EUROPÄISCHE
KOMMISSION

Brüssel, den 25.11.2020
COM(2020) 767 final

2020/0340 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über europäische Daten-Governance
(Daten-Governance-Gesetz)

(Text von Bedeutung für den EWR)

{SEC(2020) 405 final} - {SWD(2020) 295 final} - {SWD(2020) 296 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Daten-Governance[1] beigefügt. Es handelt sich um die erste einer Reihe von Maßnahmen, die in der 2020 veröffentlichten europäischen Datenstrategie[2] angekündigt wurden. Das Instrument zielt darauf ab, die Verfügbarkeit von Daten zur Nutzung zu fördern, indem das Vertrauen in die Datenmittler erhöht wird und die Mechanismen für die gemeinsame Datennutzung in der gesamten EU gestärkt werden. Das Instrument bezieht sich auf Folgendes:

- Bereitstellung von Daten des öffentlichen Sektors zur Weiterverwendung in Fällen, in denen diese Daten den Rechten anderer unterliegen[3],
- gemeinsame Datennutzung durch Unternehmen gegen Entgelt in jedweder Form,
- Ermöglichung der Nutzung personenbezogener Daten mithilfe eines „Mittlers für die gemeinsame Nutzung personenbezogener Daten“, der Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen soll,
- Ermöglichung der Nutzung von Daten aus altruistischen Gründen.

• Kohärenz mit den bestehenden Vorschriften in diesem Bereich

Die vorliegende Initiative umfasst verschiedene Arten von Datenmittlern, die sowohl personenbezogene als auch nicht personenbezogene Daten verarbeiten. Daher ist das Zusammenspiel mit den Rechtsvorschriften über personenbezogenen Daten besonders wichtig. Mit der Datenschutz-Grundverordnung (DSGVO)[4] und der e-Datenschutzrichtlinie[5] hat die EU einen soliden und vertrauenswürdigen Rechtsrahmen für den Schutz personenbezogener Daten und einen weltweiten Standard geschaffen.

Der vorliegende Vorschlag ergänzt die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Richtlinie über offene Daten)[6]. Der vorliegende Vorschlag betrifft im Besitz öffentlicher Stellen befindliche Daten, die den Rechten Dritter unterliegen und daher nicht in den Anwendungsbereich dieser Richtlinie fallen. Der Vorschlag steht in logischer und kohärenter Verbindung zu den anderen in der europäischen Datenstrategie angekündigten Initiativen. Er zielt darauf ab, die gemeinsame Datennutzung zu erleichtern, u. a. durch die Stärkung des Vertrauens in die Mittler für die gemeinsame Datennutzung, die in den verschiedenen Datenräumen eingesetzt werden sollen. Er zielt nicht darauf ab, wesentliche Rechte auf den Zugang zu Daten und deren Nutzung zu gewähren, zu

---

1 Die endgültige Form des Rechtsakts wird durch den Inhalt des Instruments bestimmt.

2 COM(2020)66 final.

3 „Daten, deren Nutzung von den Rechten anderer abhängig ist“ oder „Daten, die den Rechten anderer unterliegen“, umfassen Daten, die Datenschutzvorschriften oder Rechten des geistigen Eigentums unterliegen oder Geschäftsgeheimnisse oder andere sensible Geschäftsinformationen enthalten können.

4 ABl. L 119 vom 4.5.2016, S. 1.

5 ABl. L 201 vom 31.7.2002, S. 37.

6 ABl. L 172 vom 26.6.2019, S. 56.

ändern oder zu beseitigen. Es ist geplant, diese Art von Maßnahmen in einen möglichen Rechtsakt über Daten (2021) aufzunehmen[7].

Das Instrument orientiert sich an den für Forschungsdaten entwickelten Grundsätzen für Datenmanagement und -weiterverwendung. Die FAIR-Datengrundsätze[8] sehen vor, dass solche Daten grundsätzlich auffindbar, zugänglich, interoperabel und weiterverwendbar sein sollten.

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

Sektorspezifische Rechtsvorschriften über den Datenzugang sind bereits in Kraft und/oder werden derzeit ausgearbeitet, um festgestellte Marktdefizite in Bereichen wie Automobilindustrie[9], Zahlungsdienstleister[10], Daten intelligenter Verbrauchsmesssysteme[11], Stromnetzdaten[12], intelligente Verkehrssysteme[13], Umweltinformationen[14], Geodaten[15] und Gesundheitswesen[16] zu beseitigen. Der vorliegende Vorschlag unterstützt die Nutzung von Daten, die im Rahmen bestehender Vorschriften zur Verfügung gestellt werden, ohne diese Vorschriften zu ändern oder neue sektorale Verpflichtungen zu schaffen.

Ebenso lässt der Vorschlag das Wettbewerbsrecht unberührt und steht im Einklang mit den Artikeln 101 und 102 AEUV; darüber hinaus lässt er auch die Bestimmungen der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt[17] unberührt.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Als einschlägige Rechtsgrundlage für diese Verordnung wurde Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union („AEUV“) herangezogen. Diesem Artikel zufolge erlässt die EU Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes in der EU zum Gegenstand haben. Diese Initiative ist Teil der europäischen Datenstrategie von 2020, die darauf abzielt, den Binnenmarkt für Daten zu stärken. Mit der wachsenden Digitalisierung von Wirtschaft und Gesellschaft besteht die Gefahr, dass die Mitgliedstaaten datenbezogene Fragen zunehmend ohne Koordinierung gesetzlich regeln, was die Fragmentierung des Binnenmarkts verstärken würde. Die Einrichtung von Governance-Strukturen und -Mechanismen, die zu einem koordinierten Ansatz für die Nutzung von Daten in allen Sektoren und Mitgliedstaaten führen, würde den Akteuren der Datenwirtschaft helfen, sich die Größe des Binnenmarkts zunutze zu machen. Dies wird zur Verwirklichung des

---

7 Siehe COM/2020/66 final.

8 https://www.force11.org/group/fairgroup/fairprinciples

9 ABl. L 188 vom 18.7.2009, S. 1, geändert durch ABl. L 151 vom 14.6.2018, S. 1.

10 ABl. L 337 vom 23.12.2015, S. 35.

11 ABl. L 158 vom 14.6.2019, S. 125; ABl. L 211 vom 14.8.2009, S. 94.

12 ABl. L 220 vom 25.8.2017, S. 1; ABl. L 113 vom 1.5.2015, S. 13.

13 ABl. L 207 vom 6.8.2010, S. 1.

14 ABl. L 41 vom 14.2.2003, S. 26.

15 ABl. L 108 vom 25.4.2007, S. 1.

16 Ein Vorschlag für einen Rechtsakt über den europäischen Gesundheitsdatenraum ist für das vierte Quartal 2021 geplant, https://eur-lex.europa.eu/search.html?lang=en&text=%22A+Union+of+vitality+in+a+world+of+fragility%22&qid=1605969128718&type=quick&scope=EURLEX&locale=de

17 ABl. L 178 vom 17.7.2000, S. 1.

Datenbinnenmarkts beitragen, indem die Entstehung und das grenzüberschreitende Funktionieren neuartiger Dienste durch eine Reihe harmonisierter Bestimmungen gewährleistet werden.

Die Digitalpolitik fällt in die geteilte Zuständigkeit der EU und ihrer Mitgliedstaaten. Nach Artikel 4 Absätze 2 und 3 AEUV kann die EU in den Bereichen Binnenmarkt und technologische Entwicklung spezifische Maßnahmen treffen, ohne die Handlungsfreiheit der Mitgliedstaaten in denselben Bereichen zu berühren.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Unternehmen benötigen häufig Daten aus mehreren Mitgliedstaaten, damit sie EU-weite Produkte und Dienstleistungen entwickeln können, da die in den einzelnen Mitgliedstaaten verfügbaren Datensätze oft nicht die Spannbreite und Vielfalt aufweisen, die eine „Big Data"-Mustererkennung oder maschinelles Lernen ermöglichen. Ferner müssen datenbasierte Produkte und Dienstleistungen, die in einem Mitgliedstaat entwickelt werden, möglicherweise an die Präferenzen der Kunden in einem anderen Mitgliedstaat angepasst werden, wozu lokale Daten auf der Ebene der Mitgliedstaaten erforderlich sind. Die Daten müssen problemlos durch EU-weite und sektorübergreifende Wertschöpfungsketten fließen können, wofür ein hochgradig harmonisiertes rechtliches Umfeld unerlässlich ist. Darüber hinaus kann in Anbetracht des grenzüberschreitenden Charakters der gemeinsamen Datennutzung und ihrer Bedeutung nur durch Maßnahmen auf Unionsebene sichergestellt werden, dass sich ein europäisches Datenaustauschmodell mit vertrauenswürdigen Datenmittlern für die gemeinsame B2B-Datennutzung und für persönliche Datenräume durchsetzt.

Ein Datenbinnenmarkt sollte sicherstellen, dass Daten des öffentlichen Sektors von Unternehmen und Bürgern so wirksam und verantwortungsvoll wie möglich abgerufen und genutzt werden können, während die Unternehmen und Bürger gleichzeitig die Kontrolle über die von ihnen erzeugten Daten behalten und die Investitionen in ihre Erhebung geschützt werden. Ein verbesserter Zugang zu Daten würde Unternehmen und Forschungseinrichtungen bei ihren repräsentativen wissenschaftlichen Entwicklungen und Marktinnovationen in der EU insgesamt voranbringen, was besonders in Situationen wichtig ist, in denen es eines koordinierten Vorgehens der EU bedarf, wie etwa in der COVID-19-Krise.

- **Verhältnismäßigkeit**

Die Initiative steht in einem angemessenen Verhältnis zu den angestrebten Zielen. Mit dem vorgeschlagenen Rechtsakt wird ein förderlicher Rahmen geschaffen, der nicht über das zur Erreichung der Ziele erforderliche Maß hinausgeht. Dadurch werden eine Reihe von Verfahren für die gemeinsame Datennutzung harmonisiert, wobei das Vorrecht der Mitgliedstaaten gewahrt bleibt, ihre Verwaltung zu organisieren und Rechtsvorschriften über den Zugang zu Informationen des öffentlichen Sektors zu erlassen. Der Anmelderahmen für Datenmittler sowie die Mechanismen für Datenaltruismus dienen dazu, ein höheres Maß an Vertrauen in diese Dienste zu erreichen, ohne die Tätigkeiten unnötig einzuschränken, und tragen zur Entwicklung eines Binnenmarkts für den Austausch solcher Daten bei. Die Initiative wird auch ein erhebliches Maß an Flexibilität für die Anwendung auf sektorspezifischer Ebene beinhalten, darunter für die künftige Entwicklung europäischer Datenräume.

Die vorgeschlagene Verordnung wird finanzielle und administrative Aufwendungen verursachen, die hauptsächlich von den nationalen Behörden, teilweise aber auch von den Datennutzern und den Anbietern für die gemeinsame Datennutzung getragen werden; dies ist

notwendig, um die Einhaltung der in der Verordnung festgelegten Verpflichtungen sicherzustellen. Die Auslotung verschiedener Optionen und ihrer erwarteten Kosten und Nutzeffekte hat jedoch zu einer ausgewogenen Gestaltung des Instruments geführt. So wird den nationalen Behörden genügend Flexibilität eingeräumt, sodass sie über die Höhe der finanziellen Investitionen entscheiden und Möglichkeiten zur Deckung dieser Kosten durch Verwaltungsgebühren oder -abgaben prüfen können, während gleichzeitig für eine Gesamtkoordinierung auf EU-Ebene gesorgt wird. Ebenso werden die Kosten für die Datennutzer und Anbieter für die gemeinsame Datennutzung durch die Vorteile ausgeglichen, die sich aus einem breiteren Datenzugang und einer breiteren Datennutzung sowie aus der Markteinführung neuartiger Dienste ergeben.

- **Wahl des Instruments**

Die Wahl einer Verordnung als Rechtsinstrument ist dadurch gerechtfertigt, dass Elemente überwiegen, die eine einheitliche Anwendung ohne Umsetzungsspielraum der Mitgliedstaaten erfordern und durch die ein vollständig horizontaler Rahmen geschaffen wird. Zu diesen Elementen zählen die Anmeldung für Anbieter von Diensten für die gemeinsame Datennutzung, die Mechanismen für Datenaltruismus, die Grundprinzipien für die Weiterverwendung von Daten des öffentlichen Sektors, die nicht als offene Daten zur Verfügung gestellt werden können oder nicht Gegenstand sektorspezifischer EU-Rechtsvorschriften sind, und die Einrichtung von Koordinierungsstrukturen auf europäischer Ebene. Da die Verordnung unmittelbar anwendbar wäre, würden der Umsetzungszeitraum und das Umsetzungsverfahren auf Ebene der Mitgliedstaaten vermieden und gleichzeitig die baldige Einrichtung gemeinsamer europäischer Datenräume im Einklang mit dem EU-Aufbauplan[18] ermöglicht.

Darüber hinaus sind die Bestimmungen der Verordnung nicht übermäßig präskriptiv und lassen den Mitgliedstaaten auf verschiedenen Ebenen Raum für Maßnahmen in Bezug auf Elemente, die den Zielen der Initiative nicht zuwiderlaufen, insbesondere die Organisation der zuständigen Einrichtungen, die öffentliche Stellen bei ihren Aufgaben im Zusammenhang mit der Weiterverwendung bestimmter Kategorien von Daten des öffentlichen Sektors unterstützen.

3. ERGEBNISSE DER EX-POST-BEWERTUNGEN, DER KONSULTATIONEN DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNGEN

- **Konsultation der Interessenträger**

Am 19. Februar 2020, dem Tag der Annahme der europäischen Datenstrategie[19], wurde eine öffentliche Online-Konsultation eingeleitet, die am 31. Mai 2020 endete. In der Konsultation wurde ausdrücklich darauf hingewiesen, dass sie der Vorbereitung der vorliegenden Initiative dienen sollte, weshalb sie Abschnitte und Fragen zu den in der Initiative behandelten Themen enthielt. Sie richtete sich an alle Arten von Interessenträgern.

Insgesamt gingen bei der Kommission 806 Beiträge ein, davon 219 von Unternehmen, 119 von Wirtschaftsverbänden, 201 von EU-Bürgern, 98 von Hochschul-/Forschungseinrichtungen und 57 von Behörden. Die Verbraucher wurden durch 7 Teilnehmer repräsentiert, und 54 Teilnehmer waren Nichtregierungsorganisationen (darunter 2 Umweltorganisationen). Von den 219 Unternehmen/Unternehmensverbänden waren 43,4 % KMU. Insgesamt kamen 92,2 % der Antworten aus der EU-27. Nur sehr

[18] COM(2020) 456 final.
[19] COM(2020) 66 final.

wenige Teilnehmer gaben an, ob ihre Organisation lokal, regional, national oder international tätig ist.

230 Positionspapiere wurden eingereicht, entweder als Anlage zu den Antworten auf den Fragebogen (210) oder als eigenständige Beiträge (20). Die Papiere gaben unterschiedliche Ansichten zu den Themen des Online-Fragebogens wieder, insbesondere in Bezug auf die Verwaltung gemeinsamer Datenräume. Sie enthielten Stellungnahmen zu den wichtigsten Grundsätzen für diese Räume und brachten eine große Unterstützung für die Priorisierung von Standards und für das Konzept des Datenaltruismus zum Ausdruck. Darüber hinaus wurde auf die Notwendigkeit von Schutzvorkehrungen bei der Entwicklung von Maßnahmen im Zusammenhang mit Datenmittlern hingewiesen.

- **Einholung und Nutzung von Expertenwissen**

Um die Rahmenbedingungen für die Schaffung gemeinsamer europäischer Datenräume in den ermittelten Sektoren gemeinsam mit den einschlägigen Experten zu sondieren, fanden 2019 eine Serie von 10 Workshops zu gemeinsamen europäischen Datenräumen und im Mai 2020 ein weiterer Workshop statt. Die Workshops, an denen insgesamt mehr als 300 Interessenträger, hauptsächlich aus dem privaten und dem öffentlichen Sektor, teilnahmen, betrafen verschiedene Sektoren (Landwirtschaft, Gesundheit, Finanzen/Banken, Energie, Verkehr, Nachhaltigkeit/Umwelt, öffentliche Dienstleistungen, intelligente Fertigung) und stärker bereichsübergreifende Aspekte (Datenethik, Datenmärkte). Die mit diesen Bereichen befassten Dienststellen der Kommission nahmen an den Workshops teil. Die sektoralen Workshops trugen dazu bei, gemeinsame Elemente aller Sektoren zu ermitteln, die durch die Festlegung eines horizontalen Governance-Rahmens angegangen werden müssen.

- **Folgenabschätzung**

Für diesen Vorschlag wurde eine Folgenabschätzung durchgeführt. Am 9. September 2020 gab der Ausschuss für Regulierungskontrolle eine ablehnende Stellungnahme ab. Am 5. Oktober 2020 gab der Ausschuss eine befürwortende Stellungnahme mit Vorbehalten ab.

In der Folgenabschätzung werden die Basisszenarien, die politischen Optionen und ihre Auswirkungen auf vier Interventionsbereiche untersucht, nämlich a) Mechanismen für die verstärkte Nutzung von Daten des öffentlichen Sektors, die nicht als offene Daten zur Verfügung gestellt werden können, b) einen Zertifizierungs- oder Kennzeichnungsrahmen für Datenmittler, c) Maßnahmen zur Förderung des Datenaltruismus und d) Mechanismen zur Koordinierung und Steuerung horizontaler Aspekte der Governance in Form einer Struktur auf EU-Ebene.

Für alle Interventionsbereiche wurde Option 1 – die Koordinierung auf EU-Ebene mit weichen Regulierungsmaßnahmen – als unzureichend erachtet, da sie die Situation gegenüber dem Basisszenario nicht wesentlich verändern würde. Die Hauptanalyse konzentrierte sich daher auf die Optionen 2 und 3, die Regulierungsmaßnahmen mit niedriger bzw. hoher Intensität vorsahen. Als bevorzugte Option stellte sich eine Kombination aus Regulierungsmaßnahmen mit niedrigerer und höherer Intensität heraus, und zwar in folgender Weise:

Im Hinblick auf Mechanismen für die verstärkte Nutzung bestimmter Daten des öffentlichen Sektors, deren Nutzung den Rechten anderer unterliegt, würden sowohl durch die Optionen mit niedriger als auch diejenigen mit hoher Intensität EU-weite Vorschriften für die Weiterverwendung solcher Informationen eingeführt (insbesondere die Nichtausschließlichkeit). Regulierungsmaßnahmen mit niedriger Intensität würden

voraussetzen, dass einzelne öffentliche Stellen, die diese Art der Weiterverwendung erlauben, technisch so ausgestattet wären, dass Datenschutz, Privatsphäre und Vertraulichkeit in vollem Umfang gewahrt blieben. Damit wäre auch eine Verpflichtung für die Mitgliedstaaten verbunden, zumindest eine zentrale Anlaufstelle für Anträge auf Zugang zu solchen Daten vorzusehen, ohne ihre genaue institutionelle und administrative Form festzulegen. Die Option mit hoher Intensität sah pro Mitgliedstaat die Einrichtung einer zentralen Genehmigungsstelle vor. Angesichts der damit verbundenen Kosten und Durchführbarkeitsfragen ist die Regulierung mit niedrigerer Intensität die bevorzugte Option.

Für die Zertifizierung oder Kennzeichnung vertrauenswürdiger Datenmittler wurde eine Regulierung mit niedrigerer Intensität in Form eines weicheren, freiwilligen Kennzeichnungsmechanismus ins Auge gefasst, bei dem eine Prüfung der Einhaltung der Anforderungen für den Erwerb und die Erteilung der Kennzeichnung durch die von den Mitgliedstaaten benannten zuständigen Behörden erfolgen würde (bei denen es sich auch um die zentralen Anlaufstellen handeln kann, die für die verstärkte Weiterverwendung von Daten des öffentlichen Sektors eingerichtet werden können). Die Regulierungsmaßnahme mit hoher Intensität bestand in einem obligatorischen Zertifizierungssystem, das von privaten Konformitätsbewertungsstellen verwaltet wird. Da ein obligatorisches System mit höheren Kosten verbunden wäre, das potenziell prohibitive Auswirkungen auf KMU und Start-ups haben könnte, und da der Markt noch nicht reif für ein obligatorisches Zertifizierungssystem ist, wurde eine Regulierung mit niedrigerer Intensität als bevorzugte politische Option ermittelt. Die Regulierungsmaßnahme mit höherer Intensität in Form eines obligatorischen Systems wurde dennoch auch als gangbare Alternative angesehen, da sie das Vertrauen in die Funktionsweise der Datenmittler deutlich erhöhen und klare Regeln dafür schaffen würde, wie diese Mittler auf dem europäischen Datenmarkt agieren sollen. Nach weiteren Erörterungen in der Kommission wurde eine Zwischenlösung gewählt. Sie besteht in einer Anmeldepflicht mit einer nachträglichen Kontrolle der Einhaltung der Anforderungen für die Ausübung der Tätigkeiten durch die zuständigen Behörden der Mitgliedstaaten. Diese Lösung bietet den Vorteil einer verbindlichen Regelung, während der Verwaltungsaufwand für die Marktteilnehmer begrenzt wird.

In Bezug auf den Datenaltruismus bestand die Regulierungsmaßnahme mit niedrigerer Intensität in einem freiwilligen Zertifizierungsrahmen für Organisationen, die solche Dienste anbieten wollen, während die Regulierung mit hoher Intensität einen obligatorischen Genehmigungsrahmen vorsah. Letztere wurde in der Folgenabschätzung als bevorzugte Option für diesen Interventionsbereich herausgestellt, da sie – bei vergleichbaren Kosten – ein höheres Maß an Vertrauen in die Datenbereitstellung gewährleisten würde und so dazu beitragen könnte, dass mehr Daten von betroffenen Personen und Unternehmen zur Verfügung gestellt würden und ein höheres Entwicklungs- und Forschungsniveau erreicht würde. In den weiteren Erörterungen innerhalb der Kommission wurden jedoch zusätzliche Bedenken hinsichtlich des potenziellen Verwaltungsaufwands für Organisationen, die Datenaltruismus betreiben, und im Hinblick darauf geäußert, wie sich die Verpflichtungen auf künftige sektorale Datenaltruismus-Initiativen auswirken könnten. Aus diesem Grund wurde eine alternative Lösung gewählt, bei der Organisationen, die Datenaltruismus betreiben, die Möglichkeit erhalten, sich als „in der Union anerkannte datenaltruistische Organisation“ eintragen zu lassen. Dieser Mechanismus der Freiwilligkeit wird zur Erhöhung des Vertrauens beitragen und im Vergleich mit sowohl der Regelung für obligatorische Genehmigungen als auch der Regelung für freiwillige Zertifizierungen einen geringeren Verwaltungsaufwand verursachen.

Was schließlich den horizontalen europäischen Governance-Mechanismus betrifft, so sah die Regulierungsmaßnahme mit niedriger Intensität die Einrichtung einer Expertengruppe vor, während die Regulierungsmaßnahme mit hoher Intensität in der Schaffung einer unabhängigen Struktur mit Rechtspersönlichkeit (ähnlich dem Europäischen Datenschutzausschuss) bestand. Angesichts der hohen Kosten und der geringen politischen Durchführbarkeit, die mit der Einführung der Option mit höherer Intensität verbunden waren, wurde die politische Option mit niedriger Intensität gewählt.

In der Studie zur Unterstützung der Folgenabschätzung[20] wurde darauf hingewiesen, dass nach dem Basisszenario die Datenwirtschaft und der wirtschaftliche Wert der gemeinsamen Datennutzung auf schätzungsweise 533–510 Mrd. EUR (3,87 % des BIP) anwachsen dürften, während sich dieser Wert bei der bevorzugten gebündelten Option auf 540,7–544,4 Mrd. EUR (3,92 % bis 3,95 % des BIP) erhöhen würde. Bei diesen Beträgen werden die nachgelagerten Vorteile in Form besserer Produkte, höherer Produktivität und neuer Wege zur Bewältigung gesellschaftlicher Herausforderungen (z. B. Klimawandel) nur begrenzt berücksichtigt. Diese Vorteile dürften in der Tat erheblich größer sein als die direkten Vorteile.

Gleichzeitig würde diese gebündelte politische Option es ermöglichen, ein europäisches Modell für die gemeinsame Datennutzung zu schaffen, das durch die Entstehung neutraler Datenmittler eine Alternative zum derzeitigen Geschäftsmodell integrierter Technologieplattformen böte. Diese Initiative kann für die Datenwirtschaft von Vorteil sein, da sie Vertrauen in die gemeinsame Datennutzung und Anreize für die Entwicklung gemeinsamer europäischer Datenräume schafft, in denen natürliche und juristische Personen die Kontrolle über die von ihnen erzeugten Daten haben.

- **Grundrechte**

Da einige Elemente der Verordnung personenbezogene Daten betreffen, wurden die Maßnahmen so konzipiert, dass sie den Datenschutzvorschriften in vollem Umfang entsprechen und in der Praxis die Kontrolle natürlicher Personen über die von ihnen erzeugten Daten tatsächlich stärken.

Was die verstärkte Weiterverwendung von Daten des öffentlichen Sektors anbelangt, so werden die grundlegenden Rechte auf Datenschutz, Privatsphäre und Eigentum (Eigentumsrechte an bestimmten Daten, die z. B. Geschäftsgeheimnisse enthalten oder durch Rechte des geistigen Eigentums geschützt sind) gewahrt. Auch Anbieter von Diensten für die gemeinsame Datennutzung, die Dienste für betroffene Personen erbringen, müssen die geltenden Datenschutzvorschriften einhalten.

Der Anmelderahmen für Datenmittler würde in die unternehmerische Freiheit eingreifen, da er bestimmte Beschränkungen in Form unterschiedlicher Anforderungen als Voraussetzung für das Funktionieren solcher Einrichtungen vorsehen würde.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Dieser Vorschlag hat keine Auswirkungen auf den Haushalt.

[20] Europäische Kommission (2020, noch nicht erschienen). *Studie zur Unterstützung dieser Folgenabschätzung*, SMART 2019/0024, erstellt von Deloitte.

5. WEITERE ANGABEN

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

Aufgrund des dynamischen Charakters der Datenwirtschaft ist die Überwachung der Entwicklung der Auswirkungen ein wesentlicher Bestandteil der Maßnahmen in diesem Bereich. Um sicherzustellen, dass die ausgewählten politischen Maßnahmen tatsächlich zu den angestrebten Ergebnissen führen, und um etwaige künftige Überarbeitungen zu ermöglichen, ist es erforderlich, die Durchführung dieser Verordnung zu überwachen und zu bewerten.

Die Überwachung der spezifischen Ziele und der rechtlichen Verpflichtungen wird durch elektronische Befragungen von Interessenträgern, durch die Arbeit des Unterstützungszentrums für die gemeinsame Datennutzung, durch Aufzeichnungen des Europäischen Dateninnovationsrats zu den verschiedenen von den zuständigen nationalen Behörden gemeldeten Interventionsbereichen und durch eine Bewertungsstudie zur Unterstützung der Überprüfung des Instruments erfolgen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

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

Kapitel II schafft einen Mechanismus für die Weiterverwendung bestimmter Kategorien geschützter Daten des öffentlichen Sektors, die der Achtung der Rechte anderer unterliegen (insbesondere aus Gründen des Schutzes personenbezogener Daten, aber auch des Schutzes der Rechte des geistigen Eigentums und des Geschäftsgeheimnisses). Dieser Mechanismus lässt sektorspezifische EU-Rechtsvorschriften über den Zugang zu diesen Daten und deren Weiterverwendung unberührt. Die Weiterverwendung solcher Daten fällt nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024 (Richtlinie über offene Daten). Die Bestimmungen dieses Kapitels begründen kein Recht auf Weiterverwendung solcher Daten, sondern sehen eine Reihe harmonisierter grundlegender Bedingungen vor, unter denen die Weiterverwendung solcher Daten erlaubt werden kann (z. B. das Erfordernis der Nichtausschließlichkeit). Öffentliche Stellen, die diese Art der Weiterverwendung erlauben, müssen technisch so ausgestattet sein, dass Datenschutz, Privatsphäre und Vertraulichkeit in vollem Umfang gewahrt bleiben. Die Mitgliedstaaten müssen eine zentrale Anlaufstelle einrichten, die Forscher und innovative Unternehmen bei der Ermittlung geeigneter Daten unterstützt, und müssen Strukturen schaffen, die öffentliche Stellen mit technischen Mitteln und rechtlicher Beratung unterstützen.

Kapitel III zielt darauf ab, das Vertrauen in die gemeinsame Nutzung personenbezogener und nicht personenbezogener Daten zu stärken und die Transaktionskosten im Zusammenhang mit der gemeinsamen B2B- und C2B-Datennutzung zu senken, indem eine Anmelderegelung für Anbieter für die gemeinsame Datennutzung geschaffen wird. Die Anbieter werden eine Reihe von Anforderungen zu erfüllen haben; dabei müssen sie insbesondere neutral in Bezug auf die ausgetauschten Daten bleiben. Sie dürfen diese Daten nicht für andere Zwecke verwenden. Bei Anbietern, die Dienste für die gemeinsame Datennutzung für natürliche Personen erbringen, muss auch das zusätzliche Kriterium der Übernahme treuhänderischer Pflichten gegenüber den Personen, die diese Dienste nutzen, erfüllt sein.

Mit diesem Ansatz soll sichergestellt werden, dass die Dienste für die gemeinsame Datennutzung offen und kooperativ funktionieren, wobei gleichzeitig die Position natürlicher und juristischer Personen gestärkt wird, indem ihnen ein besserer Überblick und eine bessere Kontrolle über ihre Daten ermöglicht wird. Eine von den Mitgliedstaaten benannte zuständige Behörde wird für die Überwachung der Einhaltung der mit der Bereitstellung dieser Dienste verbundenen Anforderungen zuständig sein.

Kapitel IV erleichtert Datenaltruismus (freiwillige Datenbereitstellung durch Einzelpersonen oder Unternehmen zum Wohl der Allgemeinheit). Dazu ist die Möglichkeit vorgesehen, dass sich Organisationen, die Datenaltruismus betreiben, als „in der Union anerkannte datenaltruistische Organisation“ eintragen lassen, um das Vertrauen in ihre Tätigkeiten zu stärken. Darüber hinaus wird ein gemeinsames europäisches Einwilligungsformular für Datenaltruismus entwickelt, um die Kosten für die Einholung der Einwilligung zu senken und die Übertragbarkeit der Daten zu erleichtern (wenn die zur Verfügung zu stellenden Daten nicht im Besitz der betroffenen Person sind).

Kapitel V enthält die Anforderungen an die Arbeitsweise der zuständigen Behörden, die für die Überwachung und Umsetzung des Anmelderahmens für Anbieter von Diensten für die gemeinsame Datennutzung und für Datenaltruismus betreibende Einrichtungen benannt wurden. Außerdem enthält es Bestimmungen über das Recht, Beschwerde gegen Entscheidungen dieser Stellen einzulegen, und über die Rechtsbehelfe.

Mit **Kapitel VI** wird eine formale Expertengruppe (der „Europäische Dateninnovationsrat“) eingesetzt, die die Entwicklung bewährter Verfahren durch die Behörden der Mitgliedstaaten erleichtern wird, insbesondere mit Blick auf die Bearbeitung von Anträgen auf Weiterverwendung von Daten, die den Rechten anderer unterliegen (gemäß Kapitel II), die Sicherstellung einer einheitlichen Vorgehensweise in Bezug auf den Anmelderahmen für die Anbieter von Diensten für die gemeinsame Datennutzung (Kapitel III) und den Datenaltruismus (Kapitel IV). Darüber hinaus wird die formal eingesetzte Expertengruppe die Kommission bei der Steuerung der sektorübergreifenden Normung und der Ausarbeitung strategischer sektorübergreifender Normungsaufträge unterstützen und beraten. In diesem Kapitel werden auch die Zusammensetzung der Expertengruppe und ihre Arbeitsweise geregelt.

Kapitel VII ermöglicht der Kommission den Erlass von Durchführungsrechtsakten in Bezug auf das europäische Einwilligungsformular für Datenaltruismus.

In **Kapitel VIII** sind Übergangsbestimmungen für das Funktionieren der allgemeinen Erlaubnisregelung für Anbieter von Diensten für die gemeinsame Datennutzung sowie Schlussbestimmungen festgelegt.

2020/0340 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über europäische Daten-Governance (Daten-Governance-Gesetz)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

nach Stellungnahme des Ausschusses der Regionen[22],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Der Vertrag über die Arbeitsweise der Europäischen Union (AEUV) sieht die Schaffung eines Binnenmarkts und die Einführung eines Systems vor, das Wettbewerbsverzerrungen im Binnenmarkt verhindert. Die Festlegung von Regeln und Verfahren in den Mitgliedstaaten in Bezug auf den Aufbau eines gemeinsamen Rahmens für die Daten-Governance ist, dürfte zu diesen Zielen beitragen.

(2) In nur wenigen Jahren hat die Digitaltechnik mit ihrem Einfluss auf alle Tätigkeitsbereiche und das tägliche Leben die Wirtschaft und Gesellschaft tiefgreifend verändert. Daten stehen im Mittelpunkt dieses Wandels: Die von Daten vorangetriebene Innovation wird den Bürgerinnen und Bürgern enorme Vorteile bringen, beispielsweise durch eine verbesserte personalisierte Medizin, durch eine neue Mobilität und durch ihren Beitrag zum europäischen Grünen Deal[23]. In ihrer Datenstrategie[24] erläuterte die Kommission ihre Vorstellung eines gemeinsamen europäischen Datenraums, d. h. eines Binnenmarkts für Daten, in dem Daten unabhängig vom physischen Ort ihrer Speicherung in der Union unter Einhaltung des geltenden Rechts verwendet werden können. Zudem forderte sie einen freien und sicheren Datenverkehr mit Drittländern, wobei allerdings Ausnahmen und Beschränkungen im Zusammenhang mit der öffentlichen Sicherheit, der öffentlichen Ordnung und anderen berechtigten Zielen des Gemeinwohls in der Europäischen

[21] ABl. C … vom …, S. ….

[22] ABl. C … vom …, S. ….

[23] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Der europäische Grüne Deal, COM(2019) 640 final.

[24] COM(2020) 66 final.

Union sowie internationale Verpflichtungen zu beachten sind. Damit hieraus Realität wird, schlägt sie vor, zur Konkretisierung dieser Vision gemeinsame europäische Datenräume für verschiedene Bereiche einzurichten, in denen Daten gemeinsam genutzt und gebündelt werden können. Wie bereits in der Strategie angedacht, können sich solche gemeinsamen europäischen Datenräume auf Bereiche wie Gesundheit, Mobilität, Fertigung, Finanzdienstleistungen, Energie und Landwirtschaft oder auf Themen wie den europäischen Grünen Deal oder europäische Datenräume für die öffentliche Verwaltung oder Qualifikationen erstrecken.

(3) Es ist notwendig, die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt zu verbessern und dazu einen harmonisierten Rahmen für den Datenaustausch zu schaffen. Mit sektorspezifischen Vorschriften, wie beispielsweise zum europäischen Gesundheitsdatenraum[25] und zum Zugang zu Fahrzeugdaten, können je nach den Besonderheiten eines Sektors neue und ergänzende Elemente entwickelt, angepasst und vorgeschlagen werden. Zudem werden bestimmte Wirtschaftssektoren bereits durch sektorspezifisches Unionsrecht reguliert. Hierunter fallen die Vorschriften für die grenzüberschreitende bzw. unionsweite gemeinsame Nutzung von Daten und den Zugang zu Daten[26]. Daher bleiben folgende Rechtsvorschriften von dieser Verordnung unberührt: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[27] (insbesondere darf die Durchführung der vorliegenden Verordnung die grenzüberschreitende Übertragung von Daten nach Kapitel V der Verordnung (EU) 2016/679 nicht verhindern), Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[28], Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates[29], Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates[30], Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates[31],

---

25 Siehe: Anhänge der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Arbeitsprogramm der Kommission 2021, COM(2020) 690 final.

26 Beispielsweise die Richtlinie 2011/24/EU im Zusammenhang mit dem europäischen Gesundheitsdatenraum sowie das einschlägige Verkehrsrecht, z. B. Richtlinie 2010/40/EU, Verordnung (EU) 2019/1239 und Verordnung (EU) 2020/1056 mit Blick auf den europäischen Mobilitätsdatenraum.

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

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

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

30 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (ABl. L 303 vom 28.11.2018, S. 59).

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

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates[32], Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates[33], Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates[34], Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates[35], Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates[36] sowie Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates[37], Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates[38] und auf deren Grundlage erlassene delegierte Verordnungen sowie andere sektorspezifische Unionsvorschriften für den Zugang zu Daten und deren Weiterverwendung. Auch der Zugang zu Daten und deren Weiterverwendung für Zwecke der internationalen Zusammenarbeit bei der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sollte von dieser Verordnung unberührt bleiben. Für die Weiterverwendung geschützter und im Besitz öffentlicher Stellen befindlicher Daten bestimmter Kategorien sowie für die Erbringung von Diensten für die gemeinsame Datennutzung und von auf Datenaltruismus beruhenden Diensten in der Union sollte eine horizontale Regelung geschaffen werden. Aufgrund der Besonderheiten verschiedener Sektoren kann es erforderlich sein, ausgehend von den Anforderungen dieser Verordnung sektorale datengestützte Systeme zu konzipieren. Sind öffentliche Stellen, Anbieter von Diensten für die gemeinsame Datennutzung oder eingetragene Einrichtungen, die Datenaltruismus-Dienste anbieten, aufgrund sektorspezifischer Unionsvorschriften verpflichtet, bestimmte zusätzliche technische, administrative oder organisatorische Bestimmungen einzuhalten, etwa im Rahmen von Genehmigungs- oder Zertifizierungsverfahren, sollten auch diese Bestimmungen der sektorspezifischen Unionsvorschriften Anwendung finden.

(4) Auf Unionsebene besteht Handlungsbedarf, denn es gilt, die Hemmnisse für eine gut funktionierende Datenwirtschaft abzubauen und einen unionsweiten Rechtsrahmen für den Zugang zu Daten und für deren Verwendung zu schaffen. Dies bezieht sich insbesondere auf die Weiterverwendung bestimmter Arten von Daten, die im Besitz des öffentlichen Sektors sind, die Erbringung von Diensten für gewerbliche Nutzer und betroffene Personen durch Anbieter von Diensten für die gemeinsame

---

32 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr) (ABl. L 178 vom 17.7.2000, S. 1).

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

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

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

36 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172 vom 26.6.2019, S. 56).

37 Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG (ABl. L 151 vom 14.6.2018, S. 1).

38 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 vom 6.8.2010, S. 1).

Datennutzung sowie auf die Sammlung und Verarbeitung von Daten, die von natürlichen und juristischen Personen für altruistische Zwecke zur Verfügung gestellt werden.

(5) Die Vorstellung, dass Daten, die mithilfe öffentlicher Gelder generiert wurden, auch der Gesellschaft zugutekommen sollten, hat seit Langem Eingang in die Strategie der Union gefunden. Die Richtlinie (EU) 2019/1024 sowie sektorspezifische Vorschriften zielen darauf ab, dass der öffentliche Sektor die Zugänglichkeit der von ihm erzeugten Daten für die Verwendung und Weiterverwendung in größerem Umfang erleichtert. Dennoch werden in öffentlichen Datenbanken vorhandene Daten bestimmter Kategorien oft nicht einmal für Forschungszwecke oder innovative Tätigkeiten zur Verfügung gestellt (vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten, durch die Rechte Dritter am geistigen Eigentum geschützte Daten, Geschäftsgeheimnisse und personenbezogene Daten, zu denen aufgrund bestimmter nationaler Vorschriften oder des Unionsrechts, wie der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680, kein Zugang gewährt werden darf). Zur Wahrung der Rechte Dritter an diesen sensiblen Daten müssen bestimmte verfahrenstechnische und rechtliche Hürden überwunden werden, bevor solche Daten zur Verfügung gestellt werden können. Die Überwindung dieser Hürden braucht in der Regel viel Zeit und Sachverstand, weshalb solche Daten bislang kaum genutzt werden. Zwar haben einige Mitgliedstaaten Strukturen und Verfahren geschaffen und mitunter Vorschriften erlassen, um die Weiterverwendung dieser Art von Daten zu erleichtern, doch gilt das nicht für die gesamte Union.

(6) Für Datenbanken, die personenbezogene Daten enthalten, gibt es Techniken, die datenschutzfreundliche Analysen ermöglichen, z. B. Anonymisierung, Pseudonymisierung, differentielle Privatsphäre, Generalisierung oder Datenunterdrückung und Randomisierung. Mithilfe dieser dem Schutz der Privatsphäre dienenden Techniken im Verbund mit umfassenden Datenschutzkonzepten dürfte eine sichere Weiterverwendung personenbezogener Daten und vertraulicher Geschäftsdaten für Forschung, Innovation und statistische Zwecke gewährleistet werden können. In vielen Fällen bedeutet dies, dass es für die Verwendung und Weiterverwendung von Daten in diesem Zusammenhang einer sicheren Verarbeitungsumgebung bedarf, die vom öffentlichen Sektor eingerichtet und beaufsichtigt wird. Auf Unionsebene gibt es Erfahrungen mit solchen sicheren Verarbeitungsumgebungen, die auf der Grundlage der Verordnung (EU) Nr. 557/2013 der Kommission[39] für Forschungsarbeiten zu statistischen Mikrodaten genutzt werden. Allgemein sollte die Verarbeitung personenbezogener Daten stets auf einem der Rechtsgründe beruhen, die in Artikel 6 der Verordnung (EU) 2016/679 aufgeführt sind.

(7) Daten, die sich in Besitz öffentlicher Stellen befinden und unter die Kategorien fallen, für die eine Weiterverwendung nach dieser Verordnung infrage kommen, fallen nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024, die Daten ausschließt, die unzugänglich sind, weil es sich um vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten oder durch Rechte Dritter am geistigen Eigentum geschützte Daten handelt. Die Richtlinie (EU) 2019/1024 erfasst nämlich keine personenbezogenen Daten, da nach ihren Zugangsregelungen der

[39] Verordnung (EU) Nr. 557/2013 der Kommission vom 17. Juni 2013 zur Durchführung der Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates über europäische Statistiken in Bezug auf den Zugang zu vertraulichen Daten für wissenschaftliche Zwecke und zur Aufhebung der Verordnung (EG) Nr. 831/2002 der Kommission (ABl. L 164 vom 18.6.2013, S. 16).

Zugang zu diesen Daten aus Gründen des Datenschutzes, des Schutzes der Privatsphäre und der Integrität des Einzelnen nach den Datenschutzvorschriften ausgeschlossen oder eingeschränkt ist. Die Weiterverwendung von Daten, die möglicherweise Geschäftsgeheimnisse enthalten, sollte unbeschadet der Richtlinie (EU) 2016/943[40] erfolgen, die den Rahmen für die Rechtmäßigkeit von Erwerb, Nutzung oder Offenlegung von Geschäftsgeheimnissen festlegt. Auf Unionsebene oder nationaler Ebene geltende Vorschriften, die im Einzelnen noch genauer festlegen, welche Bedingungen öffentliche Stellen an die Weiterverwendung von Daten knüpfen müssen, sollten von dieser Verordnung unberührt bleiben und von ihr ergänzt werden.

(8) Die in dieser Verordnung enthaltene Weiterverwendungsregelung sollte für Daten gelten, deren Bereitstellung in den Mitgliedstaaten unter den gesetzlich oder anderweitig verbindlich festgelegten öffentlichen Auftrag der betreffenden öffentlichen Stellen fällt. Bestehen keine entsprechenden Vorschriften, sollte der Umfang des öffentlichen Auftrags, unter der Voraussetzung, dass er transparent ist und überprüft wird, im Einklang mit der allgemeinen Verwaltungspraxis der Mitgliedstaaten festgelegt werden. Der öffentliche Auftrag könnte allgemein oder für einzelne öffentliche Stellen fallbezogen festgelegt werden. Da die Begriffsbestimmung für öffentliche Stellen keine öffentlichen Unternehmen erfasst, sollten die in deren Besitz befindlichen Daten nicht unter diese Verordnung fallen. Auch sollte diese Verordnung nicht für Daten gelten, die sich im Besitz von Kultur- oder Bildungseinrichtungen befinden und bei denen die Rechte des geistigen Eigentums keine Nebenrechte darstellen, sondern in Bezug auf derart eigentumsrechtlich geschützte Werke und sonstigen Dokumente Hauptrechte sind.

(9) Bei der Festlegung der Grundsätze für die Weiterverwendung der in ihrem Besitz befindlichen Daten sollten öffentliche Stellen das Wettbewerbsrecht einhalten und den Abschluss von Vereinbarungen möglichst vermeiden, deren Ziel oder Wirkung darin bestehen könnte, für die Weiterverwendung bestimmter Daten ausschließliche Rechte zu begründen. Solche Vereinbarungen sollten nur dann zulässig sein, wenn sie sich aus Gründen rechtfertigen lassen, die in der Erbringung eines Dienstes von allgemeinem Interesse liegen, und sie hierfür notwendig sind. Dies könnte der Fall sein, wenn sich nur mit ihrer ausschließlichen Verwendung ein optimaler gesellschaftlicher Nutzen der betreffenden Daten erzielen lässt, weil es beispielsweise nur eine Einrichtung gibt (die sich auf die Verarbeitung eines bestimmten Datensatzes spezialisiert hat), die einen Dienst oder ein Produkt erbringen kann, mit dem eine öffentliche Stelle in die Lage versetzt wird, einen fortgeschrittenen digitalen Dienst im allgemeinen Interesse zu erbringen. Solche Vereinbarungen sollten jedoch im Einklang mit den öffentlichen Vergabevorschriften geschlossen werden und einer regelmäßigen Überprüfung anhand von Marktanalysen unterzogen werden, damit festgestellt werden kann, ob die Gewährung der Ausschließlichkeit nach wie vor notwendig ist. Ferner sollten solche Vereinbarungen gegebenenfalls den einschlägigen Vorschriften über staatliche Beihilfen entsprechen und nur für einen begrenzten Zeitraum, der drei Jahre nicht überschreiten sollte, geschlossen werden. Im Sinne der Transparenz sollten solche Ausschließlichkeitsvereinbarungen im Internet veröffentlicht werden, unabhängig von einer etwaigen Veröffentlichung der Vergabe eines öffentlichen Auftrags.

(10) Bereits vor Inkrafttreten dieser Verordnung bestehende und nunmehr verbotene Ausschließlichkeitsvereinbarungen und sonstige Praktiken oder Vereinbarungen zwischen Inhabern und Weiterverwendern von Daten, die zwar keine

[40] ABl. L 157 vom 15.6.2016, S. 1.

Ausschließlichkeitsrechte gewähren, bei denen jedoch nach vernünftigem Ermessen davon ausgegangen werden kann, dass sie die Verfügbarkeit von Daten für die Weiterverwendung einschränken, sollten nach Ablauf ihrer Gültigkeit nicht erneuert werden. Unbefristete oder langfristige Vereinbarungen sollten innerhalb von drei Jahren nach Inkrafttreten dieser Verordnung beendet werden.

(11) Es sollten Bedingungen für die Weiterverwendung geschützter Daten festgelegt werden, die für öffentliche Stellen gelten, die nach nationalem Recht dafür zuständig sind, die Weiterverwendung zu erlauben, wobei die Rechte und Pflichten in Bezug auf den Zugang zu solchen Daten unberührt bleiben sollten. Solche Bedingungen sollten nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen den Wettbewerb nicht einschränken. Öffentliche Stellen, die die Weiterverwendung von Daten erlauben, sollten insbesondere über die für den Schutz der Rechte und Interessen Dritter erforderlichen technischen Mittel verfügen. Die Bedingungen für die Weiterverwendung von Daten sollten sich darauf beschränken, was zur Wahrung der Rechte und Interessen anderer an den Daten und der Integrität der Informatik- und Kommunikationssysteme der öffentlichen Stellen notwendig ist. Die von öffentlichen Stellen auferlegten Bedingungen sollten den Interessen der Weiterverwender bestmöglich dienen, ohne dass dem öffentlichen Sektor hieraus ein unverhältnismäßig hoher Aufwand erwächst. Abhängig vom jeweiligen Fall sollten personenbezogene Daten vor ihrer Übermittlung vollständig anonymisiert werden, sodass definitiv ausgeschlossen ist, dass die Betroffenen identifiziert werden können, oder Daten, die vertrauliche Geschäftsinformationen enthalten, so verändert werden, dass keine vertraulichen Informationen offengelegt werden. Entspricht die Bereitstellung anonymisierter oder veränderter Daten nicht dem Bedarf des Weiterverwenders, könnte die Weiterverwendung der Daten in den Räumlichkeiten der öffentlichen Stelle oder der Fernzugang zur Verarbeitung in einer sicheren Verarbeitungsumgebung erlaubt werden. Die Datenanalysen in solchen sicheren Verarbeitungsumgebungen sollten von der öffentlichen Stelle beaufsichtigt werden, damit die Rechte und Interessen Dritter geschützt werden. Insbesondere sollten personenbezogene Daten nur dann zur Weiterverwendung an Dritte übermittelt werden, wenn es hierfür eine Rechtsgrundlage gibt. Öffentliche Stellen könnten den Rückgriff auf solche sicheren Verarbeitungsumgebungen davon abhängig machen, dass der Weiterverwender eine Vertraulichkeitsvereinbarung unterschreibt, die es ihm untersagt, Informationen offenzulegen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, wenn dadurch die Rechte und Interessen Dritter verletzt würden. Öffentliche Stellen sollten gegebenenfalls die Weiterverwendung von Daten auf der Grundlage der Einwilligung bzw. Erlaubnis der betroffenen natürlichen und juristischen Personen zur Weiterverwendung ihrer Daten mit geeigneten technischen Mitteln erleichtern. In diesem Zusammenhang sollten öffentliche Stellen die potenziellen Weiterverwender der Daten bei der Einholung dieser Einwilligung oder Erlaubnis unterstützen, indem sie technische Mechanismen schaffen, mit denen Einwilligungsanfragen der Weiterverwender weitergeleitet werden können, soweit dies praktikabel ist. Dabei sollten keine Kontaktangaben weitergegeben werden, die es Weiterverwendern ermöglichen würden, die betreffenden natürlichen oder juristischen Personen direkt zu kontaktieren.

(12) Rechte Dritter am geistigen Eigentum sollten von dieser Verordnung unberührt bleiben. Diese Verordnung berührt weder bestehende Rechte öffentlicher Stellen am geistigen Eigentum oder deren Inhaberschaft daran, noch schränkt sie die Ausübung dieser Rechte über die in dieser Verordnung gesetzten Grenzen hinaus ein. Die sich aus dieser Verordnung ergebenden Verpflichtungen sollten nur insoweit gelten, wie

sie mit völkerrechtlichen Übereinkommen zum Schutz der Rechte des geistigen Eigentums, insbesondere der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (Berner Übereinkunft), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS-Übereinkommen) und dem WIPO-Urheberrechtsvertrag (WCT) vereinbar sind. Öffentliche Stellen sollten ihre Urheberrechte jedoch auf eine Weise ausüben, die eine Weiterverwendung erleichtert.

(13) Daten, für die Rechte des geistigen Eigentums gelten, sowie Geschäftsgeheimnisse sollten nur dann an Dritte übermittelt werden, wenn diese Übermittlung nach Unionsrecht oder nationalem Recht rechtmäßig ist oder die Zustimmung des Rechteinhabers vorliegt. Sofern öffentliche Stellen Rechteinhaber nach Artikel 7 Absatz 1 der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates[41] sind, sollten sie dieses Recht nicht in Anspruch nehmen, um die Weiterverwendung der Daten zu verhindern oder über die in dieser Verordnung festgelegten Beschränkungen hinaus einzuschränken.

(14) Juristische und natürliche Personen sollten darauf vertrauen können, dass die Weiterverwendung von geschützten Daten bestimmter Kategorien, die sich im Besitz des öffentlichen Sektors befinden, in einer Art und Weise erfolgt, die ihre Rechte und Interessen wahrt. Daher sollten zusätzliche Schutzvorkehrungen für Situationen getroffen werden, in denen die Weiterverwendung solcher Daten des öffentlichen Sektors so erfolgt, dass Daten außerhalb des öffentlichen Sektors verarbeitet werden. Solche zusätzlichen Schutzvorkehrungen könnten darin bestehen, dass öffentliche Stellen die Rechte und Interessen natürlicher und juristischer Personen (insbesondere den Schutz personenbezogener Daten und sensibler Geschäftsdaten sowie den Schutz der Rechte des geistigen Eigentums) in vollem Umfang berücksichtigen, wenn solche Daten in Drittländer übertragen werden.

(15) Außerdem gilt es, nicht personenbezogene sensible Geschäftsdaten, vor allem Geschäftsgeheimnisse, aber auch nicht personenbezogene Daten von Inhalten, die durch Rechte des geistigen Eigentums geschützt sind, vor unrechtmäßigem Zugriff, der möglicherweise den Diebstahl geistigen Eigentums oder Industriespionage zur Folge hat, zu schützen. Zum Schutz der Grundrechte oder Interessen der Dateninhaber sollten nicht personenbezogene Daten, die nach Unionsrecht oder nationalem Recht vor unrechtmäßigem oder unbefugtem Zugriff geschützt werden sollen und die sich im Besitz öffentlicher Stellen befinden, nur dann in Drittländer übertragen werden, wenn angemessene Schutzvorkehrungen für die Nutzung der Daten getroffen wurden. Angemessene Schutzvorkehrungen sollten dann als vorhanden gelten, wenn in dem betreffenden Drittland gleichwertige Maßnahmen getroffen wurden, mit denen gewährleistet wird, dass für nicht personenbezogene Daten ein ähnliches Schutzniveau gilt wie das, das auf der Grundlage des Unionsrechts und nationalen Rechts vor allem in Hinblick auf den Schutz von Geschäftsgeheimnissen und der Rechte des geistigen Eigentums Anwendung findet. Hierzu kann die Kommission Durchführungsrechtsakte erlassen, in denen sie erklärt, dass ein Drittland ein Schutzniveau bietet, das im Wesentlichen dem durch Unionsrecht und nationales Recht gewährten Schutzniveau gleichwertig ist. Bei der Bewertung des in dem betreffenden Drittland gewährten Schutzniveaus sollten insbesondere die einschlägigen allgemeinen und sektoralen Rechtsvorschriften berücksichtigt werden, auch solche, die sich auf die öffentliche Sicherheit, die Verteidigung und die nationale Sicherheit beziehen, sowie die

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

strafrechtlichen Vorschriften in Bezug auf den Zugriff auf und den Schutz von nicht personenbezogenen Daten und auf etwaige Zugriffe durch die Behörden des betreffenden Drittlands auf die übertragenen Daten; außerdem sollten das Vorhandensein und die wirksame Funktionsweise unabhängiger Aufsichtsbehörden, die in dem betreffenden Drittland für die Einhaltung und Durchsetzung der Rechtsvorschriften, mit denen der Zugriff auf solche Daten geregelt wird, zuständig sind, sowie die internationalen Verpflichtungen, die das betreffende Drittland hinsichtlich des Datenschutzes eingegangen ist, oder die Verpflichtungen, die sich aus rechtsverbindlichen Übereinkommen oder Instrumenten sowie aus der Teilnahme an multilateralen oder regionalen Systemen ableiten, berücksichtigt werden. Im Zusammenhang mit der Übertragung nicht personenbezogener Daten in Drittländer ist es von besonderer Bedeutung, ob Dateninhabern, öffentlichen Stellen oder Anbietern von Diensten für die gemeinsame Datennutzung in dem betreffenden Drittland wirksame Rechtsbehelfe zur Verfügung stehen. Solche Schutzvorkehrungen sollten daher auch das Bestehen durchsetzbarer Rechte und wirksamer Rechtsbehelfe umfassen.

(16) Falls die Kommission keinen Durchführungsrechtsakt in Bezug auf ein Drittland erlassen hat, in dem sie erklärt, dass das betreffende Drittland vor allem im Hinblick auf den Schutz sensibler Geschäftsdaten und der Rechte am geistigen Eigentum, ein Schutzniveau bietet, das im Wesentlichen dem durch Unionsrecht oder nationales Recht gewährten Schutzniveau gleichwertig ist, sollte die öffentliche Stelle nur dann geschützte Daten einem Weiterverwender übermitteln, wenn dieser Verpflichtungen zum Schutz der Daten eingeht. Der Weiterverwender, der beabsichtigt, die Daten in ein solches Drittland zu übertragen, sollte sich dazu verpflichten, die in dieser Verordnung festgelegten Bedingungen selbst nach der Übertragung der Daten in das Drittland einzuhalten. Für eine ordnungsgemäße Durchsetzung der Einhaltung dieser Verpflichtungen sollte der Weiterverwender zur Beilegung von Rechtsstreitigkeiten zudem die Gerichtsbarkeit des Mitgliedstaats der öffentlichen Stelle, die die Weiterverwendung der Daten erlaubt hat, als zuständig anerkennen.

(17) Einige Drittländer erlassen Gesetze, Verordnungen und sonstige Rechtsakte, die auf die unmittelbare Übertragung nicht personenbezogener Daten oder den unmittelbaren Zugriff auf diese Daten, die in der Union der Kontrolle natürlicher oder juristischer Personen in der Gerichtsbarkeit von Mitgliedstaaten unterliegen, abzielen. In Drittländern ergangene Gerichtsurteile oder Verwaltungsentscheidungen, mit denen eine solche Übertragung nicht personenbezogener Daten gefordert wird, sollten vollstreckbar sein, wenn sie sich auf eine internationale Vereinbarung, etwa ein Rechtshilfeabkommen, stützen, dass zwischen dem betreffenden Drittland und der Union oder einem Mitgliedstaat besteht. Mitunter kann es dazu kommen, dass die sich aus einem Gesetz eines Drittlands ergebende Verpflichtung zur Übertragung nicht personenbezogener Daten oder zur Gewährung des Zugangs zu diesen Daten mit der Verpflichtung zum Schutz dieser Daten nach Unionsrecht oder nationalem Recht kollidiert, insbesondere im Hinblick auf den Schutz sensibler Geschäftsdaten und Rechte des geistigen Eigentums, darunter auch vertragliche Vertraulichkeitspflichten nach einem solchen Gesetz. Besteht keine internationale Vereinbarung zur Regelung dieser Fragen sollte die Übertragung oder der Zugang nur unter bestimmten Bedingungen erlaubt werden, insbesondere unter der Bedingung, dass das Rechtssystem des betreffenden Drittlands die Begründung und Verhältnismäßigkeit sowie die hinreichende Bestimmtheit der gerichtlichen Anordnung oder Entscheidung vorschreibt und dem Adressaten die Möglichkeit einräumt, seinen begründeten Einwand dem zuständigen Gericht des Drittlands, das befugt ist, die einschlägigen

rechtlichen Interessen des Bereitstellers der Daten gebührend zu berücksichtigen, zur Überprüfung vorzulegen.

(18) Zur Vermeidung unrechtmäßiger Zugriffe auf nicht personenbezogene Daten sollten öffentliche Stellen, natürliche oder juristische Personen, denen das Recht auf Weiterverwendung von Daten gewährt wurde, Anbieter von Diensten für die gemeinsame Datennutzung und im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen alle Maßnahmen ergreifen, die nach vernünftigem Ermessen den Zugang zu den Systemen verhindern, in denen nicht personenbezogene Daten gespeichert sind, auch durch Verschlüsselung der Daten oder innerbetriebliche Vorgaben.

(19) Für die Übertragung bestimmter Arten nicht personenbezogener Daten, die als hoch sensibel gelten, in Drittländer ist es zum Aufbau von Vertrauen in die Weiterverwendungsmechanismen und für den Fall, dass eine solche Übertragung Ziele des Gemeinwohls gefährden könnte, möglicherweise notwendig, im Einklang mit internationalen Verpflichtungen an diese Übertragung strengere Bedingungen zu knüpfen. So könnten im Gesundheitsbereich bestimmte Datensätze, die sich im Besitz von öffentlichen Gesundheitseinrichtungen, wie beispielsweise Krankenhäusern, befinden, als hochsensible Gesundheitsdaten gelten. Um hier unionsweit einheitlich vorzugehen, sollte im Unionsrecht, beispielsweise im Zusammenhang mit dem europäischen Gesundheitsdatenraum oder anderen sektorspezifischen Vorschriften, festgelegt werden, welche nicht personenbezogenen öffentlichen Daten als hoch sensibel gelten. Die Bedingungen für die Übertragung solcher Daten in Drittländer sollten in delegierten Rechtsakten festgelegt werden. Die Bedingungen sollten verhältnismäßig, nichtdiskriminierend und für den Schutz der genannten berechtigten Ziele des Gemeinwohls notwendig sein, wie etwa für den Schutz der öffentlichen Gesundheit, der öffentlichen Ordnung, der Sicherheit, der Umwelt, der guten Sitten, der Verbraucher sowie der Privatsphäre und personenbezogener Daten. Die Bedingungen sollten den Risiken entsprechen, die mit Blick auf die Sensibilität dieser Daten bestehen, etwa dem Risiko der erneuten Identifizierung von Einzelpersonen. Diese Bedingungen könnten Auflagen für die Übertragung oder technische Vorkehrungen enthalten, z. B. die Anforderung der Verwendung einer sicheren Verarbeitungsumgebung, Beschränkungen der Weiterverwendung der Daten in Drittländern oder Kategorien von Personen, die berechtigt sind, diese Daten in Drittländer zu übertragen und die in dem betreffenden Drittland Zugang zu den Daten haben. In außergewöhnlichen Fällen könnten sie zum Schutz öffentlicher Interessen auch Beschränkungen in Bezug auf die Übertragung der Daten in Drittländer enthalten.

(20) Öffentliche Stellen sollten Gebühren für die Weiterverwendung von Daten erheben können, aber auch entscheiden können, beispielsweise für bestimmte Kategorien der Weiterverwendung, etwa für nichtkommerzielle Zwecke oder durch kleine und mittlere Unternehmen, die Daten zu niedrigeren Gebühren oder unentgeltlich zur Verfügung zu stellen, um so Anreize für die Weiterverwendung der Daten in Forschung und Innovation zu schaffen und im Einklang mit den Vorschriften über staatliche Beihilfen Unternehmen zu unterstützen, von denen wichtige Innovationen ausgehen und für die es in der Regel schwieriger ist, einschlägige Daten selbst zu sammeln. Solche Gebühren sollten angemessen, transparent und nichtdiskriminierend sein und im Internet veröffentlicht werden.

(21) Als Anreiz für die Weiterverwendung von Daten dieser Kategorie sollten die Mitgliedstaaten eine zentrale Informationsstelle einrichten, die als erste Anlaufstelle

für diejenigen dient, die die Weiterverwendung von im Besitz öffentlicher Stellen befindlichen Daten beabsichtigen. Die Informationsstelle sollte sektorübergreifend angelegt sein und erforderlichenfalls sektorale Regelungen ergänzen. Ferner sollten die Mitgliedstaaten zuständige Stellen benennen, einrichten oder deren Einrichtung erleichtern, die öffentliche Stellen unterstützen, die die Weiterverwendung geschützter Daten bestimmter Kategorien erlauben. Ihre Aufgaben könnten auch die Gewährung des Zugangs zu Daten umfassen, sofern ihnen hierzu auf der Grundlage von sektoralem Unionsrecht oder nationalem Recht der Auftrag erteilt wurde. Diese zuständigen Stellen können öffentliche Stellen mit moderner Technik unterstützen, etwa durch die Bereitstellung sicherer Datenverarbeitungsumgebungen, die es ermöglichen, Daten unter Wahrung des Datenschutzes und der Privatsphäre zu analysieren. Solche Strukturen können die Dateninhaber beim Einwilligungsmanagement unterstützen, wenn beispielsweise für bestimmte Bereiche der wissenschaftlichen Forschung die Einwilligung unter der Voraussetzung gegeben wird, dass anerkannte Standards der Ethik für die wissenschaftliche Forschung eingehalten werden. Die Datenverarbeitung sollte unter der Verantwortung der für das Datenregister zuständigen öffentlichen Stelle erfolgen, bei der es sich auch weiterhin und sofern es personenbezogene Daten betrifft, um den Datenverantwortlichen im Sinne der Verordnung (EU) 2016/679 handelt. Die Mitgliedstaaten können eine oder mehrere zuständige Stellen benennen, die für verschiedene Sektoren zuständig sind.

(22) Anbieter von Diensten für die gemeinsame Datennutzung (Datenmittler) dürften eine Schlüsselrolle in der Datenwirtschaft spielen, da sie das Aggregieren und den Austausch erheblicher Mengen einschlägiger Daten erleichtern. Datenmittler, die Dienste anbieten, die die verschiedenen Akteure miteinander verbinden, können zur effizienten Bündelung von Daten sowie zur Erleichterung des bilateralen Datenaustauschs beitragen. Spezialisierte Datenmittler, die sowohl von Dateninhabern als auch von Datennutzern unabhängig sind, können bei der Entstehung neuer von etwaigen Akteuren mit beträchtlicher Marktmacht unabhängiger datengetriebener Ökosysteme eine unterstützende Rolle spielen. Diese Verordnung sollte ausschließlich für Anbieter von Diensten für die gemeinsame Datennutzung gelten, deren Hauptziel in der Herstellung einer geschäftlichen, rechtlichen und möglicherweise auch technischen Beziehung zwischen den Dateninhabern, einschließlich betroffener Personen, einerseits und möglichen Nutzern andererseits sowie darin besteht, die Parteien bei einer Transaktion von Datenbeständen zwischen beiden zu unterstützen. Sie sollte sich lediglich auf Dienste erstrecken, die auf die Vermittlung zwischen einer unbestimmten Zahl von Dateninhabern und Datennutzern abzielen, nicht aber auf Dienste für die gemeinsame Datennutzung, die für eine geschlossene Gruppe von Dateninhabern und -nutzern gedacht sind. Anbieter von Cloud-Diensten sowie Diensteanbieter, die Daten von Dateninhabern einholen, sie aggregieren, anreichern oder umwandeln und Lizenzen für die Nutzung der sich daraus ergebenden Daten an die Datennutzer vergeben, ohne eine direkte Beziehung zwischen Dateninhabern und Datennutzern herzustellen, z. B. Werbe- oder Datenmakler, Datenberatungsunternehmen und Anbieter von Datenprodukten, deren Mehrwert der Diensteanbieter aus den Daten erzeugt hat, sollten ausgenommen sein. Gleichzeitig sollte es Anbietern von Diensten für die gemeinsame Datennutzung gestattet sein, die ausgetauschten Daten auf Wunsch des Datennutzers so anzupassen, dass dies die Nutzbarkeit der Daten durch den Datennutzer verbessert (z. B. durch Umwandlung in bestimmte Formate). Darüber hinaus sollten Dienste, die sich auf die Vermittlung von Inhalten, insbesondere von urheberrechtlich geschützten Inhalten, konzentrieren, nicht unter diese Verordnung fallen. Plattformen für den Datenaustausch, die ausschließlich

von einem einzigen Dateninhaber genutzt werden, um die Nutzung der in seinem Besitz befindlichen Daten zu ermöglichen, sowie Plattformen, die im Zusammenhang mit Objekten und Geräten, die mit dem Internet der Dinge verbunden sind, entwickelt wurden und deren Hauptziel darin besteht, die Funktionen des verbundenen Objekts oder Geräts sicherzustellen und Mehrwertdienste zu ermöglichen, sollten nicht unter diese Verordnung fallen. „Bereitsteller konsolidierter Datenträger“ im Sinne von Artikel 4 Absatz 1 Nummer 53 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates[42] sowie „Kontoinformationsdienstleister“ im Sinne von Artikel 4 Nummer 19 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates[43] sollten für die Zwecke dieser Verordnung nicht als Anbieter von Diensten für die gemeinsame Datennutzung gelten. Einrichtungen, die lediglich die Nutzung von Daten erleichtern, die auf der Grundlage von Datenaltruismus bereitgestellt werden, und ohne Erwerbszweck tätig sind, sollten nicht unter Kapitel III dieser Verordnung fallen, da deren Tätigkeit Zielen von allgemeinem Interesse dient, indem sie die für diese Zwecke verfügbaren Datenmengen steigert.

(23) Zu einer besonderen Kategorie von Datenmittlern gehören Anbieter von Diensten für die gemeinsame Datennutzung, die ihre Dienste betroffenen Personen im Sinne der Verordnung (EU) 2016/679 anbieten. Solche Anbieter konzentrieren sich ausschließlich auf personenbezogene Daten und wollen die Handlungsfähigkeit und die Kontrolle des Einzelnen in Bezug auf die ihn betreffenden Daten verbessern. Sie unterstützen Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679, insbesondere in Bezug auf die Handhabung ihrer Einwilligung in die Datenverarbeitung, das Recht auf Auskunft über ihre eigenen Daten, das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht auf Löschung oder das Recht auf Vergessenwerden, das Recht auf Einschränkung der Verarbeitung und das Recht auf Datenübertragbarkeit, das es betroffenen Personen ermöglicht, ihre personenbezogenen Daten von einem für die Verarbeitung Verantwortlichen auf einen anderen zu übertragen. In diesem Zusammenhang ist es wichtig, dass ihr Geschäftsmodell sicherstellt, dass keine falschen Anreize bestehen, die den Einzelnen dazu bewegen, mehr Daten für die Verarbeitung zur Verfügung zu stellen, als im Interesse des Einzelnen liegt. Dies könnte die Beratung von Einzelpersonen über die Verwendung ihrer Daten, in die sie einwilligen könnten, und die Durchführung von Sorgfaltsprüfungen bei den Datennutzern umfassen, bevor diese Kontakt zu betroffenen Personen aufnehmen dürfen, um betrügerische Praktiken zu vermeiden. In bestimmten Situationen könnte es wünschenswert sein, die eigentlichen Daten in einem Raum zur Speicherung personenbezogener Daten oder „persönlichen Datenraum“ zusammenzustellen, damit eine Verarbeitung innerhalb dieses Raums erfolgen kann, ohne dass personenbezogene Daten an Dritte übermittelt werden, um die personenbezogenen Daten und die Privatsphäre bestmöglich zu schützen.

(24) Datengenossenschaften sind bestrebt, die Position von Einzelpersonen bei der sachkundigen Entscheidung vor der Einwilligung zur Datennutzung zu stärken, die Geschäftsbedingungen von Datennutzerorganisationen im Zusammenhang mit der Datennutzung zu beeinflussen oder mögliche Streitigkeiten zwischen Mitgliedern

[42] Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

[43] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

einer Gruppe darüber beizulegen, wie Daten verwendet werden können, wenn sich diese Daten auf mehrere betroffene Personen innerhalb dieser Gruppe beziehen. In diesem Zusammenhang ist es wichtig anzuerkennen, dass die Rechte gemäß der Verordnung (EU) 2016/679 nur von der jeweiligen Einzelperson selbst ausgeübt und nicht an eine Datengenossenschaft übertragen oder delegiert werden können. Datengenossenschaften könnten auch ein nützliches Instrument für Ein-Personen-Betriebe, Kleinstunternehmen sowie kleine und mittlere Unternehmen darstellen, die in Bezug auf das Wissen über die Weitergabe von Daten häufig mit Einzelpersonen vergleichbar sind.

(25) Um das Vertrauen in solche Dienste für die gemeinsame Datennutzung zu stärken, insbesondere in Bezug auf die Nutzung von Daten und die Einhaltung der von den Dateninhabern auferlegten Bedingungen, ist es erforderlich, einen Rechtsrahmen auf Unionsebene zu schaffen, in dem stark harmonisierte Anforderungen an die vertrauenswürdige Erbringung solcher Dienste für die Datennutzung festgelegt werden. Dies wird dazu beitragen, dass Dateninhaber und Datennutzer eine bessere Kontrolle über den Zugang zu ihren Daten und deren Nutzung im Einklang mit dem Unionsrecht haben. Sowohl bei der Datenweitergabe zwischen Unternehmen als auch zwischen Unternehmen und Verbrauchern sollten die Anbieter von Diensten für die gemeinsame Datennutzung eine neuartige europäische Art der Daten-Governance ermöglichen, indem sie eine Trennung zwischen der Bereitstellung, der Vermittlung und der Nutzung von Daten in der Datenwirtschaft vorsehen. Anbieter von Diensten für die gemeinsame Datennutzung können auch eine spezifische technische Infrastruktur für die Vernetzung von Dateninhabern und Datennutzern bereitstellen.

(26) Ein Schlüsselelement zur Schaffung von Vertrauen in die Dienste für die gemeinsame Datennutzung und zur Stärkung der Kontrolle über diese Dienste durch die Dateninhaber und Datennutzer ist die Neutralität der Anbieter dieser Dienste in Bezug auf die zwischen Dateninhabern und Datennutzern weitergegebenen Daten. Es ist daher notwendig, dass Anbieter von Diensten für die gemeinsame Datennutzung bei den Transaktionen lediglich als Mittler tätig werden und die weitergegebenen Daten nicht für andere Zwecke verwenden. Dies erfordert auch eine strukturelle Trennung zwischen dem Dienst für die gemeinsame Datennutzung und allen anderen erbrachten Diensten, um Interessenkonflikte zu vermeiden. Dies bedeutet, dass der Dienst für die gemeinsame Datennutzung von einer juristischen Person erbracht werden sollte, die von den anderen Tätigkeiten dieses Dienstes getrennt ist. Anbieter von Diensten für die gemeinsame Datennutzung, die die Datenweitergabe zwischen Einzelpersonen als Dateninhaber und juristischen Personen vermitteln, sollten darüber hinaus treuhänderische Pflichten gegenüber den natürlichen Personen haben, damit sichergestellt ist, dass sie im besten Interesse der Dateninhaber handeln.

(27) Um zu gewährleisten, dass die Anbieter von Diensten für die gemeinsame Datennutzung die in dieser Verordnung festgelegten Bedingungen erfüllen, sollten diese Anbieter in der Union niedergelassen sein. Bietet ein Anbieter von Diensten für die gemeinsame Datennutzung, der keine Niederlassung in der Union hat, Dienste in der Union an, so sollte er stattdessen einen Vertreter benennen. Die Benennung eines Vertreters ist notwendig, da solche Anbieter von Diensten für die gemeinsame Datennutzung personenbezogene Daten sowie vertrauliche Geschäftsdaten verarbeiten, weshalb es notwendig ist, dass die Einhaltung der in dieser Verordnung festgelegten Bedingungen durch diese Diensteanbieter überwacht wird. Um festzustellen, ob ein solcher Anbieter von Diensten für die gemeinsame Datennutzung in der Union Dienste anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Personen in einem

oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website oder einer E-Mail-Adresse und anderer Kontaktdaten des Anbieters von Diensten für die gemeinsame Datennutzung in der Union oder die Verwendung einer Sprache, die in dem Drittland, in dem der Anbieter von Diensten für die gemeinsame Datennutzung niedergelassen ist, allgemein gebräuchlich ist, sollte hierfür kein ausreichender Anhaltspunkt sein. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser anderen Sprache zu bestellen, oder die Erwähnung von Nutzern in der Union darauf hindeuten, dass der Anbieter von Diensten für die gemeinsame Datennutzung beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag des Anbieters von Diensten für die gemeinsame Datennutzung handeln, und es sollte für die zuständigen Behörden möglich sein, mit ihm Kontakt aufzunehmen. Der Anbieter von Diensten für die gemeinsame Datennutzung sollte den Vertreter benennen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen in seinem Auftrag zu handeln.

(28) Diese Verordnung sollte die Verpflichtung der Anbieter von Diensten für die gemeinsame Datennutzung zur Einhaltung der Verordnung (EU) 2016/679 und die Verantwortung der Aufsichtsbehörden, die Einhaltung dieser Verordnung sicherzustellen, unberührt lassen. Handelt es sich bei den Anbietern von Diensten für die gemeinsame Datennutzung um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter im Sinne der Verordnung (EU) 2016/679, so sind sie an die Bestimmungen der genannten Verordnung gebunden. Die Anwendung des Wettbewerbsrechts sollte von dieser Verordnung unberührt bleiben.

(29) Die Anbieter von Diensten für die gemeinsame Datennutzung sollten auch Maßnahmen ergreifen, um die Einhaltung des Wettbewerbsrechts sicherzustellen. Die gemeinsame Datennutzung kann verschiedene Arten von Effizienzgewinnen bewirken, aber auch zu Wettbewerbsbeschränkungen führen, insbesondere wenn sie den Austausch sensibler wettbewerbsrelevanter Informationen umfasst. Dies gilt insbesondere dann, wenn es die gemeinsame Datennutzung den Unternehmen ermöglicht, Kenntnis der Marktstrategien ihrer tatsächlichen oder potenziellen Wettbewerber zu erlangen. Zu den sensiblen wettbewerbsrelevanten Informationen gehören in der Regel Informationen über künftige Preise, Produktionskosten, Mengen, Umsätze, Verkäufe oder Kapazitäten.

(30) Es sollte ein Anmeldeverfahren für Dienste für die gemeinsame Datennutzung eingeführt werden, um eine Daten-Governance auf der Grundlage einer vertrauenswürdigen Datenweitergabe in der Union zu gewährleisten. Die Vorteile eines vertrauenswürdigen Umfelds ließen sich am besten dadurch erreichen, dass eine Reihe von Anforderungen an die Erbringung von Diensten für die gemeinsame Datennutzung geknüpft würde, ohne dass jedoch eine ausdrückliche Entscheidung oder ein Verwaltungsakt der zuständigen Behörde für die Erbringung solcher Dienste erforderlich wäre.

(31) Um eine wirksame grenzüberschreitende Erbringung von Dienstleistungen zu unterstützen, sollte der Anbieter von Diensten für die gemeinsame Datennutzung aufgefordert werden, eine Anmeldung nur an die benannte zuständige Behörde des Mitgliedstaats zu richten, in dem sich seine Hauptniederlassung oder sein gesetzlicher Vertreter befindet. Eine solche Anmeldung sollte nicht mehr als eine einfache Erklärung der Absicht beinhalten, solche Dienste zu erbringen, und nur durch die in dieser Verordnung genannten Informationen ergänzt werden.

(32) Die Hauptniederlassung des Anbieters von Diensten für die gemeinsame Datennutzung in der Union sollte in dem Mitgliedstaat sein, in dem sich seine Hauptverwaltung in der Union befindet. Zur Bestimmung der Hauptniederlassung eines Anbieters von Diensten für die gemeinsame Datennutzung in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Verwaltungstätigkeiten sein.

(33) Die zuständigen Behörden, die für die Überwachung der Einhaltung der Anforderungen dieser Verordnung durch die Dienste für die gemeinsame Datennutzung benannt wurden, sollten auf der Grundlage ihrer Kapazitäten und ihres Fachwissens in Bezug auf den horizontalen oder sektoralen Datenaustausch ausgewählt werden und bei der Wahrnehmung ihrer Aufgaben unabhängig sowie transparent und unparteiisch sein. Die Mitgliedstaaten sollten der Kommission die Namen der benannten zuständigen Behörden melden.

(34) Der in dieser Verordnung festgelegte Anmelderahmen sollte spezifische zusätzliche Vorschriften für die Erbringung von Diensten für die gemeinsame Datennutzung, die aufgrund sektorspezifischer Rechtsvorschriften gelten, unberührt lassen.

(35) Die Nutzung von Daten, die von betroffenen Personen auf der Grundlage ihrer Einwilligung freiwillig oder – wenn es sich um nicht personenbezogene Daten handelt – von juristischen Personen für Zwecke von allgemeinem Interesse bereitgestellt werden, birgt ein großes Potenzial. Zu diesen Zwecken gehören die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Erstellung amtlicher Statistiken oder die bessere Erbringung öffentlicher Dienstleistungen. Die Unterstützung der wissenschaftlichen Forschung, einschließlich z. B. der technologischen Entwicklung und Demonstration, der Grundlagenforschung, der angewandten Forschung und der privat finanzierten Forschung, sollte ebenfalls als Zweck von allgemeinem Interesse betrachtet werden. Ziel dieser Verordnung ist es, zur Entstehung von Datenbeständen beizutragen, die auf der Grundlage von Datenaltruismus bereitgestellt werden und so groß sind, dass sie Datenanalysen und maschinelles Lernen auch grenzüberschreitend in der Union ermöglichen.

(36) Juristische Personen, die bestrebt sind, Zwecke von allgemeinem Interesse zu unterstützen, indem sie einschlägige Daten auf der Grundlage von Datenaltruismus in größerem Maßstab zur Verfügung stellen und bestimmte Anforderungen erfüllen, sollten sich als „in der Union anerkannte datenaltruistische Organisationen“ eintragen lassen können. Dies könnte zur Einrichtung von Datenarchiven führen. Die Eintragung in einem Mitgliedstaat wäre unionsweit gültig, was die grenzüberschreitende Datennutzung innerhalb der Union und die Entstehung von Datenbeständen, die mehrere Mitgliedstaaten abdecken, erleichtern dürfte. Die betroffenen Personen würden in bestimmte Zwecke der Datenverarbeitung einwilligen, könnten aber auch der Datenverarbeitung in bestimmten Forschungsbereichen oder Teilen von Forschungsprojekten zustimmen, da es zum Zeitpunkt der Datensammlung häufig nicht möglich ist, den Zweck der Verarbeitung personenbezogener Daten für wissenschaftliche Forschungszwecke vollständig zu bestimmen. Juristische Personen könnten die Verarbeitung ihrer nicht personenbezogenen Daten für eine Reihe von Zwecken erlauben, die zum Zeitpunkt der Erteilung der Erlaubnis noch nicht festgelegt waren. Die freiwillige Erfüllung der Anforderungen durch diese eingetragenen Einrichtungen sollte für Vertrauen sorgen, dass die für altruistische Zwecke bereitgestellten Daten dem allgemeinem Interesse dienen. Dieses Vertrauen sollte sich insbesondere aus einem Niederlassungsort in der Union sowie aus der

Anforderung, dass eingetragene Einrichtungen keinen Erwerbszweck verfolgen dürfen, aus Transparenzanforderungen und aus spezifischen Garantien zum Schutz der Rechte und Interessen der betroffenen Personen und Unternehmen ergeben. Weitere Garantien sollten umfassen, dass einschlägige Daten in einer von einer eingetragenen Einrichtung betriebenen sicheren Verarbeitungsumgebung verarbeitet werden können, dass mithilfe von Aufsichtsmechanismen wie Ethikräten oder -gremien sichergestellt wird, dass der für die Verarbeitung Verantwortliche hohe wissenschaftliche Ethikstandards einhält, dass wirksame technische Mittel vorhanden sind, um die Einwilligung auf der Grundlage der Informationspflichten der für die Verarbeitung Verantwortlichen gemäß der Verordnung (EU) 2016/679 jederzeit widerrufen oder ändern zu können, sowie Mittel, mit deren Hilfe sich die betroffenen Personen über die Verwendung der von ihnen bereitgestellten Daten laufend informieren können.

(37) Diese Verordnung lässt die Einrichtung, Organisation und Funktionsweise von Einrichtungen, die sich nach nationalem Recht dem Datenaltruismus verschreiben, unberührt. Dies stützt sich auf die Anforderung, dass die Tätigkeiten einer Organisation ohne Erwerbszweck in einem Mitgliedstaaten nach nationalem Recht rechtmäßig sein müssen. Einrichtungen, die die Anforderungen dieser Verordnung erfüllen, sollten die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ führen dürfen.

(38) In der Union anerkannte datenaltruistische Organisationen sollten einschlägige Daten direkt bei natürlichen und juristischen Personen sammeln oder von Dritten gesammelte Daten verarbeiten können. In der Regel stützt sich Datenaltruismus auf die Einwilligung der betroffenen Personen im Sinne von Artikel 6 Absatz 1 Buchstabe a und Artikel 9 Absatz 2 Buchstabe a sowie auf die Einhaltung der Anforderungen an eine rechtmäßige Einwilligung gemäß Artikel 7 der Verordnung (EU) 2016/679. Gemäß der Verordnung (EU) 2016/679 können wissenschaftliche Forschungszwecke, bestimmte Forschungsbereiche oder Teile von Forschungsprojekten durch die Einwilligung in die Weiterverarbeitung der Daten für diese Zwecke unterstützt werden, sofern anerkannte Standards der Ethik für die wissenschaftliche Forschung eingehalten werden. Gemäß Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 sollte eine Weiterverarbeitung der Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 der Verordnung (EU) 2016/679 nicht als unvereinbar mit den ursprünglichen Zwecken gelten.

(39) Um mehr Rechtssicherheit in Bezug auf die Einwilligung und deren Widerruf zu schaffen, insbesondere im Zusammenhang mit Daten, die auf altruistischer Grundlage für die wissenschaftliche Forschung und für Statistikzwecke zur Verfügung gestellt werden, sollte ein europäisches Einwilligungsformular für Datenaltruismus entwickelt und bei der altruistischen Datenweitergabe verwendet werden. Ein solches Formular sollte für die betroffenen Personen zu mehr Transparenz darüber beitragen, dass ihre Daten in Übereinstimmung mit ihrer Einwilligung und unter uneingeschränkter Einhaltung der Datenschutzvorschriften abgerufen und verwendet werden. Es könnte auch verwendet werden, um den Datenaltruismus von Unternehmen zu vereinheitlichen und einen Mechanismus bereitzustellen, der es diesen Unternehmen ermöglicht, ihre Erlaubnis zur Nutzung der Daten zurückzuziehen. Um den Besonderheiten einzelner Sektoren – auch aus datenschutzrechtlicher Sicht – Rechnung zu tragen, sollte das europäische Einwilligungsformular für Datenaltruismus an den jeweiligen Sektor angepasst werden können.

(40) Zur erfolgreichen Umsetzung des Rahmens für die Daten-Governance sollte ein Europäischer Dateninnovationsrat in Form einer Expertengruppe eingerichtet werden. Der Innovationsrat sollte sich aus Vertretern der Mitgliedstaaten, der Kommission und einschlägiger Datenräume sowie spezifischer Sektoren (wie Gesundheit, Landwirtschaft, Verkehr und Statistik) zusammensetzen. Der Europäische Datenschutzausschuss sollte aufgefordert werden, einen Vertreter in den Europäischen Dateninnovationsrat zu entsenden.

(41) Unbeschadet der Normungsarbeit in bestimmten Sektoren oder Bereichen sollte der Innovationsrat die Kommission bei der Koordinierung nationaler Verfahren und Strategien zu den unter diese Verordnung fallenden Themen sowie bei der sektorübergreifenden Datennutzung unterstützen, indem er die Grundsätze des Europäischen Interoperabilitätsrahmens (EIF) befolgt und Normen und Spezifikationen (wie die Kernvokabulare[44] und die CEF-Bausteine[45]) nutzt. Die Arbeiten an der technischen Normung können die Festlegung von Prioritäten für die Entwicklung von Normen und die Festlegung und Aufrechterhaltung einer Reihe technischer und rechtlicher Normen für die Datenübermittlung zwischen zwei Verarbeitungsumgebungen umfassen, die die Organisation von Datenräumen ohne Rückgriff auf zwischengeschaltete Stellen ermöglichen. Der Innovationsrat sollte mit sektoralen Gremien, Netzen oder Expertengruppen oder anderen sektorübergreifenden Organisationen, die sich mit der Weiterverwendung von Daten befassen, zusammenarbeiten. Im Hinblick auf den Datenaltruismus sollte der Innovationsrat die Kommission in Absprache mit dem Europäischen Datenschutzausschuss bei der Entwicklung des Einwilligungsformulars für Datenaltruismus unterstützen.

(42) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse zur Entwicklung des Einwilligungsformulars für Datenaltruismus übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[46] ausgeübt werden.

(43) Um der Besonderheit bestimmter Kategorien von Daten Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um besondere Bedingungen für Übertragungen bestimmter nicht personenbezogener Daten, die als hochsensibel gelten, in Drittländer in besonderen, nach einem Gesetzgebungsverfahren erlassenen Rechtsakten der Union festzulegen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit, auch auf der Ebene von Sachverständigen, angemessene Konsultationen durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

---

44 https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

45 https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef

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

(44) Diese Verordnung sollte die Anwendung der Wettbewerbsvorschriften, insbesondere der Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union, unberührt lassen. Die in dieser Verordnung vorgesehenen Maßnahmen dürfen nicht dazu verwendet werden, den Wettbewerb entgegen den Vorschriften des Vertrags über die Arbeitsweise der Europäischen Union einzuschränken. Dies betrifft insbesondere die Vorschriften für den Austausch sensibler wettbewerbsrelevanter Informationen zwischen tatsächlichen oder potenziellen Wettbewerbern durch Dienste für die gemeinsame Datennutzung.

(45) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[47] angehört und haben am [...] eine Stellungnahme abgegeben.

(46) Diese Verordnung achtet die Grundrechte und wahrt die Grundsätze, die insbesondere in der Charta anerkannt sind, darunter die Achtung der Privatsphäre, der Schutz personenbezogener Daten, die unternehmerische Freiheit, das Eigentumsrecht und die Integration von Menschen mit Behinderungen —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand und Anwendungsbereich

(1) In dieser Verordnung wird Folgendes festgelegt:

a) Bedingungen für die Weiterverwendung von Daten bestimmter Datenkategorien, die im Besitz öffentlicher Stellen sind, innerhalb der Union;

b) ein Anmelde- und Aufsichtsrahmen für die Erbringung von Diensten für die gemeinsame Datennutzung;

c) ein Rahmen für die freiwillige Eintragung von Einrichtungen, die für altruistische Zwecke zur Verfügung gestellte Daten sammeln und verarbeiten.

(2) Die besonderen Bestimmungen anderer Rechtsakte der Union über den Zugang zu bestimmten Kategorien von Daten oder deren Weiterverwendung sowie die Anforderungen in Bezug auf die Verarbeitung personenbezogener oder nicht personenbezogener Daten bleiben von dieser Verordnung unberührt. Müssen öffentliche Stellen, Anbieter von Diensten für die gemeinsame Datennutzung oder eingetragene Einrichtungen, die Datenaltruismus-Dienste erbringen, aufgrund sektorspezifischer Unionsvorschriften bestimmte zusätzliche technische, administrative oder organisatorische Bestimmungen einhalten, etwa im Rahmen von Genehmigungs- oder Zertifizierungsverfahren, so finden auch diese Bestimmungen der sektorspezifischen Unionsvorschriften Anwendung.

[47] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

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. „Weiterverwendung“ die Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch natürliche oder juristische Personen für kommerzielle oder nichtkommerzielle Zwecke, die sich von dem ursprünglichen Zweck im Rahmen des öffentlichen Auftrags, für den die Daten erstellt wurden, unterscheiden, abgesehen vom Austausch von Daten zwischen öffentlichen Stellen ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags;

3. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 sind;

4. „Metadaten“ Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zwecks Erbringung eines Dienstes für die gemeinsame Datennutzung erfasst werden; dazu gehören Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Dienst nutzenden Person hergestellt werden;

5. „Dateninhaber“ eine juristische Person oder eine betroffene Person, die nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten, unter ihrer Kontrolle befindlichen personenbezogenen oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben;

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

7. „gemeinsame Datennutzung“ die Weitergabe von Daten durch einen Dateninhaber an einen Datennutzer für eine gemeinschaftliche oder individuelle Nutzung der geteilten Daten auf der Grundlage freiwilliger Vereinbarungen, sowohl direkt als auch über einen Mittler;

8. „Zugang“ die Verarbeitung der von einem Dateninhaber weitergegebenen Daten durch einen Datennutzer im Einklang mit bestimmten technischen, rechtlichen oder organisatorischen Anforderungen, ohne dass diese Daten hierzu zwingend übertragen oder heruntergeladen werden müssen;

9. „Hauptniederlassung“ einer Rechtsperson den Ort, an dem sich ihre Hauptverwaltung in der Union befindet;

10. „Datenaltruismus“ die Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder die Erlaubnis anderer Dateninhaber zur unentgeltlichen Nutzung ihrer nicht personenbezogenen Daten für Zwecke von allgemeinem Interesse wie die wissenschaftliche Forschung oder die Verbesserung öffentlicher Dienstleistungen;

11. „öffentliche Stelle“ den Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen;

12. „Einrichtungen des öffentlichen Rechts“ Einrichtungen, die die folgenden Eigenschaften aufweisen:

    a) sie wurden zu dem besonderen Zweck gegründet, im allgemeinen Interesse liegende Aufgaben zu erfüllen, und haben keinen gewerblichen oder kommerziellen Charakter,

    b) sie besitzen Rechtspersönlichkeit,

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

13. „öffentliches Unternehmen“ ein Unternehmen, auf das öffentliche Stellen aufgrund ihres Eigentums, ihrer finanziellen Beteiligung oder der für das Unternehmen geltenden Bestimmungen unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben können; von einem beherrschenden Einfluss der öffentlichen Stellen ist im Sinne dieser Begriffsbestimmung in jedem der folgenden Fälle auszugehen, in denen diese Stellen unmittelbar oder mittelbar

    a) die Mehrheit des gezeichneten Kapitals des Unternehmens halten,

    b) über die Mehrheit der mit den Anteilen am Unternehmen verbundenen Stimmrechte verfügen,

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

14. „sichere Verarbeitungsumgebung“ die physische oder virtuelle Umgebung und die organisatorischen Mittel, die es ermöglichen, Daten in einer Weise weiterzuverwenden, die es dem Betreiber der sicheren Verarbeitungsumgebung erlaubt, alle Datenverarbeitungsvorgänge zu bestimmen und zu beaufsichtigen, darunter auch das Anzeigen, Speichern, Herunterladen und Exportieren der Daten und das Berechnen abgeleiteter Daten mithilfe von Rechenalgorithmen;

15. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters von Diensten für die gemeinsame Datennutzung oder einer Einrichtung, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus für Ziele von allgemeinem Interesse zur Verfügung gestellte Daten sammelt, zu handeln, und an die sich eine zuständige nationale Behörde – statt an den betreffenden Anbieter von Diensten für die gemeinsame Datennutzung bzw. die betreffende Einrichtung – hinsichtlich der Verpflichtungen des Anbieters von Diensten für die gemeinsame Datennutzung oder der Einrichtung aus dieser Verordnung wenden kann.

KAPITEL II
WEITERVERWENDUNG BESTIMMTER KATEGORIEN GESCHÜTZTER DATEN IM BESITZ ÖFFENTLICHER STELLEN

Artikel 3
Datenkategorien

(1) Dieses Kapitel gilt für Daten, die sich im Besitz öffentlicher Stellen befinden und aus folgenden Gründen geschützt sind:

a) geschäftliche Geheimhaltung,

b) statistische Geheimhaltung,

c) Schutz geistigen Eigentums Dritter,

d) Schutz personenbezogener Daten.

(2) Dieses Kapitel gilt nicht für

a) Daten, die im Besitz öffentlicher Unternehmen sind,

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

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

d) Daten, die aus Gründen der nationalen Sicherheit, der Verteidigung oder der öffentlichen Sicherheit geschützt sind;

e) Daten, deren Bereitstellung nicht unter den im betreffenden Mitgliedstaat gesetzlich oder anderweitig verbindlich festgelegten öffentlichen Auftrag der betreffenden öffentlichen Stellen fällt oder, in Ermangelung solcher Rechtsvorschriften, nicht unter den durch allgemeine Verwaltungspraxis in dem Mitgliedstaat festgelegten öffentlichen Auftrag fällt, vorausgesetzt, dass der Umfang der öffentlichen Aufträge transparent ist und regelmäßig überprüft wird.

(3) Die Bestimmungen dieses Kapitels begründen weder eine Verpflichtung für öffentliche Stellen, die Weiterverwendung von Daten zu erlauben, noch befreien sie öffentliche Stellen von ihren Geheimhaltungspflichten. Das Unionsrecht und nationale Rechtsvorschriften oder internationale Übereinkünfte, denen die Union oder die Mitgliedstaaten beigetreten sind, bleiben in Bezug auf den Schutz von Daten der in Absatz 1 genannten Datenkategorien von diesem Kapitel unberührt. Das Unionsrecht und nationale Rechtvorschriften in Bezug auf den Zugang zu Dokumenten sowie die nach Unionsrecht und nationalem Recht geltenden Verpflichtungen öffentlicher Stellen, die Weiterverwendung von Daten zu erlauben, bleiben von diesem Kapitel unberührt.

Artikel 4
Verbot von Ausschließlichkeitsvereinbarungen

(1) Vereinbarungen oder sonstige Praktiken in Bezug auf die Weiterverwendung von Daten, die im Besitz öffentlicher Stellen sind und Daten der in Artikel 3 Absatz 1 genannten Datenkategorien enthalten, sind verboten, soweit sie ausschließliche

Rechte gewähren oder aber zum Gegenstand haben oder bewirken, dass solche ausschließlichen Rechte gewährt werden oder die Verfügbarkeit von Daten zur Weiterverwendung durch andere Einrichtungen als die Parteien solcher Vereinbarungen oder sonstigen Praktiken eingeschränkt wird.

(2) Abweichend von Absatz 1 kann ein ausschließliches Recht auf Weiterverwendung der in dem Absatz genannten Daten gewährt werden, soweit dies für die Erbringung eines Dienstes oder die Bereitstellung eines Produkts im allgemeinen Interesse erforderlich ist.

(3) Ein solches ausschließliches Recht muss im Rahmen eines einschlägigen Dienstleistungs- oder Konzessionsvertrags und im Einklang mit dem geltenden Unionsrecht und den nationalen Rechtsvorschriften für die Vergabe öffentlicher Aufträge und Konzessionen oder – im Falle eines Auftrags mit einem Wert, für den weder Unionsvorschriften noch nationale Vorschriften für die Vergabe öffentlicher Aufträge und Konzessionen gelten – im Einklang mit den Grundsätzen der Transparenz, der Gleichbehandlung und der Nichtdiskriminierung aus Gründen der Staatsangehörigkeit gewährt werden.

(4) In allen nicht von Absatz 3 erfassten Fällen, in denen der Zweck von allgemeinem Interesse ohne Gewährung eines ausschließlichen Rechts nicht erreicht werden kann, gelten die Grundsätze der Transparenz, der Gleichbehandlung und der Nichtdiskriminierung aus Gründen der Staatsangehörigkeit.

(5) Der Ausschließlichkeitszeitraum des Rechts auf Weiterverwendung von Daten darf drei Jahre nicht überschreiten. Die Laufzeit des vergebenen Auftrags wird bei Vertragsschluss so festgelegt, dass sie mit dem Ausschließlichkeitszeitraum übereinstimmt.

(6) Die Gewährung eines ausschließlichen Rechts nach den Absätzen 2 bis 5, einschließlich der Begründung, warum die Gewährung eines solchen Rechts erforderlich ist, muss transparent sein und wird – unabhängig von einer möglichen Veröffentlichung der Vergabe öffentlicher Aufträge oder Konzessionen – im Internet öffentlich zugänglich gemacht.

(7) Vereinbarungen oder andere Praktiken, die unter das Verbot des Absatzes 1 fallen und die Bedingungen des Absatzes 2 nicht erfüllen, die aber vor Inkrafttreten dieser Verordnung bereits bestanden haben, werden zum Vertragsende, auf jeden Fall aber spätestens innerhalb von drei Jahren nach dem Inkrafttreten dieser Verordnung beendet.

Artikel 5
Bedingungen für die Weiterverwendung

(1) Öffentliche Stellen, die nach nationalem Recht dafür zuständig sind, den Zugang zur Weiterverwendung von Daten einer oder mehrerer der in Artikel 3 Absatz 1 genannten Datenkategorien zu gewähren oder zu verweigern, machen die Bedingungen für das Erlauben einer solchen Weiterverwendung öffentlich zugänglich. Dabei können sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

(2) Die Bedingungen für die Weiterverwendung müssen in Bezug auf die Datenkategorien, die Zwecke der Weiterverwendung und die Art der Daten, deren Weiterverwendung erlaubt wird, nichtdiskriminierend, verhältnismäßig und objektiv

gerechtfertigt sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen.

(3) Öffentliche Stellen können die Verpflichtung auferlegen, dass nur aufbereitete Daten weiterverwendet werden dürfen, sofern durch diese Aufbereitung personenbezogene Daten anonymisiert oder pseudonymisiert oder vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse gelöscht werden sollen.

(4) Öffentliche Stelle können die Verpflichtungen auferlegen,

a) dass der Zugang zu den Daten und deren Weiterverwendung in einer vom öffentlichen Sektor bereitgestellten und kontrollierten sicheren Verarbeitungsumgebung erfolgen muss,

b) dass der Zugang zu den Daten und deren Weiterverwendung innerhalb der physischen Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, erfolgen muss, wenn ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden.

(5) Die öffentlichen Stellen erlegen Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird. Die öffentliche Stelle muss in der Lage sein, die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung zu überprüfen, und behält sich das Recht vor, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen Dritter gefährden.

(6) Wenn die Weiterverwendung von Daten nicht gemäß den in den Absätzen 3 bis 5 festgelegten Verpflichtungen erlaubt werden kann und es keine andere Rechtsgrundlage für die Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, unterstützt die öffentliche Stelle die Weiterverwender bei der Einholung der Einwilligung der betroffenen Personen und/oder der Erlaubnis der Rechtsträger, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, sofern dies ohne unverhältnismäßig hohe Kosten für den öffentlichen Sektor machbar ist. Dabei können sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

(7) Die Weiterverwendung von Daten ist nur unter Wahrung der Rechte des geistigen Eigentums zulässig. Öffentliche Stellen nehmen das in Artikel 7 Absatz 1 der Richtlinie 96/9/EG vorgesehene Recht der Hersteller von Datenbanken nicht in Anspruch, um dadurch die Weiterverwendung von Daten zu verhindern oder diese Weiterverwendung über die in dieser Verordnung festgelegten Beschränkungen hinaus einzuschränken.

(8) Werden angeforderte Daten nach Unionsrecht oder nationalen Rechtsvorschriften über das Geschäftsgeheimnis als vertraulich angesehen, stellen die öffentlichen Stellen sicher, dass die vertraulichen Informationen infolge der Weiterverwendung nicht offengelegt werden.

(9) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie erklärt, dass die Rechts-, Aufsichts- und Durchsetzungsmechanismen eines Drittlands

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

b) wirksam angewendet und durchgesetzt werden und

c) wirksame gerichtliche Rechtsbehelfe vorsehen.

Diese Durchführungsrechtsakte werden nach dem in Artikel 29 Absatz 2 genannten Beratungsverfahren erlassen.

(10) Öffentliche Stellen übermitteln vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten nur dann an einen Weiterverwender, der beabsichtigt, die Daten in ein nicht gemäß Absatz 9 benanntes Drittland zu übertragen, wenn der Weiterverwender sich verpflichtet,

a) die gemäß den Absätzen 7 bis 8 auferlegten Verpflichtungen auch nach der Übertragung der Daten in das Drittland weiterhin zu erfüllen und

b) die Zuständigkeit der Gerichte des Mitgliedstaats der öffentlichen Stelle für alle Streitigkeiten im Zusammenhang mit der Erfüllung der Verpflichtung nach Buchstabe a anzuerkennen.

(11) Wird in besonderen Rechtsakten der Union, die nach einem Gesetzgebungsverfahren erlassenen wurden, festgelegt, dass bestimmte Kategorien nicht personenbezogener Daten, die im Besitz öffentlicher Stellen sind, für die Zwecke dieses Artikels als hochsensibel gelten, so wird der Kommission die Befugnis übertragen, gemäß Artikel 28 delegierte Rechtsakte zur Ergänzung dieser Verordnung durch Festlegung besonderer Bedingungen für Übertragungen in Drittländer zu erlassen. Die Bedingungen für die Übertragung in Drittländer richten sich nach der Art der Datenkategorien, die im Rechtsakt der Union aufgeführt werden, und den Gründen, aus denen sie als hochsensibel gelten; sie sind nichtdiskriminierend und auf das erforderliche Maß zur Erreichung der im Rechtsakt der Union festgelegten Ziele des Gemeinwohls wie Sicherheit und öffentliche Gesundheit beschränkt; sie berücksichtigen Risiken einer erneuten Identifizierung betroffener Personen anhand anonymisierter Daten und stehen im Einklang mit den internationalen Verpflichtungen der Union. Sie können Vorgaben für die Übertragung oder diesbezügliche technische Vorkehrungen, Beschränkungen bezüglich der Weiterverwendung von Daten in Drittländern oder Kategorien von Personen, die berechtigt sind, solche Daten in Drittländer zu übertragen, oder – in Ausnahmefällen – Beschränkungen für Übertragungen in Drittländer umfassen.

(12) Die natürliche oder juristische Person, der das Recht auf Weiterverwendung nicht personenbezogener Daten gewährt wurde, darf die Daten nur in solche Drittländer übertragen, die die Anforderungen der Absätze 9 bis 11 erfüllen.

(13) Beabsichtigt der Weiterverwender, nicht personenbezogene Daten in ein Drittland zu übertragen, so informiert die öffentliche Stelle den Dateninhaber über die Datenübertragung in dieses Drittland.

Artikel 6
Gebühren

(1) Öffentliche Stellen, die eine Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien erlauben, können Gebühren für die Erlaubnis der Weiterverwendung dieser Daten erheben.

(2) Solche Gebühren müssen nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen den Wettbewerb nicht einschränken.

(3) Öffentliche Stellen müssen gewährleisten, dass alle Gebühren online über weithin verfügbare grenzüberschreitende Zahlungsdienste ohne Diskriminierung aufgrund

des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union bezahlt werden können.

(4) Erheben die öffentlichen Stellen Gebühren, ergreifen sie Maßnahmen, um – im Einklang mit den Vorschriften über staatliche Beihilfen – Anreize für die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu nichtkommerziellen Zwecken und durch kleine und mittlere Unternehmen zu schaffen.

(5) Die Gebühren werden aus den Kosten abgeleitet, die im Zusammenhang mit der Bearbeitung von Anträgen auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien entstehen. Die Gebührenberechnungsmethode wird im Voraus veröffentlicht.

(6) Die öffentliche Stelle veröffentlicht eine Beschreibung der wichtigsten Kostenarten und die Regeln der Kostenzuweisung.

Artikel 7
Zuständige Stellen

(1) Die Mitgliedstaaten benennen eine oder mehrere – möglicherweise auch für bestimmte Sektoren – zuständige Stellen, die öffentliche Stellen, die Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien gewähren, bei der Wahrnehmung dieser Aufgabe unterstützen.

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

a) Leistung technischer Unterstützung durch Bereitstellung einer sicheren Verarbeitungsumgebung für die Gewährung des Zugangs zur Weiterverwendung von Daten;

b) Leistung technischer Unterstützung bei der Anwendung erprobter Techniken, die gewährleisten, dass die Datenverarbeitung in einer Weise erfolgt, bei der die Privatsphäre in Bezug auf die Informationen in den Daten, deren Weiterverwendung erlaubt wird, gewahrt bleibt; dazu gehören auch Techniken zur Pseudonymisierung, Anonymisierung, Generalisierung, Unterdrückung und Randomisierung personenbezogener Daten;

c) gegebenenfalls Unterstützung der öffentlichen Stellen bei der Einholung der Einwilligung oder Erlaubnis zur Weiterverwendung für altruistische und andere Zwecke durch die Weiterverwender entsprechend den besonderen Festlegungen der Dateninhaber, auch im Hinblick auf das Hoheitsgebiet oder die Hoheitsgebiete, in denen die Datenverarbeitung stattfinden soll;

d) Unterstützung öffentlicher Stellen bei der Beurteilung, ob die von einem Weiterverwender nach Artikel 5 Absatz 10 eingegangenen Verpflichtungen angemessen sind.

(3) Die zuständigen Stellen können nach Unionsrecht oder nationalem Recht, in dem eine solche Zugangsgewährung vorgesehen ist, auch damit betraut werden, den Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu gewähren. Bei der Wahrnehmung ihrer Aufgabe, den Zugang zur Weiterverwendung zu gewähren oder zu verweigern, finden die Artikel 4, 5, 6 und Artikel 8 Absatz 3 auf diese zuständigen Stellen Anwendung.

(4) Die zuständigen Stellen müssen über angemessene rechtliche und technische Kapazitäten und Sachkenntnis verfügen, damit sie in der Lage sind, das einschlägige Unionsrecht bzw. nationale Recht in Bezug auf die Regelungen für den Zugang zu Daten der in Artikel 3 Absatz 1 genannten Datenkategorien einzuhalten.

(5) Die Mitgliedstaaten teilen der Kommission bis zum [Beginn der Anwendung dieser Verordnung] die Namen der nach Absatz 1 benannten zuständigen Stellen mit. Sie teilen der Kommission auch alle späteren diesbezüglichen Änderungen mit.

Artikel 8
Zentrale Informationsstelle

(1) Die Mitgliedstaaten gewährleisten, dass alle einschlägigen Informationen in Bezug auf die Anwendung der Artikel 5 und 6 über eine zentrale Informationsstelle erhältlich sind.

(2) Die zentrale Informationsstelle nimmt Anträge auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien entgegen und übermittelt sie an die zuständigen öffentlichen Stellen oder gegebenenfalls an die in Artikel 7 Absatz 1 genannten zuständigen Stellen. Die zentrale Informationsstelle stellt auf elektronischem Wege ein Verzeichnis der verfügbaren Datenressourcen bereit, das einschlägige Informationen mit einer Beschreibung der Art der verfügbaren Daten enthält.

(3) Anträge auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien werden von den zuständigen öffentlichen Stellen oder den in Artikel 7 Absatz 1 genannten zuständigen Stellen innerhalb einer angemessenen Frist, jedenfalls aber innerhalb von zwei Monaten nach Antragstellung genehmigt oder abgelehnt.

(4) Jede natürliche oder juristische Person, die von einer Entscheidung einer öffentlichen Stelle bzw. einer zuständigen Stelle betroffen ist, hat ein Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen diese Entscheidung bei den Gerichten des Mitgliedstaats, in dem die betreffende Stelle ihren Sitz hat.

KAPITEL III
ANFORDERUNGEN AN DIENSTE FÜR DIE GEMEINSAME DATENNUTZUNG

Artikel 9
Anbieter von Diensten für die gemeinsame Datennutzung

(1) Die Erbringung der folgenden Dienste für die gemeinsame Datennutzung unterliegt einem Anmeldeverfahren:

a) Vermittlungsdienste zwischen Dateninhabern, die juristische Personen sind, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu solchen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Verwertung von Daten ermöglichen, sowie die Einrichtung einer speziellen Infrastruktur für die Vernetzung von Dateninhabern und Datennutzern gehören;

b) Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste, in Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte;

c) Dienste von Datengenossenschaften, d. h. Dienstleistungen zur Unterstützung betroffener Personen oder von Ein-Personen-Betrieben, Kleinstunternehmen und kleinen und mittleren Unternehmen, die Mitglieder der Genossenschaft sind oder der Genossenschaft die Befugnis übertragen, vor ihrer Einwilligung die Bedingungen der Datenverarbeitung auszuhandeln, damit sie eine sachkundige Entscheidung treffen können, bevor sie in die Datenverarbeitung einwilligen, und zur Bereitstellung von Mechanismen für den Meinungsaustausch über die Zwecke und Bedingungen der Datenverarbeitung, die den Interessen der betroffenen Personen oder juristischen Personen am besten gerecht werden.

(2) Die Anwendung anderen Unionsrechts und nationalen Rechts auf die Anbieter von Diensten für die gemeinsame Datennutzung ebenso wie die Befugnisse der Aufsichtsbehörden zur Gewährleistung der Einhaltung des geltenden Rechts, insbesondere in Bezug auf den Schutz personenbezogener Daten und das Wettbewerbsrecht, bleiben von diesem Kapitel unberührt.

Artikel 10

Anmeldung der Anbieter von Diensten für die gemeinsame Datennutzung

(1) Jeder Anbieter von Diensten für die gemeinsame Datennutzung, der beabsichtigt, die in Artikel 9 Absatz 1 genannten Dienste zu erbringen, muss sich bei der in Artikel 12 genannten zuständigen Behörde anmelden.

(2) Für die Zwecke dieser Verordnung gilt, dass ein Anbieter von Diensten für die gemeinsame Datennutzung, der in mehreren Mitgliedstaaten niedergelassen ist, der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem er seine Hauptniederlassung hat.

(3) Ein Anbieter von Diensten für die gemeinsame Datennutzung, der nicht in der Union niedergelassen ist, aber die in Artikel 9 Absatz 1 genannten Dienste in der Union anbietet, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in denen diese Dienste angeboten werden. Es gilt, dass der Anbieter der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem der gesetzliche Vertreter niedergelassen ist.

(4) Nach der Anmeldung kann der Anbieter von Diensten für die gemeinsame Datennutzung die Tätigkeit unter den in diesem Kapitel festgelegten Bedingungen aufnehmen.

(5) Die Anmeldung berechtigt den Anbieter zur Erbringung von Diensten für die gemeinsame Datennutzung in allen Mitgliedstaaten.

(6) Die Anmeldung muss folgende Angaben enthalten:

a) den Namen des Anbieters von Diensten für die gemeinsame Datennutzung,

b) den Rechtsstatus, die Rechtsform und die Registernummer des Anbieters, sofern dieser im Handelsregister oder einem anderen vergleichbaren öffentlichen Register eingetragen ist,

c) die Anschrift der Hauptniederlassung des Anbieters in der Union, falls zutreffend, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gemäß Absatz 3 benannten gesetzlichen Vertreters,

d) eine Website mit Informationen über den Anbieter und seine Tätigkeiten, falls zutreffend,

e) die Kontaktpersonen und Kontaktangaben des Anbieters,

f) eine Beschreibung des Dienstes, den der Anbieter zu erbringen beabsichtigt,

g) das voraussichtliche Datum der Aufnahme der Tätigkeit,

h) die Mitgliedstaaten, in denen der Anbieter seine Dienste zu erbringen beabsichtigt.

(7) Auf Antrag des Anbieters gibt die zuständige Behörde innerhalb einer Woche eine standardisierte Erklärung ab, in der sie bestätigt, dass der Anbieter die in Absatz 4 genannte Anmeldung vorgenommen hat.

(8) Die zuständige Behörde leitet jede Anmeldung unverzüglich auf elektronischem Wege an die zuständigen nationalen Behörden der Mitgliedstaaten weiter.

(9) Die zuständige Behörde teilt der Kommission jede neue Anmeldung mit. Die Kommission führt ein Register der Anbieter von Diensten für die gemeinsame Datennutzung.

(10) Die zuständige Behörde kann Gebühren erheben. Diese Gebühren sind verhältnismäßig und objektiv gerechtfertigt und beruhen auf den Verwaltungskosten, die durch die Überwachung der Einhaltung der Vorschriften und andere Marktkontrolltätigkeiten der zuständigen Behörden in Bezug auf Anmeldungen von Diensten für die gemeinsame Datennutzung entstehen.

(11) Stellt ein Anbieter von Diensten für die gemeinsame Datennutzung seine Tätigkeiten ein, so meldet er dies der nach den Absätzen 1, 2 und 3 bestimmten zuständigen Behörde innerhalb von 15 Tagen. Die zuständige Behörde leitet diese Abmeldung unverzüglich auf elektronischem Wege an die zuständigen nationalen Behörden der Mitgliedstaaten und an die Kommission weiter.

Artikel 11

Bedingungen für die Erbringung von Diensten für die gemeinsame Datennutzung

Die Erbringung von Diensten für die gemeinsame Datennutzung nach Artikel 9 Absatz 1 unterliegt folgenden Bedingungen:

1. der Anbieter darf die Daten, für die er Dienste erbringt, für keine anderen Zwecke verwenden, als sie den Datennutzern zur Verfügung zu stellen, und die Dienste für die gemeinsame Datennutzung müssen bei einer gesonderten Rechtsperson angesiedelt sein;

2. die Metadaten, die bei der Erbringung des Dienstes für die gemeinsame Datennutzung erfasst werden, dürfen nur für die Entwicklung dieses Dienstes verwendet werden;

3. der Anbieter stellt sicher, dass das Verfahren für den Zugang zu seinem Dienst sowohl für Dateninhaber als auch für Datennutzer – auch in Bezug auf die Preise – fair, transparent und nichtdiskriminierend ist;

4. der Anbieter ermöglicht den Austausch der Daten in dem Format, in dem er diese vom Dateninhaber erhält; eine Umwandlung der Daten in bestimmte Formate darf nur erfolgen, um die Interoperabilität innerhalb und zwischen Sektoren zu verbessern, wenn der Datennutzer dies verlangt, wenn das Unionsrecht dies vorschreibt oder wenn dies der Harmonisierung mit internationalen oder europäischen Datennormen dient;

5. der Anbieter verfügt über Verfahren, um betrügerische oder missbräuchliche Praktiken in Bezug auf den Zugang zu Daten zu verhindern, wenn andere Parteien über ihre Dienste Zugang zu erlangen suchen;

6. der Anbieter gewährleistet eine angemessene Kontinuität der Erbringung seiner Dienste und bietet für Dienste zur Speicherung von Daten ausreichende Garantien, die sicherstellen, dass Dateninhaber und Datennutzer im Insolvenzfall Zugang zu ihren Daten zu erhalten;

7. der Anbieter ergreift angemessene technische, rechtliche und organisatorische Maßnahmen, um die Übertragung nicht personenbezogener Daten oder den Zugang zu diesen Daten zu verhindern, die nach Maßgabe des Unionsrechts rechtswidrig sind;

8. der Anbieter trifft Maßnahmen, um ein hohes Sicherheitsniveau bei der Speicherung und Übermittlung nicht personenbezogener Daten zu gewährleisten;

9. der Anbieter verfügt über Verfahren, die sicherstellen, dass das Wettbewerbsrecht der Union und die nationalen Wettbewerbsvorschriften eingehalten werden;

10. der Anbieter, der Dienste für betroffene Personen anbietet, handelt im besten Interesse der betroffenen Personen und erleichtert ihnen die Ausübung ihrer Rechte; insbesondere berät er betroffene Personen in Bezug auf mögliche Arten der Nutzung der Daten und übliche Geschäftsbedingungen für solche Nutzungen;

11. stellt ein Anbieter Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von juristischen Personen zur Verfügung gestellten Daten bereit, so gibt er das Hoheitsgebiet oder die Hoheitsgebiete an, in denen die Datennutzung stattfinden soll.

Artikel 12
Zuständige Behörden

(1) Jeder Mitgliedstaat benennt in seinem Hoheitsgebiet eine oder mehrere Behörden, die für die Wahrnehmung der Aufgaben im Zusammenhang mit dem Anmelderahmen zuständig sind, und teilt der Kommission bis zum [Beginn der Anwendung dieser Verordnung] die Namen dieser benannten Behörden mit. Er teilt der Kommission auch alle späteren diesbezüglichen Änderungen mit.

(2) Die benannten zuständigen Behörden müssen den Anforderungen des Artikels 23 genügen.

(3) Die benannten zuständigen Behörden, die Datenschutzbehörden, die nationalen Wettbewerbsbehörden, die für Cybersicherheit zuständigen Behörden und andere einschlägige Fachbehörden tauschen die Informationen aus, die für die Wahrnehmung ihrer Aufgaben in Bezug auf Anbieter von Diensten für die gemeinsame Datennutzung erforderlich sind.

Artikel 13
Überwachung der Einhaltung

(1) Die zuständige Behörde überwacht und beaufsichtigt die Einhaltung dieses Kapitels.

(2) Die zuständige Behörde ist befugt, von den Anbietern von Diensten für die gemeinsame Datennutzung alle Informationen anzufordern, die nötig sind, um die Einhaltung der Anforderungen der Artikel 10 und 11 zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(3) Stellt die zuständige Behörde fest, dass ein Anbieter von Diensten für die gemeinsame Datennutzung gegen eine oder mehrere Anforderungen des Artikels 10 oder 11 verstößt, teilt sie dies dem betreffenden Anbieter mit und gibt ihm Gelegenheit, innerhalb einer angemessenen Frist dazu Stellung zu nehmen.

(4) Die zuständige Behörde ist befugt, die Beendigung des in Absatz 3 genannten Verstoßes entweder unverzüglich oder innerhalb einer angemessenen Frist zu verlangen, und ergreift angemessene und verhältnismäßige Maßnahmen, um die Einhaltung sicherzustellen. In dieser Hinsicht müssen die zuständigen Behörden gegebenenfalls in der Lage sein,

a) abschreckende Geldstrafen, die Zwangsgelder mit Rückwirkung umfassen können, zu verhängen,

b) die Einstellung oder Aussetzung der Erbringung des Dienstes für die gemeinsame Datennutzung anzuordnen.

(5) Die zuständigen Behörden teilen der betreffenden Einrichtung unverzüglich die gemäß Absatz 4 auferlegten Maßnahmen und die Gründe dafür mit und setzen der Einrichtung eine angemessene Frist, damit sie den Maßnahmen nachkommen kann.

(6) Hat ein Anbieter von Diensten für die gemeinsame Datennutzung seine Hauptniederlassung oder seinen gesetzlichen Vertreter in einem Mitgliedstaat, erbringt aber Dienste in anderen Mitgliedstaaten, so arbeiten die zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder der gesetzliche Vertreter befindet, und die zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden zuständigen Behörden und das Ersuchen umfassen, die in diesem Artikel genannten Maßnahmen zu ergreifen.

Artikel 14
Ausnahmen

Dieses Kapitel gilt nicht für Einrichtungen ohne Erwerbszweck, deren Tätigkeit ausschließlich darin besteht, für Ziele von allgemeinem Interesse Daten zu sammeln, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus zur Verfügung gestellt werden.

KAPITEL IV
DATENALTRUISMUS

Artikel 15
Register der anerkannten datenaltruistischen Organisationen

(1) Jede nach Artikel 20 benannte zuständige Behörde führt ein Register der anerkannten datenaltruistischen Organisationen.

(2) Die Kommission pflegt ein Unionsregister der anerkannten datenaltruistischen Organisationen.

(3) Eine gemäß Artikel 16 im Register eingetragene Einrichtung darf sich in ihrer schriftlichen und mündlichen Kommunikation als „in der Union anerkannte datenaltruistische Organisation“ bezeichnen.

Artikel 16
Allgemeine Eintragungsanforderungen

Um für eine Eintragung infrage zu kommen, muss die datenaltruistische Organisation

a) Rechtspersönlichkeit haben und zur Verfolgung von Zielen von allgemeinem Interesse gegründet worden sein;

b) selbst ohne Erwerbszweck tätig sein und unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln;

c) die Datenaltruismus-Tätigkeiten über eine rechtlich unabhängige Struktur ausüben, die von anderen Tätigkeiten, die sie durchführt, getrennt ist.

Artikel 17
Eintragung

(1) Jede Einrichtung, die die Anforderungen des Artikels 16 erfüllt, kann die Eintragung in das in Artikel 15 Absatz 1 genannte Register der anerkannten datenaltruistischen Organisationen beantragen.

(2) Für die Zwecke dieser Verordnung gilt, dass eine Einrichtung, die datenaltruistische Tätigkeiten ausübt und in mehreren Mitgliedstaaten niedergelassen ist, in das Register des Mitgliedstaats eingetragen wird, in dem sie ihre Hauptniederlassung hat.

(3) Eine Einrichtung, die nicht in der Union niedergelassen ist, aber die Anforderungen des Artikels 16 erfüllt, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in denen sie Daten auf der Grundlage des Datenaltruismus sammeln will. Für die Zwecke der Einhaltung dieser Verordnung gilt, dass diese Einrichtung der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem der gesetzliche Vertreter niedergelassen ist.

(4) Der Eintragungsantrag muss folgende Angaben enthalten:

a) Bezeichnung der Einrichtung,

b) Rechtsstatus, Rechtsform und Registernummer der Einrichtung, sofern sie in einem öffentlichen Register eingetragen ist,

c) die Satzung der Einrichtung, falls zutreffend,

d) die Haupteinnahmequellen der Einrichtung,

e) die Anschrift der Hauptniederlassung der Einrichtung in der Union, falls zutreffend, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gemäß Absatz 3 benannten gesetzlichen Vertreters,

f) eine Website mit Informationen über die Einrichtung und ihre Tätigkeiten,

g) die Kontaktpersonen und Kontaktangaben der Einrichtung,

h) die Zwecke von allgemeinem Interesse, die sie mit der Sammlung der Daten fördern will;

i) alle sonstigen Nachweise, die belegen, dass die Anforderungen des Artikels 16 erfüllt werden.

(5) Nachdem die Einrichtung alle erforderlichen Informationen gemäß Absatz 4 übermittelt hat und die zuständige Behörde zu dem Schluss gekommen ist, dass die Einrichtung die Anforderungen des Artikels 16 erfüllt, nimmt die Behörde innerhalb von zwölf Wochen nach Antragstellung die Eintragung der Einrichtung in das Register der anerkannten datenaltruistischen Organisationen vor. Die Eintragung gilt in allen Mitgliedstaaten. Jede Eintragung wird der Kommission zwecks Aufnahme in das Unionsregister der anerkannten datenaltruistischen Organisationen mitgeteilt.

(6) Die in Absatz 4 Buchstaben a, b, f, g und h genannten Angaben werden im nationalen Register der anerkannten datenaltruistischen Organisationen veröffentlicht.

(7) Jede Einrichtung, die im Register der anerkannten datenaltruistischen Organisationen eingetragen ist, meldet der zuständigen Behörde jede Änderung der gemäß Absatz 4 übermittelten Angaben innerhalb von 14 Kalendertagen ab dem Tag der Änderung.

Artikel 18
Transparenzanforderungen

(1) Die im nationalen Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen führen vollständige und genaue Aufzeichnungen über Folgendes:

a) alle natürlichen oder juristischen Personen, denen die Möglichkeit zur Verarbeitung der im Besitz dieser Einrichtung befindlichen Daten gegeben wurde,

b) den Zeitpunkt oder den Zeitraum einer solchen Verarbeitung,

c) den Zweck einer solchen Verarbeitung entsprechend der Erklärung der natürlichen oder juristischen Person, der die Möglichkeit zur Verarbeitung gegeben wurde,

d) etwaige Gebühren, die von den die Daten verarbeitenden natürlichen oder juristischen Personen gezahlt wurden.

(2) Alle im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen erstellen einen jährlichen Tätigkeitsbericht und übermitteln ihn der zuständigen nationalen Behörde; dieser Bericht enthält mindestens Folgendes:

a) Informationen über die Tätigkeiten der Einrichtung,

b) eine Darlegung, in welcher Weise die Zwecke von allgemeinem Interesse, zu denen die Daten gesammelt wurden, in dem betreffenden Geschäftsjahr gefördert wurden,

c) eine Liste aller natürlichen und juristischen Personen, denen erlaubt wurde, die in ihrem Besitz befindlichen Daten zu nutzen, einschließlich einer zusammenfassenden Beschreibung der Zwecke von allgemeinem Interesse, die mit dieser Datennutzung verfolgt wurden, und einer Beschreibung der hierzu herangezogenen technischen Mittel, die auch eine Beschreibung der zur Wahrung der Privatsphäre und des Datenschutzes eingesetzten Techniken umfasst,

d) gegebenenfalls eine Zusammenfassung der Ergebnisse der von der Einrichtung erlaubten Datennutzungen,

e) Informationen über die Einnahmequellen der Einrichtung, insbesondere alle Einnahmen aus der Zugänglichmachung der Daten, sowie über die Ausgaben.

Artikel 19

Besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und juristischer Personen im Hinblick auf ihre Daten

(1) Die im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen informieren Dateninhaber über Folgendes:

a) die Zwecke von allgemeinem Interesse, für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt, in leicht verständlicher Form;

b) eine etwaige Verarbeitung außerhalb der Union.

(2) Die Einrichtung stellt ferner sicher, dass die Daten nicht für andere als die Zwecke von allgemeinem Interesse, für die sie die Verarbeitung erlaubt hat, verarbeitet werden.

(3) Stellt eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von juristischen Personen zur Verfügung gestellten Daten bereit, so gibt sie das Hoheitsgebiet oder die Hoheitsgebiete an, in denen die Datennutzung stattfinden soll.

Artikel 20

Für die Eintragung zuständige Behörden

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für das Register der anerkannten datenaltruistischen Organisationen und für die Überwachung der Einhaltung der Anforderungen dieses Kapitels zuständig sind. Die benannten zuständigen Behörden müssen den Anforderungen des Artikels 23 entsprechen.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen der benannten Behörden mit.

(3) Die zuständige Behörde nimmt ihre Aufgaben in Bezug auf die Verarbeitung personenbezogener Daten in Zusammenarbeit mit der Datenschutzbehörde sowie mit den einschlägigen sektoralen Gremien desselben Mitgliedstaats wahr. In Bezug auf etwaige Fragen, die eine Prüfung der Einhaltung der Verordnung (EU) 2016/679 erfordern, ersucht die zuständige Behörde zunächst um eine Stellungnahme oder

einen Beschluss der gemäß dieser Verordnung zuständigen Aufsichtsbehörde und richtet sich nach dieser Stellungnahme oder diesem Beschluss.

Artikel 21
Überwachung der Einhaltung

(1) Die zuständige Behörde überwacht und beaufsichtigt die Einhaltung der in diesem Kapitel festgelegten Bedingungen seitens der im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen.

(2) Die zuständige Behörde ist befugt, von den im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen alle Informationen anzufordern, die nötig sind, um die Einhaltung der Bestimmungen dieses Kapitels zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(3) Stellt die zuständige Behörde fest, dass eine Einrichtung gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies der Einrichtung mit und gibt ihr Gelegenheit, innerhalb einer angemessenen Frist hierzu Stellung zu nehmen.

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

(5) Erfüllt eine Einrichtung eine oder mehrere der Anforderungen dieses Kapitels auch dann nicht, nachdem sie von der zuständigen Behörde gemäß Absatz 3 davon unterrichtet wurde, so

a) verliert sie ihr Recht, sich in ihrer schriftlichen und mündlichen Kommunikation als „in der Union anerkannte datenaltruistische Organisation“ bezeichnen, und

b) wird aus dem Register der anerkannten datenaltruistischen Organisationen gestrichen.

(6) Hat eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung ihre Hauptniederlassung oder ihren gesetzlichen Vertreter in einem Mitgliedstaat, betätigt sich aber in anderen Mitgliedstaaten, so arbeiten die zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder der gesetzliche Vertreter befindet, und die zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander, soweit notwendig. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden zuständigen Behörden und Ersuchen umfassen, die in diesem Artikel genannten Aufsichtsmaßnahmen zu ergreifen.

Artikel 22
Europäisches Einwilligungsformular für Datenaltruismus

(1) Um das Sammeln von Daten auf der Grundlage des Datenaltruismus zu erleichtern, kann die Kommission Durchführungsrechtsakte zur Festlegung eines europäischen Einwilligungsformulars für Datenaltruismus erlassen. Das Formular ermöglicht das Einholen von Einwilligungen in allen Mitgliedstaaten in einem einheitlichen Format. Diese Durchführungsrechtsakte werden nach dem in Artikel 29 Absatz 2 genannten Beratungsverfahren erlassen.

(2) Das europäische Einwilligungsformular für Datenaltruismus ist modular aufgebaut, damit es an bestimmte Sektoren und für verschiedene Zwecke angepasst werden kann.

(3) Werden personenbezogene Daten erfasst, so muss das europäische Einwilligungsformular für Datenaltruismus es ermöglichen, dass betroffene Personen gemäß der Verordnung (EU) 2016/679 damit ihre Einwilligung zu einem bestimmten Datenverarbeitungsvorgang erteilen und widerrufen können.

(4) Das Formular wird in einer Form bereitgestellt, in der es auf Papier ausgedruckt und vom Menschen gelesen werden kann, sowie in elektronischer, maschinenlesbarer Form.

KAPITEL V
ZUSTÄNDIGE BEHÖRDEN UND VERFAHRENSVORSCHRIFTEN

Artikel 23
Anforderungen an zuständige Behörden

(1) Die gemäß Artikel 12 und Artikel 20 benannten zuständigen Behörden müssen von allen Anbietern von Diensten für die gemeinsame Datennutzung und allen im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen rechtlich getrennt und funktional unabhängig sein.

(2) Die zuständigen Behörden nehmen ihre Aufgaben unparteiisch, transparent, kohärent und rechtzeitig war.

(3) Die oberste Leitungsebene und die Mitarbeiter, die für die Durchführung der in dieser Verordnung vorgesehenen einschlägigen Aufgaben der zuständigen Behörde verantwortlich sind, dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der von ihnen bewerteten Dienste noch Bevollmächtigte einer dieser Parteien sein oder sie vertreten. Dies schließt die Verwendung von bewerteten Diensten, die für die Tätigkeit der zuständigen Stelle nötig sind, oder die Verwendung solcher Dienste zum persönlichen Gebrauch nicht aus.

(4) Die oberste Leitungsebene und die Mitarbeiter dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den ihnen anvertrauten Bewertungstätigkeiten beeinträchtigen könnten.

(5) Die zuständigen Behörden müssen über angemessene finanzielle und personelle Mittel verfügen, um die ihnen übertragenen Aufgaben erfüllen zu können, einschließlich der erforderlichen Fachkenntnisse und Ressourcen.

(6) Die zuständigen Behörden eines Mitgliedstaats stellen der Kommission und den zuständigen Behörden anderer Mitgliedstaaten auf begründeten Antrag die Informationen zur Verfügung, die sie zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung benötigen. Sieht eine zuständige nationale Behörde die verlangten Informationen nach den Vorschriften der Union und nationalen Rechtsvorschriften über das Geschäftsgeheimnis als vertraulich an, so gewährleisten die Kommission und alle anderen zuständigen Behörden eine entsprechende vertrauliche Behandlung.

Artikel 24
Beschwerderecht

(1) Natürliche und juristische Personen haben das Recht, bei der jeweiligen nationalen zuständigen Behörde Beschwerde gegen einen Anbieter von Diensten für die gemeinsame Datennutzung oder gegen eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung einzulegen.

(2) Die Behörde, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung sowie über die Möglichkeit eines wirksamen gerichtlichen Rechtsbehelfs nach Artikel 25.

Artikel 25
Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Jede betroffene natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf

a) Untätigkeit im Anschluss an eine Beschwerde bei einer in den Artikeln 12 und 20 genannten zuständigen Behörde,

b) Entscheidungen der in den Artikeln 13, 17 und 21 genannten zuständigen Behörden in Bezug auf die Verwaltung, Kontrolle und Durchsetzung der Anmeldevorschriften für Anbieter von Diensten für die gemeinsame Datennutzung und in Bezug auf die Überwachung von im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen.

(2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.

KAPITEL VI
EUROPÄISCHER DATENINNOVATIONSRAT

Artikel 26
Europäischer Dateninnovationsrat

(1) Die Kommission setzt einen Europäischen Dateninnovationsrat (im Folgenden „Innovationsrat“) ein, der die Form einer Expertengruppe hat und sich aus Vertretern der zuständigen Behörden aller Mitgliedstaaten, des Europäischen Datenschutzausschusses, der Kommission, einschlägiger Datenräume und anderen Vertretern zuständiger Fachbehörden zusammensetzt.

(2) Interessenträger und maßgebliche Dritte können zur Teilnahme an den Sitzungen des Innovationsrates und zur Beteiligung an seiner Arbeit eingeladen werden.

(3) Die Kommission führt den Vorsitz in den Sitzungen des Innovationsrates.

(4) Der Innovationsrat wird von einem Sekretariat unterstützt, das von der Kommission gestellt wird.

Artikel 27
Aufgaben des Innovationsrates

Der Innovationsrat hat folgende Aufgaben:

a) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der öffentlichen Stellen und der in Artikel 7 Absatz 1 genannten zuständigen Stellen, die Anträge auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien bearbeiten;

b) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der zuständigen Behörden bei der Anwendung der Anforderungen, die für Anbieter von Diensten für die gemeinsame Datennutzung gelten;

c) Beratung der Kommission bei der Festlegung von Prioritäten für die Verwendung bzw. Entwicklung sektorübergreifender Normen für die Datennutzung und sektorübergreifende gemeinsame Datennutzung sowie für den sektorübergreifenden Vergleich und Austausch bewährter Verfahren in Bezug auf Sicherheitsanforderungen und Zugangsverfahren in bestimmten Sektoren, wobei sektorspezifische Normungstätigkeiten zu berücksichtigen sind;

d) Unterstützung der Kommission bei der Verbesserung der Interoperabilität von Daten sowie von Diensten für die gemeinsame Datennutzung zwischen verschiedenen Sektoren und Bereichen auf der Grundlage bestehender europäischer, internationaler oder nationaler Normen;

e) Erleichterung der Zusammenarbeit zwischen den zuständigen nationalen Behörden im Rahmen dieser Verordnung mittels Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für einen effizienten Informationsaustausch über das Anmeldeverfahren für Anbieter von Diensten für die gemeinsame Datennutzung und die Eintragung und Überwachung anerkannter datenaltruistischer Organisationen.

KAPITEL VII
AUSSCHUSS UND DELEGIERUNG

Artikel 28
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 5 Absatz 11 wird der Kommission auf unbestimmte Zeit ab dem […] übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5 Absatz 11 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 5 Absatz 11 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 29
Ausschussverfahren

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

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

(3) Wird die Stellungnahme des Ausschusses im schriftlichen Verfahren eingeholt, so wird das Verfahren ohne Ergebnis beendet, wenn der Vorsitz des Ausschusses dies innerhalb der Frist für die Abgabe der Stellungnahme beschließt oder ein Ausschussmitglied dies verlangt. In einem solchen Fall beruft der Vorsitz innerhalb einer angemessenen Frist eine Ausschusssitzung ein.

KAPITEL VIII
SCHLUSSBESTIMMUNGEN

Artikel 30
Internationaler Zugang

(1) Die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, der Anbieter von Diensten für die gemeinsame Datennutzung oder die im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung ergreifen alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, um die Übertragung in der Union gespeicherter nicht personenbezogener Daten oder den Zugang zu diesen Daten zu verhindern, wenn eine solche Übertragung oder ein solcher Zugang im Widerspruch zum Unionsrecht oder dem Recht des betreffenden Mitgliedstaats stünde, es sei denn, die Übertragung oder der Zugang steht im Einklang mit Absatz 2 oder Absatz 3.

(2) Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einer öffentlichen Stelle, einer natürlichen oder juristischen Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, einem Anbieter von Diensten für die gemeinsame Datennutzung oder einer im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtung die Übertragung von nicht personenbezogener Daten, die von dieser Verordnung erfasst werden, aus der Union oder der Zugang zu diesen Daten in der Union verlangt wird, dürfen nur dann

anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder auf eine solche vor dem [Inkrafttreten dieser Verordnung] geschlossene Vereinbarung zwischen dem ersuchenden Drittland und einem Mitgliedstaat gestützt sind.

(3) Ist eine Entscheidung eines Gerichts oder einer Verwaltungsbehörde eines Drittlands, mit der die Übertragung nicht personenbezogener Daten aus der Union oder der Zugang zu diesen Daten in der Union verlangt wird, an eine öffentliche Stelle, eine natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, einen Anbieter von Diensten für die gemeinsame Datennutzung oder eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung gerichtet und würde die Befolgung einer solchen Entscheidung den Adressaten in Widerspruch zum Unionsrecht oder zum Recht des betreffenden Mitgliedstaats bringen, so erfolgt die Übertragung dieser Daten an die Behörde des Drittlands oder die entsprechende Zugangsgewährung nur dann,

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

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

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

Der Adressat der Entscheidung holt die Stellungnahme der zuständigen Stellen oder Behörden gemäß dieser Verordnung ein, um festzustellen, ob diese Bedingungen erfüllt sind.

(4) Sind die Bedingungen des Absatzes 2 oder 3 nicht erfüllt, so überträgt die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, der Anbieter von Diensten für die gemeinsame Datennutzung oder die im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung aufgrund einer vertretbaren Auslegung des Ersuchens nur die auf das Ersuchen hin zulässige Mindestmenge an Daten.

(5) Die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, der Anbieter von Diensten für die gemeinsame Datennutzung oder die im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung unterrichtet den Dateninhaber über das Vorliegen eines Ersuchens einer Verwaltungsbehörde eines Drittlands auf Zugang zu seinen Daten, es sei denn, das Ersuchen dient Strafverfolgungszwecken, und solange dies zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahme erforderlich ist.

Artikel 31
Sanktionen

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. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum [Beginn der Anwendung dieser Verordnung] mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

Artikel 32
Bewertung und Überprüfung

Bis zum [*vier Jahre nach dem Beginn der Anwendung dieser Verordnung*] führt die Kommission eine Bewertung dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über deren wichtigste Ergebnisse. Die Mitgliedstaaten übermitteln der Kommission alle erforderlichen Informationen zur Ausarbeitung dieses Berichts.

Artikel 33
Änderung der Verordnung (EU) 2018/1724

In Anhang II der Verordnung (EU) 2018/1724 wird unter „Gründung, Führung und Schließung eines Unternehmens“ folgende Zeile eingefügt:

Gründung, Führung und Schließung eines Unternehmens	Anmeldung als Anbieter von Diensten für die gemeinsame Datennutzung	Bestätigung des Eingangs der Anmeldung
	Eintragung als europäische datenaltruistische Organisation	Bestätigung der Eintragung

Artikel 34
Übergangsbestimmungen

Einrichtungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung die in Artikel 9 Absatz 1 genannten Dienste für die gemeinsame Datennutzung bereits erbringen, müssen den in Kapitel III festgelegten Verpflichtungen spätestens ab dem [2 Jahre nach dem Beginn der Anwendung dieser Verordnung] nachkommen.

Artikel 35
Inkrafttreten und Anwendung

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

Sie gilt ab dem [12 Monate nach ihrem Inkrafttreten].

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

Geschehen zu Brüssel am […]

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