame Cloud-Interoperabilität der Verarbeitung von Daten auf PaaS- und SaaS-Ebene erleichtern, durch marktgesteuerte Verfahren festgelegt werden können, sollte die Kommission auf der Grundlage der vorliegenden Verordnung und im Einklang mit der Verordnung (EU) Nr. 1025/2012 in der Lage sein, europäische Normungsgremien mit der Entwicklung solcher Normen für bestimmte Dienstanbieter zu beauftragen, für die solche Normen noch nicht existieren. Darüber hinaus wird die Kommission die Marktteilnehmer anhalten, einschlägige offene Interoperabilitätsspezifikationen zu entwickeln. Im Anschluss an eine Konsultation der Interessenträger sollte die Kommission im Wege von Durchführungsrechtsakten durch

einen Verweis in einer zentralen Datenbank der Union für Normen für die Interoperabilität von Datenverarbeitungsdiensten vorschreiben können, dass für bestimmte Dienstanbieter harmonisierte Normen für die Interoperabilität oder gemeinsame Interoperabilitätsspezifikationen verwendet werden. Anbieter von Datenverarbeitungsdiensten sollten die Kompatibilität mit diesen harmonisierten Normen und gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen sicherstellen, die die Sicherheit oder die Integrität der Daten nicht beeinträchtigen sollten. Auf harmonisierte Normen für die Interoperabilität von Datenverarbeitungsdiensten und gemeinsame Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen wird nur verwiesen, wenn sie den in dieser Verordnung festgelegten Kriterien entsprechen, die denselben Stellenwert haben wie die Anforderungen in Anhang II der Verordnung (EU) Nr. 1025/2012 und die in der internationalen Norm ISO/IEC 19941:2017 definierten Interoperabilitätsaspekte. Darüber hinaus sollte bei der Normung den Bedürfnissen von KMU Rechnung getragen werden.

### **Artikel 36 Wesentliche Anforderungen an intelligente Verträge für die Ausführung von Datenweitergabevereinbarungen**

- (1) Der Anbieter einer Anwendung, in der intelligente Verträge verwendet werden, oder – in dessen Ermangelung – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit der vollständigen oder teilweisen Ausführung einer Datenbereitstellungsvereinbarung beinhaltet, muss sicherstellen, dass diese intelligenten Verträge die folgenden wesentlichen Anforderungen erfüllen:
  - a) Robustheit und Zugangskontrolle, zur Gewährleistung, dass der intelligente Vertrag so konzipiert wurde, dass er Zugangskontrollmechanismen und ein sehr hohes Maß an Robustheit bietet, um Funktionsfehler zu vermeiden und Manipulationen durch Dritte standzuhalten;
  - b) sichere Beendigung und Unterbrechung, zur Gewährleistung, dass es einen Mechanismus gibt, mit dem die weitere Ausführung von Transaktionen beendet werden kann und dass der intelligente Vertrag interne Funktionen enthält, mit denen der Vertrag zurückgesetzt oder die Anweisung ausgegeben werden kann, den Betrieb zu beenden oder zu unterbrechen, insbesondere um eine künftige unbeabsichtigte Ausführung zu vermeiden;
  - c) Datenarchivierung und Datenkontinuität, zur Gewährleistung, dass in Situationen, in denen ein intelligenter Vertrag beendet oder deaktiviert werden muss, ist die Möglichkeit der Archivierung der Transaktionsdaten, der Logik und des Programmcodes des intelligenten Vertrags besteht, damit Aufzeichnungen über Vorgänge vorliegen (Prüfbarkeit), die in der Vergangenheit mit den Daten durchgeführt wurden,
  - d) Zugangskontrolle, zur Gewährleistung, dass ein intelligenter Vertrag durch strenge Zugangskontrollmechanismen auf der Governance-Ebene und der Ebene des intelligenten Vertrags geschützt ist, und
  - e) Kohärenz, zur Gewährleistung der Übereinstimmung mit den Bedingungen der Datenweitergabevereinbarung, die mit dem intelligenten Vertrag umgesetzt wird.
- (2) Der Anbieter eines intelligenten Vertrags oder – in dessen Ermangelung – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter

Verträge für Dritte im Zusammenhang mit einer Durchführung einer Datenbereitstellungsvereinbarung oder Teilen davon beinhaltet, führt im Hinblick auf die Erfüllung der in Absatz 1 festgelegten wesentlichen Anforderungen eine Konformitätsbewertung durch und stellt bei Erfüllung dieser Anforderungen eine EU-Konformitätserklärung aus.

- (3) Mit der Ausstellung der EU-Konformitätserklärung übernimmt der Anbieter einer Anwendung, in der intelligente Verträge verwendet werden, oder – in dessen Ermangelung – die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit der Durchführung einer Datenbereitstellungsvereinbarung oder Teilen davon beinhaltet, die Verantwortung dafür, dass die in Absatz 1 festgelegten wesentlichen Anforderungen erfüllt sind.
- (4) Bei einem intelligenten Vertrag, der den harmonisierten Normen oder deren einschlägigen Teilen dieser Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht werden, entspricht, wird eine Konformität mit den in Absatz 1 festgelegten wesentlichen Anforderungen vermutet, soweit diese Anforderungen durch diese harmonisierten Normen erfasst sind.
- (5) Die Kommission beauftragt gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen, Entwürfe für harmonisierte Normen zu erarbeiten, die den in Absatz 1 des vorliegenden Artikels genannten wesentlichen Anforderungen genügen.
- (6) Die Kommission kann im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen erlassen, die einige oder alle der wesentlichen Anforderungen gemäß Absatz 1 erfassen, sofern die folgenden Voraussetzungen erfüllt sind:
  - a) Die Kommission hat gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragt, eine harmonisierte Norm zu erarbeiten, die den in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen genügt, und
    - (i) der Auftrag wurde nicht angenommen,
    - (ii) die harmonisierten Normen für diesen Auftrag sind nicht innerhalb der gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 gesetzten Frist vorgelegt worden oder
    - (iii) die harmonisierten Normen erfüllen den Auftrag nicht, und
  - b) im Amtsblatt der Europäischen Union ist für die harmonisierten Normen, die die einschlägigen, in Absatz 1 des vorliegenden Artikels festgelegten wesentlichen Anforderungen erfassen, keine Fundstelle gemäß der Verordnung (EU) Nr. 1025/2012 veröffentlicht, und eine solche Fundstelle wird voraussichtlich auch nicht innerhalb einer angemessenen Frist veröffentlicht werden.

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

- (7) Vor der Ausarbeitung eines Entwurfs des in Absatz 6 des vorliegenden Artikels genannten Durchführungsrechtsakts teilt die Kommission dem in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss mit, dass die Bedingungen des Absatzes 6 des vorliegenden Artikels ihres Erachtens erfüllt worden sind.

- (8) Bei der Ausarbeitung des Entwurfs des in Absatz 6 genannten Durchführungsrechtsakts berücksichtigt die Kommission den Rat des EDIB und die Standpunkte anderer einschlägiger Gremien oder Expertengruppen und konsultiert ordnungsgemäß alle einschlägigen Interessenträger.
- (9) Beim Anbieter eines intelligenten Vertrags oder – in dessen Ermangelung – bei der Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit den Einsatz intelligenter Verträge für Dritte im Zusammenhang mit der Durchführung einer Datenbereitstellungsvereinbarung oder Teilen davon umfasst, die die mit den in Absatz 6 genannten Durchführungsrechtsakten vollständig oder teilweise festgelegten gemeinsamen Spezifikationen erfüllt, wird eine Konformität mit den in Absatz 1 festgelegten wesentlichen Anforderungen vermutet, soweit diese Anforderungen durch diese gemeinsamen Spezifikationen ganz oder teilweise erfasst werden.
- (10) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im Amtsblatt der Europäischen Union vorgeschlagen, so bewertet die Kommission diese harmonisierte Norm gemäß der Verordnung (EU) Nr. 1025/2012. Wird die Fundstelle einer harmonisierten Norm im Amtsblatt der Europäischen Union veröffentlicht, so werden die in Absatz 6 dieses Artikels genannten Durchführungsrechtsakte, die dieselben wesentlichen Anforderungen erfassen, wie sie von dieser harmonisierten Norm erfasst sind, von der Kommission ganz oder teilweise aufgehoben.
- (11) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den in Absatz 1 genannten wesentlichen Anforderungen nicht vollständig entspricht, so setzt er die Kommission durch Übermittlung einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die ausführliche Erläuterung und kann gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde, ändern.

(104) Um die Interoperabilität von Instrumenten für die automatisierte Durchführung von Vereinbarungen über die Datenweitergabe zu fördern, müssen wesentliche Anforderungen an intelligente Verträge festgelegt werden, die Fachkräfte für andere erstellen oder in Anwendungen integrieren, die die Umsetzung von Vereinbarungen über die Datenweitergabe unterstützen. Um die Konformität solcher intelligenter Verträge mit diesen wesentlichen Anforderungen zu erleichtern, muss eine Konformitätsvermutung für die intelligenten Verträge vorgesehen werden, die ganz oder teilweise den harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 entsprechen. Der Begriff "intelligenter Vertrag" in der vorliegenden Verordnung ist technologieneutral. Intelligente Verträge können beispielsweise mit einem elektronischen Vorgangsregister verbunden werden. Die wesentlichen Anforderungen sollten nur für Anbieter intelligenter Verträge gelten, nicht aber dann, wenn sie intern intelligente Verträge, die ausschließlich für den internen Gebrauch bestimmt sind, ausarbeiten. Die wesentliche Anforderung, sicherzustellen, dass intelligente Verträge ausgesetzt und beendet werden können, setzt die gegenseitige Zustimmung der Parteien zu der Vereinbarung über die Datenweitergabe voraus. Die Anwendbarkeit der einschlägigen Vorschriften des Zivil-, Vertrags- und Verbraucherschutzes auf Vereinbarungen über die Datenweitergabe bleibt von der Nutzung intelligenter Verträge für die automatisierte Ausführung solcher Vereinbarungen unberührt oder sollte davon unberührt bleiben.

(105) Zum Nachweis, dass die wesentlichen Anforderungen dieser Verordnung erfüllt sind, sollte der Anbieter eines intelligenten Vertrags – oder in dessen Ermangelung die Person, deren gewerbliche, geschäftliche oder berufliche Tätigkeit die Einführung intelligenter Ver-

träge für Andere im Zusammenhang mit der Durchführung einer Vereinbarung oder Teilen davon über die Bereitstellung von Daten im Kontext der vorliegenden Verordnung beinhaltet, – eine Konformitätsbewertung durchführen und eine EU-Konformitätserklärung ausstellen. Diese Konformitätsbewertung sollte den allgemeinen Grundsätzen nach der Verordnung ( ) Nr. 765/2008 des Europäischen Parlaments und des Rates (34) und dem Beschluss ( ) Nr. 768/2008 des Europäischen Parlaments und des Rates (35) unterliegen.

(106) Abgesehen davon, dass professionelle Entwickler intelligenter Verträge zur Erfüllung wesentlicher Anforderungen verpflichtet werden müssen, ist es auch wichtig, diejenigen Teilnehmer in Datenräumen, die anderen Teilnehmern innerhalb von gemeinsamen europäischen Datenräumen und über diese Datenräume Daten oder datenbasierte Dienste anbieten, dazu anzuhalten, die Interoperabilität von Instrumenten für die Datenweitergabe – einschließlich intelligenter Verträge – zu unterstützen.

## Kapitel IX Anwendung und Durchsetzung

### Artikel 37 Zuständige Behörden und Datenkoordinatoren

(107) Um die Anwendung und Durchsetzung dieser Verordnung zu gewährleisten, sollten die Mitgliedstaaten eine oder mehrere zuständige Behörden benennen. Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so sollte er unter ihnen auch einen Datenkoordinator benennen. Die zuständigen Behörden sollten miteinander zusammenarbeiten. Durch die Ausübung ihrer Ermittlungsbefugnisse im Einklang mit den geltenden nationalen Verfahren sollten die zuständigen Behörden in der Lage sein, Informationen zu suchen und zu erhalten, insbesondere in Bezug auf die Tätigkeiten von Stellen in ihrem Zuständigkeitsbereich und – auch im Rahmen gemeinsamer Untersuchungen – unter gebührender Berücksichtigung des Umstands, dass Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf in die Zuständigkeit eines anderen Mitgliedstaats fallende Rechtsträger von der zuständigen Behörde dieses anderen Mitgliedstaats, gegebenenfalls im Einklang mit den Verfahren für die grenzüberschreitende Zusammenarbeit, erlassen werden sollten. Die zuständigen Behörden sollten einander rechtzeitig unterstützen, insbesondere wenn eine zuständige Behörde in einem Mitgliedstaat über relevante Informationen für eine von den zuständigen Behörden in anderen Mitgliedstaaten durchgeführte Untersuchung verfügt oder solche Informationen sammeln kann, zu denen die zuständigen Behörden in dem Mitgliedstaat, in dem die Einrichtung niedergelassen ist, keinen Zugang haben. Die zuständigen Behörden und die Datenkoordinatoren sollten in einem von der Kommission geführten öffentlichen Register aufgeführt werden. Der Datenkoordinator könnte im Hinblick auf die Erleichterung der Zusammenarbeit in grenzüberschreitenden Situationen zusätzliche Hilfe bieten, wenn etwa einer zuständigen Behörde eines bestimmten Mitgliedstaats nicht bekannt ist, an welche Behörde sie sich im Mitgliedstaat des Datenkoordinators wenden sollte, wenn beispielsweise der Fall mehr als eine zuständige Behörde oder mehr als einen Sektor betrifft. Der Datenkoordinator sollte als zentrale Anlaufstelle für alle Fragen im Zusammenhang mit der Anwendung dieser Verordnung handeln. Wurde kein Datenkoordinator benannt, so sollte die zuständige Behörde die dem Datenkoordinator gemäß dieser Verordnung übertragenen Aufgaben übernehmen. Die für die Überwachung der Einhaltung des Datenschutzes zuständigen Behörden und die nach Unionsrecht oder nationalem Recht benannten zuständigen Behörden sollten in ihren Zuständigkeitsbereichen für die Anwendung dieser Verordnung verantwortlich sein. Um Interessenkonflikte zu vermeiden, sollten die Behörden, die im Bereich der Bereitstellung von Daten im Anschluss an ein Verlangen aufgrund einer außergewöhnlichen Notwendigkeit für die Anwendung und Durchsetzung dieser Verordnung zuständig sind, nicht das Recht haben, ein solches Verlangen zu stellen.

- (1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für die Anwendung und Durchsetzung dieser Verordnung (im Folgenden “zuständige Behörden”) verantwortlich sind. Die Mitgliedstaaten können eine oder mehrere neue Behörden einrichten oder sich auf bestehende Behörden stützen.
- (2) Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so benennt er einen Datenkoordinator aus ihrer Mitte, um die Zusammenarbeit zwischen den zuständigen Behörden zu erleichtern und die Stellen, die in den Anwendungsbereich dieser Verordnung fallen, in allen Fragen im Zusammenhang mit ihrer Anwendung und Durchsetzung zu unterstützen. Die zuständigen Behörden arbeiten bei der Wahrnehmung der ihnen nach Absatz 5 übertragenen Aufgaben und Befugnisse zusammen.
- (3) Die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden sind 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 die Kommission, die Europäische Zentralbank oder Einrichtungen der Union davon betroffen sind. Artikel 62 der Verordnung (EU) 2018/1725 gilt gegebenenfalls sinngemäß.

Die in diesem Absatz genannten Aufsichtsbehörden nehmen ihre Aufgaben und Befugnisse im Hinblick auf die Verarbeitung personenbezogener Daten wahr.

- (4) Unbeschadet des Absatzes 1 gilt Folgendes:
  - a) Bei besonderen sektoralen Angelegenheiten des Datenzugangs und der Datennutzung im Zusammenhang mit der Anwendung dieser Verordnung bleibt die Zuständigkeit der sektoralen Behörden gewahrt;
  - b) die für die Anwendung und Durchsetzung der Artikel 23 bis 31 und der Artikel 34 und 35 verantwortliche zuständige Behörde muss über Erfahrungen auf dem Gebiet Daten und elektronische Kommunikationsdienste verfügen.
- (5) Die Mitgliedstaaten sorgen dafür, dass die Aufgaben und Befugnisse der zuständigen Behörden eindeutig festgelegt werden und Folgendes umfassen:
  - a) Förderung der Datenkompetenz und der Sensibilisierung von Nutzern und Stellen, die in den Anwendungsbereich dieser Verordnung fallen, in Bezug auf die Rechte und Pflichten aus dieser Verordnung;

(19) Der Begriff “Datenkompetenz” bezeichnet die Fähigkeiten, das Wissen und das Verständnis, die/das es Nutzern, Verbrauchern und Unternehmen, insbesondere KMU, die in den Anwendungsbereich dieser Verordnung fallen, ermöglichen, sich des potenziellen Werts der von ihnen generierten, produzierten und weitergegebenen Daten bewusst zu werden, und sie dazu motivieren, im Einklang mit den einschlägigen Rechtsvorschriften Zugang zu ihren Daten anzubieten und zu gewähren. Datenkompetenz sollte über den Erwerb von Wissen über Instrumente und Technologien hinausgehen und darauf abzielen, Bürgerinnen und Bürger und Unternehmen in die Lage zu versetzen und zu befähigen, aus einem inklusiven und fairen Datenmarkt Nutzen zu ziehen. Die Verbreitung von Maßnahmen zur Datenkompetenz und die Einführung angemessener Folgemaßnahmen könnten dazu beitragen, die Arbeitsbedingungen zu verbessern, und letztlich die Konsolidierung und den Innovationspfad

der Datenwirtschaft in der Union unterstützen. Die zuständigen Behörden sollten Instrumente fördern und Maßnahmen ergreifen, um die Datenkompetenz von Nutzern und Rechtsträgern, die in den Anwendungsbereich dieser Verordnung fallen, zu verbessern und sie für ihre Rechte und Pflichten aus dieser Verordnung zu sensibilisieren.

- b) Bearbeitung von Beschwerden über mutmaßliche Verstöße gegen diese Verordnung, einschließlich Bezug auf Geschäftsgeheimnisse, und angemessene Untersuchung des Beschwerdegegenstands sowie regelmäßige Unterrichtung des Beschwerdeführers – gegebenenfalls im Einklang mit nationalem Recht – innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung, insbesondere, wenn eine weitere Untersuchung oder die Abstimmung mit einer anderen zuständigen Behörde notwendig ist;
- c) Durchführung von Untersuchungen über Fragen der Anwendung dieser Verordnung, einschließlich auf der Grundlage von Informationen einer anderen zuständigen Behörde oder 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 technologischer und einschlägiger wirtschaftlicher Entwicklungen, die für die Bereitstellung und Nutzung von Daten von Bedeutung sind;
- f) Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission oder dem EDIB, um die einheitliche und effiziente Anwendung dieser Verordnung zu gewährleisten, einschließlich des unverzüglichen Austauschs aller relevanten Informationen auf elektronischem Wege, einschließlich in Bezug auf Absatz 10 des vorliegenden Artikels;
- g) Zusammenarbeit mit den einschlägigen zuständigen Behörden, die für die Anwendung anderer Rechtsakte der Union oder nationaler Rechtsakte zuständig sind, einschließlich mit auf dem Gebiet Daten und elektronische Kommunikationsdienste zuständigen Behörden, mit der für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörde oder mit sektoralen Behörden, um sicherzustellen, dass diese Verordnung im Einklang mit anderem Unionsrecht und nationalem Recht durchgesetzt wird;
- h) Zusammenarbeit mit den einschlägigen zuständigen Behörden zur Gewährleistung der Durchsetzung der Artikel 23 bis 31 und der Artikel 34 und 35 im Einklang mit anderem Unionsrecht und mit der Selbstregulierung, die für Anbieter von Datenverarbeitungsdiensten gelten;
- i) Gewährleistung der Abschaffung von Wechselentgelten gemäß Artikel 29;
- j) Prüfung von Datenverlangen nach Kapitel V.

Wird ein Datenkoordinator benannt, so erleichtert er die in Unterabsatz 1 Buchstaben f, g und h genannte Zusammenarbeit und unterstützt die zuständigen Behörden auf deren Ersuchen.

- (6) Falls eine solche zuständige Behörde benannt wurde, hat der Datenkoordinator folgende Aufgaben:

- a) Er fungiert als zentrale Anlaufstelle für alle Fragen im Zusammenhang mit der Anwendung dieser Verordnung;
  - b) Er gewährleistet die öffentliche Verfügbarkeit der von öffentlichen Stellen im Fall außergewöhnlicher Notwendigkeit nach Kapitel V gestellten Datenzugangsverlangen und fördert freiwillige Datenweitergabevereinbarungen zwischen öffentlichen Stellen und Dateninhabern;
  - c) unterrichtet die Kommission jährlich über die nach Artikel 4 Absatz 2 und Absatz 8 und Artikel 5 Absatz 11 mitgeteilten Ablehnungen.
- (7) Die Mitgliedstaaten teilen der Kommission die Namen der zuständigen Behörden und ihre Aufgaben und Befugnisse sowie gegebenenfalls den Namen des Datenkoordinators mit. Die Kommission führt ein öffentliches Register dieser Behörden.
- (8) Bei der Wahrnehmung ihrer Aufgaben und Befugnisse gemäß dieser Verordnung handeln die zuständigen Behörden unparteiisch und unterliegen keiner direkten oder indirekten Einflussnahme von außen und dürfen von anderen Behörden oder von privaten Parteien im Einzelfall keine Weisungen einholen oder entgegennehmen.
- (9) Die Mitgliedstaaten sorgen dafür, dass die zuständigen Behörden personell und technisch mit ausreichenden Mitteln und dem einschlägigen Fachwissen ausgestattet sind, damit sie ihre Aufgaben gemäß dieser Verordnung wirksam wahrnehmen können.
- (10) Rechtsträger, die in den Anwendungsbereich dieser Verordnung fallen, unterliegen der Zuständigkeit des Mitgliedstaats, in dem der Rechtsträger niedergelassen ist. Ist der Rechtsträger in mehr als einem Mitgliedstaat niedergelassen, so wird davon ausgegangen, dass er in die Zuständigkeit des Mitgliedstaats fällt, in dem er seine Hauptniederlassung hat, d. h. in dem der Rechtsträger seinen Hauptsitz oder eingetragenen Sitz hat, von dem aus die wichtigsten finanziellen Tätigkeiten und die betriebliche Kontrolle erfolgen.
- (11) Jeder in den Anwendungsbereich dieser Verordnung fallende Rechtsträger, der in der Union vernetzte Produkte bereitstellt oder Dienste anbietet und nicht in der Union niedergelassen ist, benennt einen Vertreter in einem der Mitgliedstaaten.
- (12) Damit die Einhaltung dieser Verordnung sichergestellt ist, beauftragt ein in den Anwendungsbereich dieser Verordnung fallender Rechtsträger, der in der Union vernetzte Produkte bereitstellt oder Dienste anbietet, einen Vertreter, an den sich die zuständigen Behörden in allen Fragen im Zusammenhang mit diesem Rechtsträger zusätzlich oder an seiner Stelle wenden. Dieser Vertreter arbeitet mit den zuständigen Behörden zusammen und erbringt gegenüber den zuständigen Behörden auf Anfrage den umfassenden Nachweis für die Maßnahmen und die Bestimmungen, die von dem in den Anwendungsbereich dieser Verordnung fallenden Rechtsträger, der in der Union vernetzte Produkte bereitstellt oder Dienste anbietet, zur Gewährleistung der Einhaltung dieser Verordnung ergriffen bzw. aufgestellt wurden.
- (13) Für in den Anwendungsbereich dieser Verordnung fallende Rechtsträger, die in der Union vernetzte Produkte bereitstellen oder Dienste anbieten, gilt, dass sie der Zuständigkeit des Mitgliedstaats unterliegen, in dem ihr jeweiliger Vertreter ansässig ist. Die Benennung eines Vertreters durch diesen Rechtsträger erfolgt unbeschadet der Haftung eines solchen Rechtsträgers und etwaiger rechtlicher Schritte, die gegen einen solchen Rechtsträger angestrengt werden könnten. Bis ein Rechtsträger einen Vertreter

gemäß diesem Artikel benennt, fällt er für die Zwecke der Sicherstellung der Anwendung und Durchsetzung dieser Verordnung gegebenenfalls in die Zuständigkeit aller Mitgliedstaaten. Jede zuständige Behörde kann ihre Zuständigkeit – einschließlich durch Verhängung wirksamer, verhältnismäßiger und abschreckender Sanktionen – ausüben, sofern der Rechtsträger nicht bereits Gegenstand eines durch eine andere zuständige Behörde in derselben Sache eingeleiteten Durchsetzungsverfahrens nach dieser Verordnung ist.

- (14) Die zuständigen Behörden sind befugt, von Nutzern, Dateninhabern oder Datenempfängern oder deren Vertretern, die in die Zuständigkeit ihres Mitgliedstaats fallen, alle Informationen zu verlangen, die nötig sind, um die Einhaltung dieser Verordnung zu überprüfen. Jedes Informationsverlangen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.
- (15) Ersucht eine zuständige Behörde in einem Mitgliedstaat um die Unterstützung oder Vollstreckungsmaßnahmen einer zuständigen Behörde in einem anderen Mitgliedstaat, so stellt sie ein begründetes Ersuchen. Eine zuständige Behörde beantwortet ein solches Ersuchen unverzüglich nach dessen Eingang, wobei sie die einzelnen ergriffenen oder geplanten Maßnahmen aufführt.
- (16) Die zuständigen Behörden wahren den Grundsatz der Vertraulichkeit und des Berufs- und Geschäftsgeheimnisses und schützen personenbezogene Daten nach Maßgabe des Unionsrechts oder des nationalen Rechts. Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen ausgetauscht und nach diesem Artikel bereitgestellt werden, dürfen nur für die Zwecke dieses Ersuchens verwendet werden.

## **Artikel 38 Recht auf Beschwerde**

(108) Zur Durchsetzung ihrer Rechte gemäß dieser Verordnung sollten natürliche und juristische Personen das Recht haben, bei Verletzung ihrer Rechte aus dieser Verordnung durch Beschwerdeeinlegung Rechtsmittel einzulegen. Der Datenkoordinator sollte natürlichen und juristischen Personen auf Anfrage alle erforderlichen Informationen bereitstellen, damit sie bei der betreffenden zuständigen Behörde Beschwerde einlegen können. Diese Behörden sollten zur Zusammenarbeit verpflichtet sein, damit die Beschwerde angemessen bearbeitet und wirksam und zügig 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 (36) und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates (37) geändert.

- (1) Unbeschadet eines anderen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs haben natürliche und juristische Personen das Recht, einzeln oder gegebenenfalls gemeinsam bei der jeweils zuständigen Behörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder ihrer Niederlassung Beschwerde einzulegen, wenn sie der Ansicht sind, dass ihre Rechte nach dieser Verordnung verletzt wurden. Der Datenkoordinator stellt natürlichen und juristischen Personen auf Anfrage alle erforderlichen Informationen bereit, damit sie bei der zuständigen Behörde Beschwerde einlegen können.
- (2) Die zuständige Behörde, bei der 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 zusammen, um Beschwerden wirksam und fristgemäß zu bearbeiten und zu lösen, und tauschen dazu unter anderem unverzüglich alle relevanten Informationen auf elektronischem Wege aus. Diese Zusammenarbeit betrifft nicht das Verfahren für die Zusammenarbeit gemäß den Kapiteln VI und VII der Verordnung (EU) 2016/679 und gemäß der Verordnung (EU) 2017/2394.

### **Artikel 39 Recht auf einen wirksamen gerichtlichen Rechtsbehelf**

- (1) Unbeschadet anderer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe hat jede betroffene natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen rechtsverbindliche Entscheidungen zuständiger Behörden.
- (2) Wenn eine zuständige Behörde in Bezug auf eine Beschwerde untätig bleibt, hat jede davon betroffene natürliche oder juristische Person im Einklang mit dem nationalen Recht entweder das Recht auf einen wirksamen gerichtlichen Rechtsbehelf oder Zugang zur Nachprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis.
- (3) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats der zuständigen Behörde eingeleitet, gegen die sich der Rechtsbehelf, der von einer einzelnen natürlichen oder juristischen Person oder gegebenenfalls von den Vertretern einer oder mehrerer natürlicher oder juristischer Personen eingelegt wurde, richtet.

### **Artikel 40 Sanktionen**

(109) Die zuständigen Behörden sollten sicherstellen, dass für Verstöße gegen die in dieser Verordnung festgelegten Pflichten Sanktionen gelten. Solche Sanktionen könnten finanzielle Sanktionen, Verwarnungen, Verweise oder Anordnungen, die Geschäftspraxis mit den in dieser Verordnung festgelegten Verpflichtungen in Einklang zu bringen, einschließen. Die von den Mitgliedstaaten festgelegten Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein und den Empfehlungen des EDIB Rechnung tragen und somit dazu beitragen, dass bei der Festlegung und Anwendung von Sanktionen ein Höchstmaß an Kohärenz erreicht wird. Die zuständigen Behörden sollten gegebenenfalls einstweilige Maßnahmen ergreifen, um die Auswirkungen eines mutmaßlichen Verstoßes zu begrenzen, solange die Untersuchung dieses Verstoßes noch nicht abgeschlossen ist. Dabei sollten sie unter anderem Art, Schwere, Ausmaß und Dauer der Pflichtverletzung im Hinblick auf das betreffende öffentliche Interesse, den Umfang und die Art der ausgeübten Tätigkeiten und die wirtschaftliche Leistungsfähigkeit der verstoßenden Partei berücksichtigen. Sie sollten auch berücksichtigen, ob der Rechtsverletzer seinen Pflichten aus dieser Verordnung systematisch oder wiederholt nicht nachkommt. Um die Einhaltung des Grundsatzes *ne bis in idem* zu gewährleisten und insbesondere zu vermeiden, dass ein und derselbe Verstoß gegen die Pflichten aus dieser Verordnung mehr als einmal geahndet wird, sollte ein Mitgliedstaat, der beabsichtigt, seine Zuständigkeit in Bezug auf eine verstoßende Partei auszuüben, die nicht in der Union niedergelassen ist und keinen Vertreter in der Union benannt hat, unverzüglich alle Datenkoordinatoren und die Kommission unterrichten.

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

- (2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 12. September 2025 mit und melden ihr unverzüglich alle späteren diesbezüglichen Änderungen. Die Kommission führt ein leicht zugängliches öffentliches Register dieser Maßnahmen und aktualisiert es regelmäßig.
- (3) Bei der Verhängung von Sanktionen aufgrund von Verstößen gegen diese Verordnung berücksichtigen die Mitgliedstaaten die Empfehlungen des EDIB und die folgenden nicht erschöpfenden Kriterien:
  - 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 des jeweiligen Falls;
  - f) den Jahresumsatz der verstoßenden Partei im vorangegangenen Geschäftsjahr in der Union.
- (4) Bei Verstößen gegen die Pflichten der Kapitel II, III und V dieser Verordnung können die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen 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.
- (5) Bei Verstößen gegen die Pflichten des Kapitels V dieser Verordnung kann der Europäische Datenschutzbeauftragte innerhalb seines 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 41 Mustervertragsklauseln und Standardvertragsklauseln**

(111) Um Unternehmen bei der Ausarbeitung und Aushandlung von Verträgen zu unterstützen, sollte die Kommission unverbindliche Mustervertragsklauseln für Verträge über die Datenweitergabe zwischen Unternehmen erstellen und empfehlen, erforderlichenfalls unter Berücksichtigung der Bedingungen in bestimmten Sektoren und bestehender Verfahren mit freiwilligen Datenweitergabemechanismen. Diese Mustervertragsklauseln sollten in erster Linie eine praktische Handhabe bieten, um insbesondere KMU den Abschluss eines Vertrags zu erleichtern. Werden die Mustervertragsbestimmungen umfassend und durchgehend verwendet, so dürften sie sich auch positiv auf die Gestaltung von Verträgen über den Datenzugang und die Datennutzung auswirken und somit insgesamt zu faireren Vertragsbeziehungen beim Datenzugang und bei der Datenweitergabe führen.

Die Kommission erstellt und empfiehlt vor dem 12. September 2025 unverbindliche Mustervertragsklauseln für den Datenzugang und die Datennutzung – einschließlich Bedingungen für eine angemessene Gegenleistung und den Schutz von Geschäftsgeheimnissen sowie nicht verbindliche Standardvertragsklauseln für Verträge über Cloud-Computing -, um die Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit fairen, angemessenen und nichtdiskriminierenden vertraglichen Rechten und Pflichten zu unterstützen.

## Artikel 42 Rolle des EDIB

(110) Der EDIB sollte die Kommission bei der Koordinierung der nationalen Verfahren und Strategien zu den unter diese Verordnung fallenden Themen sowie bei der Verwirklichung ihrer Ziele in Bezug auf die technische Normung zur Verbesserung der Interoperabilität beraten und unterstützen. Er sollte auch eine Schlüsselrolle übernehmen, wenn es darum geht, zwischen den zuständigen Behörden umfassende Gespräche über die Anwendung und Durchsetzung der vorliegenden Verordnung auf den Weg zu bringen. Der betreffende Informationsaustausch soll den wirksamen Zugang zur Justiz sowie die Durchsetzung und justizielle Zusammenarbeit in der gesamten Union verbessern. Neben anderen Aufgaben sollten die zuständigen Behörden den EDIB als Plattform für die Bewertung, Koordinierung und Annahme von Empfehlungen zur Festlegung von Sanktionen für Verstöße gegen diese Verordnung nutzen. Er sollte es den zuständigen Behörden ermöglichen, mit Unterstützung der Kommission einen optimalen Ansatz für die Festlegung und Verhängung solcher Sanktionen abzustimmen. Dieser Ansatz verhindert eine Fragmentierung und räumt den Mitgliedstaaten gleichzeitig Flexibilität ein, und er sollte zu wirksamen Empfehlungen führen, die die einheitliche Anwendung dieser Verordnung unterstützen. Außerdem sollte dem EDIB bei den Normungsverfahren und der Annahme gemeinsamer Spezifikationen im Wege von Durchführungsrechtsakten und bei der Annahme delegierter Rechtsakte zur Einführung eines Überwachungsmechanismus für die von den Anbietern von Datenverarbeitungsdiensten erhobenen Wechselentgelte und zur weiteren Präzisierung der wesentlichen Anforderungen an die Interoperabilität von Daten, von Mechanismen und Diensten für die Datenweitergabe sowie an die gemeinsamen europäischen Datenräume eine beratende Rolle zukommen. Ferner sollte er die Kommission bei der Annahme der Leitlinien zur Festlegung von Interoperabilitätsspezifikationen für das Funktionieren der gemeinsamen europäischen Datenräume beraten und unterstützen.

Der gemäß Artikel 29 der Verordnung (EU) 2022/868 von der Kommission als Experten-Gruppe eingesetzte EDIB, in dem die zuständigen Behörden vertreten sind, unterstützt die einheitliche Anwendung dieser Verordnung durch

- a) Beratung und Unterstützung der Kommission in Bezug auf die Entwicklung einer kohärenten Praxis der zuständigen Behörden bei der Durchsetzung der Kapitel II, III, V und VII,
- b) Erleichterung der Zusammenarbeit zwischen den zuständigen Behörden durch Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für den effizienten Austausch von Informationen über die Durchsetzung der Rechte und Pflichten nach den Kapiteln II, III und V in grenzüberschreitenden Fällen, einschließlich der Abstimmung in Bezug auf die Festlegung von Sanktionen,
- c) Beratung und Unterstützung der Kommission in Bezug auf
  - (i) die Beantwortung der Frage, ob um die Erarbeitung harmonisierter Normen gemäß Artikel 33 Absatz 4, Artikel 35 Absatz 4 und Artikel 36 Absatz 5 ersucht werden soll,
  - (ii) die Ausarbeitung der Durchführungsrechtsakte gemäß Artikel 33 Absatz 5, Artikel 35 Absätze 5 und 8 sowie Artikel 36 Absatz 6,
  - (iii) die Ausarbeitung der in Artikel 29 Absatz 7 und Artikel 33 Absatz 2 genannten delegierten Rechtsakte und
  - (iv) die Annahme der Leitlinien zur Festlegung von interoperablen Rahmen für gemeinsame Normen und Verfahren für das Funktionieren gemeinsamer europäischer Datenräume gemäß Artikel 33 Absatz 11.

# Kapitel X Schutzrecht Sui Generis nach der Richtlinie 96/9/EG

## Artikel 43 Datenbanken, die bestimmte Daten enthalten

(112) Damit nicht das Risiko besteht, dass die Inhaber von Daten, die durch physische Komponenten wie Sensoren eines vernetzten Produkts und eines verbundenen Dienstes erlangt oder generiert wurden, oder anderen maschinengenerierten Daten in Datenbanken das Schutzrecht sui generis gemäß Artikel 7 der Richtlinie 96/9/EG geltend machen und dadurch insbesondere die wirksame Ausübung des Rechts der Nutzer auf Datenzugang und Datennutzung sowie des Rechts auf die Weitergabe von Daten an Dritte gemäß dieser Verordnung behindern, sollte klargestellt werden, dass das Schutzrecht sui generis für solche Datenbanken nicht gilt. 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 Absatz 1 jenes Artikels erfüllt sind.

Das in Artikel 7 der Richtlinie 96/9/EG festgelegte Schutzrecht sui generis findet keine Anwendung, wenn Daten mittels eines in den Anwendungsbereich der vorliegenden Verordnung – und insbesondere der Artikel 4 und 5 dieser Verordnung – fallenden vernetzten Produkts oder verbundenen Dienstes erlangt oder erzeugt wurden.

# Kapitel XI Schlussbestimmungen

## Artikel 44 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 aufgrund von Rechtsvorschriften der Union, die bis zum 11. Januar 2024 in Kraft getreten sind, und darauf beruhenden delegierten Rechtsakten oder Durchführungsrechtsakten bleiben unberührt.
- (2) Diese Verordnung berührt nicht das Unionsrecht, 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.

- (3) Diese Verordnung – mit Ausnahme des Kapitels V – berührt nicht das Unionsrecht und das nationale Recht, das den Zugang zu Daten und die Genehmigung ihrer Nutzung zu Zwecken der wissenschaftlichen Forschung vorsieht.

## **Artikel 45 Ausübung der Befugnisübertragung**

(113) 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 Überwachungsmechanismus der von den Anbietern von Datenverarbeitungsdiensten auf dem Markt verlangten Wechselentgelte einzuführen, und um die wesentlichen Anforderungen im Hinblick auf die Interoperabilität für Teilnehmer von Datenräumen, die anderen Teilnehmern an Datenräumen Daten oder Datendienste anbieten, weiter zu präzisieren. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung (38) 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.

(114) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse eingeräumt werden bezüglich der Annahme gemeinsamer Spezifikationen zur Sicherstellung der Interoperabilität der Daten, der Mechanismen und Diensten für die Datenweitergabe und der gemeinsamen europäischen Datenräume, bezüglich gemeinsamer Spezifikationen für die Interoperabilität von Datenverarbeitungsdiensten und bezüglich gemeinsamer Spezifikationen für die Interoperabilität intelligenter Verträge. Auch sollten der Kommission Durchführungsbefugnisse eingeräumt werden bezüglich der Veröffentlichung der Bezugnahmen auf harmonisierten Normen und gemeinsamen Spezifikationen für die Interoperabilität von in der zentralen Datenbank der Union für Normen für die Interoperabilität von Datenverarbeitungsdiensten. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates (39) ausgeübt werden.

- (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 29 Absatz 7 und Artikel 33 Absatz 2 wird der Kommission auf unbestimmte Zeit ab dem 11. Januar 2024 übertragen.
- (3) Die Befugnisübertragung gemäß Artikel 29 Absatz 7 und Artikel 33 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

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

### **Artikel 46 Ausschussverfahren**

- (1) Die Kommission wird von dem Ausschuss, der durch die Verordnung (EU) 2022/868 eingesetzt wurde, 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 47 Änderung der Verordnung (EU) 2017/2394**

Im Anhang der Verordnung (EU) 2017/2394 wird folgende Nummer angefügt: “29. Verordnung (EU) 2023/2854 des Rates und des Europäischen Parlaments vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. L, 2023/2854, 22.12.2023, ELI: [http://data.europa.eu/eli/reg/2023/2854/oj].)(http://data.europa.eu/eli/reg/2023/2854/oj).)”

### **Artikel 48 Änderung der Richtlinie (EU) 2020/1828**

In Anhang I der Richtlinie (EU) 2020/1828 wird folgende Nummer angefügt: “68. Verordnung (EU) 2023/2854 des Rates und des Europäischen Parlaments vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. L, 2023/2854, 22.12.2023, ELI: [http://data.europa.eu/eli/reg/2023/2854/oj].)(http://data.europa.eu/eli/reg/2023/2854/oj).)”

### **Artikel 49 Bewertung und Überprüfung**

- (1) Bis zum 12. September 2028 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 ihre wichtigsten Ergebnisse. Bei dieser Bewertung wird insbesondere Folgendes bewertet:

- a) Situationen, die für die Zwecke des Artikels 15 der vorliegenden Verordnung und die praktische Anwendung von Kapitel V der vorliegenden Verordnung als Fälle außergewöhnlicher Notwendigkeit angesehen werden, insbesondere die Erfahrungen mit der Anwendung von Kapitel V der vorliegenden Verordnung durch öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union; von den zuständigen Behörden gemeldete Anzahl und Ergebnisse der Verfahren, die bei der zuständigen Behörde gemäß Artikel 18 Absatz 5 in Bezug auf die Anwendung von Kapitel V der vorliegenden Verordnung eingeleitet wurden; die Auswirkungen anderer Verpflichtungen, die im Unionsrecht oder im nationalen Recht für die Zwecke der Erfüllung von Informationszugangsverlangen festgelegt sind; die Auswirkungen von Mechanismen für die freiwillige Datenweitergabe, wie die von gemäß der Verordnung (EU) 2022/868 anerkannten datenaltuistischen Organisationen eingeführten, auf die Verwirklichung der Ziele des Kapitels V der vorliegenden Verordnung und die Rolle personenbezogener Daten im Zusammenhang mit Artikel 15 der vorliegenden Verordnung, einschließlich der Entwicklung von Technologien zur Verbesserung des Schutzes der Privatsphäre;
- b) die Auswirkungen dieser Verordnung auf die Nutzung von Daten in der Wirtschaft, auch auf Dateninnovation, Datenmonetarisierungspraxis und Datenvermittlungsdienste, sowie auf die Weitergabe von Daten innerhalb der gemeinsamen europäischen Datenräume;
- c) die Zugänglichkeit und die Nutzung der verschiedenen Kategorien und Arten von Daten;
- d) der Ausschluss bestimmter Kategorien von Unternehmen als Begünstigte nach Artikel 5,
- e) das Nichtbestehen von Auswirkungen auf die Rechte des geistigen Eigentums;
- f) die Auswirkungen auf Geschäftsgeheimnisse, auch auf den Schutz vor dem rechtswidrigen Erwerb sowie der rechtswidrigen Nutzung und Offenlegung von Geschäftsgeheimnissen, sowie die Auswirkungen des Mechanismus, in dessen Rahmen der Dateninhaber das Datenzugangsverlangen des Nutzers gemäß Artikel 4 Absatz 8 und Artikel 5 Absatz 11 ablehnen kann, dabei wird, soweit möglich, einer etwaigen Überarbeitung der Richtlinie (EU) 2016/943 Rechnung getragen;
- g) die Frage, ob die Liste missbräuchlicher Vertragsklauseln gemäß Artikel 13 angesichts neuer Geschäftsgepflogenheiten und der rasch voranschreitenden Marktinnovation noch aktuell ist;
- h) Änderungen der Vertragspraxis von Anbietern von Datenverarbeitungsdiensten und die Frage, ob Artikel 25 angesichts dieser Änderungen noch ausreichend eingehalten wird;
- i) die Senkung der Entgelte, die Anbieter von Datenverarbeitungsdiensten für den Vollzug des Wechsels verlangen, im Einklang mit der schrittweisen Abschaffung von Wechselentgelten nach Artikel 29;
- j) das Zusammenwirken dieser Verordnung mit anderen Rechtsakten der Union, die für die Datenwirtschaft von Bedeutung sind;
- k) die Verhinderung des unrechtmäßigen staatlichen Zugangs zu nicht-personenbezogenen Daten;

- l)* die Wirksamkeit der Durchsetzungsregelung nach Artikel 37;
  - m)* die Auswirkung der vorliegenden Verordnung auf KMU im Hinblick auf deren Innovationsfähigkeit und der Verfügbarkeit von Datenverarbeitungsdiensten für Nutzer in der Union sowie auf mit der Einhaltung der neuen Verpflichtungen verbundene Belastungen.
- (2) Bis zum 12. September 2028 führt die Kommission eine Bewertung dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss, zusätzlich zu ihrem Bericht gemäß Absatz 1, einen Bericht über ihre wichtigsten Ergebnisse. Bei dieser Bewertung werden die Auswirkungen der Artikel 23 bis 31, des Artikels 34 und des Artikels 35 – insbesondere in Bezug auf die Preisgestaltung und die Vielfalt der in der Union angebotenen Datenverarbeitungsdienste, unter besonderer Berücksichtigung von KMU-Anbietern – bewertet.
- (3) Die Mitgliedstaaten übermitteln der Kommission alle zur Ausarbeitung der in den Absätzen 1 und 2 genannten Berichte erforderlichen Informationen.
- (4) Die Kommission kann dem Europäischen Parlament und dem Rat auf der Grundlage der in den Absätzen 1 und 2 genannten Berichte gegebenenfalls einen Gesetzgebungsvorschlag zur Änderung dieser Verordnung vorlegen.

## **Artikel 50 Inkrafttreten und Geltungsbeginn**

(117) Damit sich die Teilnehmer, die in den Anwendungsbereich dieser Verordnung fallen, an die neuen Vorschriften dieser Verordnung anpassen und die notwendigen technischen Vorkehrungen treffen können, sollten diese Vorschriften erst ab dem 12. September 2025 anwendbar werden.

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

Sie gilt ab dem 12. September 2025.

Die Verpflichtung gemäß Artikel 3 Absatz 1 gilt für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem 12. September 2026 in Verkehr gebracht wurden.

Kapitel III gilt nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12. September 2025 in Kraft treten.

Kapitel IV gilt für Verträge, die nach dem 12. September 2025 geschlossen wurden.

Kapitel IV gilt ab dem 12. September 2027 für Verträge, die am oder vor dem 12. September 2025 geschlossen wurden, sofern

- a)* sie unbefristet sind oder
- b)* ihre Geltungsdauer frühestens 10 Jahre nach dem 11. Januar 2024 endet.

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

Geschehen zu Straßburg, am 13. Dezember 2023.

(118) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absätze 1 und 2 der Verordnung (EU) 2018/1725 angehört und haben am 4. Mai 2022 ihre Stellungnahmen abgegeben.

(Fussnoten entfernt)