

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)

Data Act, ohne Erwägungsgründe (eine Fassung mit den Erwägungsgründen findet sich auf <https://datenrecht.ch/gesetzestexte/data-act/>).

Die Texte wurden automatisiert konvertiert – wir danken für Hinweise auf Fehler an 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

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.
- (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.

- (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.
- (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.
- (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.

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;
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;

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;
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;
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;
16. **“verbundene Dienstdaten”** Daten, die die Digitalisierung von Nutzerhandlungen oder Vorgängen im Zusammenhang mit dem vernetzten Produkt darstellen und vom Nut-

zer absichtlich aufgezeichnet oder als Nebenprodukt der Handlung des Nutzers während der Bereitstellung eines verbundenen Dienstes durch den Anbieter generiert werden;

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;
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;
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;
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;
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;
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.
- (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 Datenverarbeitungsunternehmen;
 - 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

- (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.
- (6) Geschäftsgeheimnisse werden gewahrt und nur offengelegt, wenn vom Dateninhaber und vom Nutzer vor der Offenlegung alle Maßnahmen getroffen worden sind, die er-

forderlich 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.

- (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.
- (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.

- (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.
- (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.

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.

Artikel 5 Recht des Nutzers auf Weitergabe von Daten an Dritte

- (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.
- (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.

- (2) Dem Dritten ist untersagt,
- 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;
 - 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 Kleinunternehmen oder einem Kleinunternehmen hergestellt oder konzipiert werden oder die bei der Nutzung von verbundenen Diensten generiert werden, die von einem solchen Unternehmen er-

bracht 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.

- (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 anwendbaren 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.
- (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, dis-

kriminierend 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

- (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.
- (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.

Artikel 10 Streitbeilegung

- (1) Nutzer, Dateninhaber und Datenempfänger haben Zugang zu einer gemäß Absatz 5 des vorliegenden Artikels zertifizierten Streitbelegungsstelle 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.
- (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 Streitbeilegung 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 Streitbeilegung 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.
- (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.

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

- (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.
- (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:
 - 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 realistischen 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

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.

Artikel 15 Außergewöhnliche Notwendigkeit der Datennutzung

- (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-personebezogene 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-personebezogenen 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 Kleinstunternehmen und Kleinunternehmen.
- (3) Die Verpflichtung, nachzuweisen, dass die öffentliche Stelle nicht in der Lage war, nicht-personebezogene 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.
- (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.

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;
 - 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.

- (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.
- (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 außergewöhnlichen 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:
 - 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.
- (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.
- (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

- (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.

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.

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.

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

- (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.
- (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.

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.

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.
- (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

- (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.
- (3) Bei anderen als den in Absatz 1 des vorliegenden Artikels genannten Datenverarbeitungsdiensten gewährleisteten Anbietern 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 zugeschnitten 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.
- (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.

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.

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.

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.

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.

Kapitel IX Anwendung und Durchsetzung

Artikel 37 Zuständige Behörden und Datenkoordinatoren

- (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;
 - 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

- (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 berührt 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

- (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

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

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 er-sucht 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 genann-ten 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

Das in Artikel 7 der Richtlinie 96/9/ festgelegte Schutzrecht sui generis findet keine Anwen-dung, 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 Pflich-ten in Bezug auf den Datenzugang und die Datennutzung

- (1) Die besonderen Pflichten zur Bereitstellung von Daten zwischen Unternehmen, zwi-schen 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

- (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 Marktinovation 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

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.

(Fussnoten entfernt)