

## I

*(Gesetzgebungsakte)*

## VERORDNUNGEN

## VERORDNUNG (EU) 2022/868 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 30. Mai 2022

**über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)****(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 <sup>(1)</sup>,

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren <sup>(2)</sup>,

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 dürfte zu diesen Zielen unter uneingeschränkter Achtung der Grundrechte beitragen. Zudem dürfte sie die Stärkung der offenen strategischen Autonomie der Union gewährleisten und den freien internationalen Datenverkehr fördern.
- (2) Im letzten Jahrzehnt 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 sowohl den Bürgerinnen und Bürgern der Union als auch der Wirtschaft enorme Vorteile bringen, beispielsweise durch eine Verbesserung und Personalisierung der Medizin, durch das Ermöglichen einer neuen Mobilität und durch das Beitragen zu dem in der Mitteilung der Kommission vom 11. Dezember 2019 angekündigten europäischen Grünen Deal. Um diese datengesteuerte Wirtschaft für alle Unionsbürger inklusiv zu gestalten, muss der Verringerung der digitalen Kluft, der Stärkung der Teilhabe von Frauen an der Datenwirtschaft und der Förderung von auf dem neuesten Stand befindlichen europäischen Sachkenntnissen im Technologiesektor besondere Aufmerksamkeit gewidmet werden. Die Datenwirtschaft muss so gestaltet werden, dass Unternehmen – insbesondere Kleinunternehmen sowie kleine und mittlere Unternehmen (KMU) im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission <sup>(3)</sup> sowie Start-up-Unternehmen – gedeihen können, die Neutralität des Datenzugangs sowie die Datenübertragbarkeit und die Interoperabilität von Daten sichergestellt sind und Lock-in-Effekte vermieden werden. In ihrer Mitteilung vom 19. Februar 2020 über eine Europäische Datenstrategie (Europäische Datenstrategie) erläuterte die Kommission ihre Vision für einen gemeinsamen europäischen Datenraum, d. h. einen Binnenmarkt für Daten, in dem Daten unabhängig vom physischen Ort ihrer Speicherung in der Union unter Einhaltung des geltenden Rechts verwendet werden können, der unter anderem für die schnelle Entwicklung von KI-Technologien von entscheidender Bedeutung sein könnte.

<sup>(1)</sup> ABl. C 286 vom 16.7.2021, S. 38.

<sup>(2)</sup> Standpunkt des Europäischen Parlaments vom 6. April 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 16. Mai 2022.

<sup>(3)</sup> Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Zudem forderte die Kommission einen freien und sicheren Datenverkehr mit Drittländern, wobei allerdings Ausnahmen und Beschränkungen zur öffentlichen Sicherheit, zur öffentlichen Ordnung und zu anderen berechtigten Zielen des Gemeinwohls in der Union im Einklang mit internationalen Verpflichtungen, auch den Grundrechten, zu beachten sind. Damit aus dieser Vision Wirklichkeit wird, schlug die Kommission vor, gemeinsame europäische Datenräume für verschiedene Bereiche für eine gemeinsame Nutzung und Bündelung von Daten einzurichten. Wie bereits in der Europäischen Datenstrategie vorgeschlagen, können sich diese gemeinsamen europäischen Datenräume auf Bereiche wie Gesundheit, Mobilität, Fertigung, Finanzdienstleistungen, Energie und Landwirtschaft oder auf eine Kombination dieser Bereiche, beispielsweise der Bereiche Energie und Klima, sowie auf Themen wie den europäischen Grünen Deal oder europäische Datenräume für die öffentliche Verwaltung oder Qualifikationen erstrecken. Die gemeinsamen europäischen Datenräume sollten dafür sorgen, dass Daten auffindbar, zugänglich, interoperabel und weiterverwendbar sind (im Folgenden „FAIR-Datengrundsätze“) und gleichzeitig ein hohes Maß an Cybersicherheit gewährleistet ist. Wenn in der Datenwirtschaft gleiche Wettbewerbsbedingungen bestehen, stützt sich der Wettbewerb der Unternehmen auf die Qualität der Dienstleistungen und nicht auf die Menge der von ihnen kontrollierten Daten. Für die Gestaltung, Schaffung und Aufrechterhaltung gleicher Wettbewerbsbedingungen in der Datenwirtschaft bedarf es solider Governance mit Beteiligung und Vertretung relevanter Interessenträger eines gemeinsamen europäischen Datenraums.

- (3) Es ist notwendig, die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt zu verbessern und dazu einen harmonisierten Rahmen für den Datenaustausch zu schaffen sowie bestimmte grundlegende Anforderungen an die Daten-Governance festzulegen, wobei der Erleichterung der Kooperation besondere Aufmerksamkeit zu widmen ist. Ziel dieser Verordnung sollte es sein, die Entwicklung eines grenzfreien digitalen Binnenmarktes sowie eine auf den Menschen ausgerichtete, vertrauenswürdige und sichere Datengesellschaft und -wirtschaft voranzutreiben. Mit sektorspezifischem Unionsrecht, wie beispielsweise dem vorgesehenen Unionsrecht zum europäischen Gesundheitsdatenraum 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, darunter auch Vorschriften für die grenzüberschreitende bzw. unionsweite gemeinsame Nutzung von Daten und den Zugang zu Daten, beispielsweise die Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates <sup>(4)</sup> im Zusammenhang mit dem europäischen Gesundheitsdatenraum sowie die einschlägigen Gesetzgebungsakte im Bereich Verkehr, z. B. die Verordnungen (EU) 2019/1239 <sup>(5)</sup> und (EU) 2020/1056 <sup>(6)</sup> und die Richtlinie 2010/40/EU <sup>(7)</sup> des Europäischen Parlaments und des Rates mit Blick auf den europäischen Mobilitätsdatenraum.

<sup>(4)</sup> Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

<sup>(5)</sup> Verordnung (EU) 2019/1239 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Einrichtung eines europäischen Umfelds zentraler Meldeportale für den Seeverkehr und zur Aufhebung der Richtlinie 2010/65/EU (ABl. L 198 vom 25.7.2019, S. 64).

<sup>(6)</sup> Verordnung (EU) 2020/1056 des Europäischen Parlaments und des Rates vom 15. Juli 2020 über elektronische Frachtbeförderungsinformationen (ABl. L 249 vom 31.7.2020, S. 33).

<sup>(7)</sup> 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).

Daher sollten die Verordnungen (EG) Nr. 223/2009 <sup>(8)</sup>, (EU) 2018/858 <sup>(9)</sup> und (EU) 2018/1807 <sup>(10)</sup> und die Richtlinien 2000/31/EG <sup>(11)</sup>, 2001/29/EG <sup>(12)</sup>, 2004/48/EG <sup>(13)</sup>, 2007/2/EG <sup>(14)</sup>, 2010/40/EU, (EU) 2015/849 <sup>(15)</sup>, (EU) 2016/943 <sup>(16)</sup>, (EU) 2017/1132 <sup>(17)</sup>, (EU) 2019/790 <sup>(18)</sup> und (EU) 2019/1024 <sup>(19)</sup> des Europäischen Parlaments und des Rates sowie anderes sektorspezifisches Unionsrecht für den Zugang zu Daten und deren Weiterverwendung unberührt bleiben. Das Unionsrecht und das nationale Recht über den Zugang zu Daten und deren Weiterverwendung für Zwecke der Prävention, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie die diesbezügliche internationale Zusammenarbeit sollten von dieser Verordnung unberührt bleiben.

Diese Verordnung sollte die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit unberührt lassen. Die Weiterverwendung von aus diesen Gründen geschützten und im Besitz öffentlicher Stellen befindlichen Daten, einschließlich Daten aus Vergabeverfahren, die in den Anwendungsbereich der Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates <sup>(20)</sup> fallen, sollte nicht unter diese Verordnung fallen. Für die Weiterverwendung geschützter und im Besitz öffentlicher Stellen befindlicher Daten bestimmter Kategorien sowie für die Erbringung von Datenvermittlungsdiensten 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. Anbieter von Datenvermittlungsdiensten, die die Anforderungen dieser Verordnung erfüllen, sollten die Bezeichnung „in der Union anerkannter Anbieter von Datenvermittlungsdiensten“ führen dürfen. Juristische Personen, die bestrebt sind, Ziele von allgemeinem Interesse zu unterstützen, indem sie einschlägige Daten auf der Grundlage von Datenaltruismus in entsprechend großem Maßstab zur Verfügung stellen und die in dieser Verordnung festgelegten Anforderungen erfüllen, sollten sich als „in der Union anerkannte datenaltruistische Organisation“ eintragen lassen und diese Bezeichnung führen können. Sind diese öffentlichen Stellen, Anbieter von Datenvermittlungsdiensten oder, juristischen Personen (im Folgenden „anerkannte datenaltruistische Organisationen“) gemäß sektorspezifischem Unionsrecht oder nationalem Recht verpflichtet, bestimmte zusätzliche technische, administrative oder organisatorische Anforderungen einzuhalten, etwa im Rahmen von Genehmigungs- oder Zertifizierungsverfahren, so sollten auch diese Bestimmungen des sektorspezifischen Unionsrecht oder des nationalen Rechts Anwendung finden.

- 
- <sup>(8)</sup> 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).
- <sup>(9)</sup> 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).
- <sup>(10)</sup> 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).
- <sup>(11)</sup> 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).
- <sup>(12)</sup> 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).
- <sup>(13)</sup> 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).
- <sup>(14)</sup> Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) (ABl. L 108 vom 25.4.2007, S. 1).
- <sup>(15)</sup> Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. L 141 vom 5.6.2015, S. 73).
- <sup>(16)</sup> 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).
- <sup>(17)</sup> Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über bestimmte Aspekte des Gesellschaftsrechts (ABl. L 169 vom 30.6.2017, S. 46).
- <sup>(18)</sup> 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).
- <sup>(19)</sup> 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).
- <sup>(20)</sup> Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit und zur Änderung der Richtlinien 2004/17/EG und 2004/18/EG (ABl. L 216 vom 20.8.2009, S. 76).

- (4) Diese Verordnung sollte die Verordnungen (EU) 2016/679 <sup>(21)</sup> und (EU) 2018/1725 <sup>(22)</sup> des Europäischen Parlaments und des Rates sowie die Richtlinien 2002/58/EG <sup>(23)</sup> und (EU) 2016/680 <sup>(24)</sup> des Europäischen Parlaments und des Rates und die entsprechenden Bestimmungen des nationalen Rechts unberührt lassen, einschließlich in den Fällen, in denen personenbezogene und nicht personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden sind. Insbesondere sollte mit dieser Verordnung keine neue Rechtsgrundlage für die Verarbeitung personenbezogener Daten für irgendeine der regulierten Tätigkeiten geschaffen werden bzw. keine Änderung der Informationsanforderungen gemäß der Verordnung (EU) 2016/679 bewirkt werden. Die Durchführung dieser Verordnung sollte der grenzüberschreitenden Datenübertragung im Einklang mit Kapitel V der Verordnung (EU) 2016/679 nicht im Wege stehen. Im Fall eines Konflikts zwischen dieser Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem gemäß diesem Unionsrecht erlassenen nationalen Recht sollte das einschlägige Unionsrecht oder das nationale Recht über den Schutz personenbezogener Daten Vorrang haben. Es sollte möglich sein, Datenschutzbehörden als gemäß dieser Verordnung zuständige Behörden zu betrachten. Wenn andere Behörden als zuständige Behörden gemäß dieser Verordnung handeln, sollten sie dabei die Aufsichtsbefugnisse und –zuständigkeiten der Datenschutzbehörden gemäß der Verordnung (EU) 2016/679 davon unberührt bleiben.
- (5) Es muss auf Unionsebene gehandelt werden, um das Vertrauen in die gemeinsame Datennutzung zu stärken, indem geeignete Mechanismen geschaffen werden, die es den betroffenen Personen und Dateninhabern ermöglichen, Kontrolle über die sie betreffenden Daten auszuüben, und sonstige Hemmnisse für eine gut funktionierende und wettbewerbsfähige datengesteuerte Wirtschaft abzubauen. Die Verpflichtungen und Zusagen, die sich aus den von der Union abgeschlossenen völkerrechtlichen Handelsabkommen ergeben, sollten von dieser Maßnahme unberührt bleiben. Ein unionsweiter Governance-Rahmen sollte zum Ziel haben, das Vertrauen unter Einzelpersonen und Unternehmen in Bezug auf den Zugang zu Daten, deren Kontrolle, gemeinsame Nutzung, Verwendung und Weiterverwendung zu stärken, und zwar insbesondere durch die Schaffung geeigneter Mechanismen, die es den betroffenen Personen ermöglichen, ihre Rechte zu kennen und effektiv wahrzunehmen, sowie mit Blick auf die Weiterverwendung bestimmter Arten von Daten, die im Besitz des öffentlichen Sektors sind, auf die Erbringung von Diensten durch Anbieter von Datenvermittlungsdiensten für betroffene Personen, Dateninhaber und Datennutzer sowie auf die Erhebung und Verarbeitung von Daten, die von natürlichen und juristischen Personen für altruistische Zwecke zur Verfügung gestellt werden. Insbesondere kann durch mehr Transparenz hinsichtlich des Zwecks der Datennutzung und der Bedingungen, unter denen Unternehmen Daten speichern, zur Verbesserung des Vertrauens beitragen werden.
- (6) Die Vorstellung, dass Daten, die von öffentlichen Stellen oder sonstigen Einrichtungen mithilfe öffentlicher Gelder generiert oder erhoben wurden, auch der Gesellschaft zugutekommen sollten, hat seit Langem Eingang in die Strategie der Union gefunden. Die Richtlinie (EU) 2019/1024 und sektorspezifisches Unionsrecht zielen darauf ab, dass öffentliche Stellen die Zugänglichkeit der von ihnen erzeugten Daten für die Verwendung und Weiterverwendung in größerem Umfang erleichtern. Dennoch werden in öffentlichen Datenbanken vorhandene Daten bestimmter Kategorien, wie vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten, durch die Rechte Dritter an geistigem Eigentum geschützte Daten, einschließlich Geschäftsgeheimnissen und personenbezogener Daten, oft nicht einmal für Forschungszwecke oder innovative Tätigkeiten im öffentlichen Interesse zur Verfügung gestellt, obwohl diese Verfügbarkeit gemäß dem anwendbaren Unionsrecht, insbesondere der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG und der Richtlinie (EU) 2016/680, möglich ist. Aufgrund der Sensibilität solcher Daten müssen bestimmte verfahrenstechnische und rechtliche Anforderungen erfüllt werden, bevor sie zur Verfügung gestellt werden, nicht zuletzt zur Wahrung der Rechte Dritter an diesen sensiblen Daten oder zur Begrenzung nachteiliger Auswirkungen auf die Grundrechte, den Grundsatz der Nichtdiskriminierung und den Datenschutz. Die Erfüllung dieser Anforderungen erfordert in der Regel viel Zeit und Sachverstand. Dies hat dazu geführt, dass diese Daten unzureichend genutzt werden. Zwar haben einige Mitgliedstaaten Strukturen und Verfahren geschaffen oder Vorschriften erlassen, um die Weiterverwendung dieser Art von Daten zu erleichtern, doch gilt das nicht für die gesamte Union. Um die Nutzung von Daten für die europäische Forschung und Innovation durch private und öffentliche Einrichtungen zu erleichtern, bedarf es klarer Bedingungen für den Zugang zu solchen Daten und deren Nutzung in der gesamten Union.

<sup>(21)</sup> 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).

<sup>(22)</sup> 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).

<sup>(23)</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

<sup>(24)</sup> 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).

- (7) Für Datenbanken, die personenbezogene Daten enthalten, gibt es Techniken, die Analysen ermöglichen, z. B. Anonymisierung, differentielle Privatsphäre, Generalisierung oder Datenunterdrückung und Randomisierung, Verwendung synthetischer Daten oder ähnlicher Methoden sowie sonstige dem Stand der Technik entsprechende Methoden zur Wahrung der Privatsphäre, die zu einer datenschutzfreundlicheren Datenverarbeitung beitragen könnten. Die Mitgliedstaaten sollten öffentliche Stellen dabei unterstützen, solche Techniken optimal zu nutzen, um so viele Daten wie möglich für die gemeinsame Nutzung verfügbar zu machen. Mithilfe dieser Techniken im Verbund mit umfassenden Datenschutz-Folgenabschätzungen und sonstigen Schutzvorkehrungen kann ein Beitrag zu mehr Sicherheit bei der Verwendung und Weiterverwendung personenbezogener Daten geleistet werden und dürfte eine sichere Weiterverwendung vertraulicher Geschäftsdaten für Forschung, Innovation und statistische Zwecke gewährleistet werden können. In vielen Fällen bedeutet die Anwendung solcher Techniken, Folgenabschätzungen und sonstiger Schutzvorkehrungen, dass die Verwendung und Weiterverwendung von Daten nur in einer sicheren Verarbeitungsumgebung möglich ist, die der öffentlichen Stelle 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 <sup>(25)</sup> für Forschungsarbeiten zu statistischen Mikrodaten genutzt werden. Allgemein sollte die Verarbeitung personenbezogener Daten stets auf einer der Rechtsgrundlagen beruhen, die in den Artikeln 6 und 9 der Verordnung (EU) 2016/679 bestimmt sind.
- (8) Im Einklang mit der Verordnung (EU) 2016/679 sollten die Grundsätze des Datenschutzes nicht auf anonyme Informationen angewendet werden, d. h. auf Informationen, die sich nicht auf eine bestimmte oder bestimmbar natürliche Person beziehen, oder auf personenbezogene Daten, die in einer Weise anonymisiert wurden, dass die betroffene Person nicht oder nicht mehr bestimmt werden kann. Die erneute Identifizierung betroffener Personen anhand anonymisierter Datensätze sollte untersagt sein. Dies sollte die Möglichkeit unberührt lassen, im Einklang mit der Verordnung (EU) 2016/679 durchgeführte Forschungsarbeiten zu Anonymisierungstechniken durchzuführen, insbesondere um die Informationssicherheit zu gewährleisten, bestehende Anonymisierungstechniken zu verbessern und zur allgemeinen Zuverlässigkeit der Anonymisierung beizutragen.
- (9) Um den Schutz personenbezogener Daten und vertraulicher Daten zu erleichtern und das Verfahren für die Bereitstellung solcher Daten zur Weiterverwendung gemäß dieser Verordnung zu beschleunigen, sollten die Mitgliedstaaten die öffentliche Stellen dazu anhalten, Daten im Einklang mit dem in Artikel 5 Absatz 2 der Richtlinie (EU) 2019/1024 genannten Grundsatz „konzeptionell und standardmäßig offen“ zu erstellen und sie zugänglich zu machen, und die Erstellung und Beschaffung von Daten in Formaten und Strukturen fördern, die diesbezüglich eine Anonymisierung ermöglichen.
- (10) Daten, die sich im Besitz öffentlicher Stellen befinden und unter die Kategorien fallen, für die eine Weiterverwendung nach dieser Verordnung infrage kommt, 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 und Daten handelt, die Teil von Werken oder sonstigen Schutzgegenständen sind und durch Rechte Dritter an geistigem Eigentum geschützt werden. Vertrauliche Geschäftsdaten umfassen Daten, die durch das Geschäftsgeheimnis geschützt sind, geschütztes Know-how und etwaige sonstige Informationen, deren unrechtmäßige Offenlegung die Marktposition oder die finanzielle Solidität eines Unternehmens beeinträchtigen würde. Diese Verordnung sollte für personenbezogene Daten gelten, die insoweit nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024 fallen, als nach deren Zugangsregelungen der Zugang zu diesen Daten aus Gründen des Datenschutzes, des Schutzes der Privatsphäre und der Integrität von Einzelpersonen nach den Datenschutzvorschriften ausgeschlossen oder eingeschränkt ist. Die Weiterverwendung von Daten, die möglicherweise Geschäftsgeheimnisse enthalten, sollte unbeschadet der Richtlinie (EU) 2016/943 erfolgen, die den Rahmen für die Rechtmäßigkeit von Erwerb, Nutzung oder Offenlegung von Geschäftsgeheimnissen festlegt.
- (11) Diese Verordnung sollte keine Verpflichtung begründen, die Weiterverwendung von Daten zu erlauben, die sich im Besitz öffentlicher Stellen befinden. Daher sollte jeder Mitgliedstaat insbesondere entscheiden können, ob Daten zur Weiterverwendung zugänglich gemacht werden, und zwar auch im Hinblick auf die Zwecke und den Umfang eines solchen Zugangs. 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. Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden. Unter Berücksichtigung der Rolle des Zugangs der Öffentlichkeit zu amtlichen Dokumenten und der Transparenz in einer demokratischen Gesellschaft sollte diese Verordnung auch das Unionsrecht und das nationale Recht über die Gewährung des Zugangs zu amtlichen Dokumenten und deren Offenlegung unberührt lassen. Der Zugang zu amtlichen Dokumenten kann insbesondere entweder im Einklang mit nationalem Recht, ohne besondere Bedingungen festzulegen, oder durch die Festlegung besonderer Bedingungen, die in dieser Verordnung nicht vorgesehen sind, gewährt werden.

<sup>(25)</sup> 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).

- (12) 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 Besitz öffentlicher Unternehmen befindlichen Daten nicht unter diese Verordnung fallen. Auch sollte diese Verordnung nicht für Daten gelten, die sich im Besitz von Kultureinrichtungen – etwa von Bibliotheken, Archiven und Museen sowie Orchestern, Opern, Balletten und Theatern – oder Bildungseinrichtungen befinden, da die sich in ihrem Besitz befindlichen Werke und sonstigen Dokumente vorrangig den Rechten Dritter an geistigem Eigentum unterliegen. Forschungseinrichtungen und Forschungsfördereinrichtungen könnten auch als öffentliche Stellen oder Einrichtungen des öffentlichen Rechts aufgestellt werden.

Für solche hybriden Einrichtungen gilt diese Richtlinie nur in Bezug auf ihre Funktion als Forschungseinrichtung. Befinden sich Daten im Besitz einer Forschungseinrichtung, die Teil eines spezifischen öffentlich-privaten Zusammenschlusses mit Einrichtungen des privaten Sektors oder sonstigen öffentlichen Stellen, Einrichtungen des öffentlichen Rechts oder hybriden Forschungseinrichtungen, d. h. sowohl als öffentliche Stelle als auch als öffentliches Unternehmen aufgestellte Einrichtungen, mit dem Hauptzweck der Forschung ist, so sollten diese Daten ebenfalls nicht unter diese Verordnung fallen. Die Mitgliedstaaten sollten diese Verordnung gegebenenfalls auf öffentliche Unternehmen oder private Unternehmen, die Aufgaben des öffentlichen Sektors wahrnehmen oder Dienstleistungen von allgemeinem Interesse bereitstellen, anwenden können. Ein Austausch von Daten zwischen öffentlichen Stellen in der Union oder zwischen öffentlichen Stellen in der Union und öffentlichen Stellen in Drittländern oder internationalen Organisationen, der ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags stattfindet, sollte ebenso wie der Austausch von Daten zwischen Forschern zu nichtkommerziellen Forschungszwecken, nicht den Bestimmungen dieser Verordnung in Bezug auf die Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen unterliegen.

- (13) 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 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 oder der Bereitstellung eines Produkts im 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 erbringen oder ein Produkt bereitstellen kann, mit dem eine öffentliche Stelle in die Lage versetzt wird, einen Dienst im allgemeinen Interesse zu erbringen. Diese Vereinbarungen sollten jedoch gemäß dem anwendbaren Unionsrecht oder nationalen Recht 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 eine begrenzte Dauer, der zwölf Monate nicht überschreiten sollte, geschlossen werden. Im Sinne der Transparenz sollten solche Ausschließlichkeitsvereinbarungen im Internet in einer Form veröffentlicht werden, die im Einklang mit dem einschlägigen Unionsrecht über die Vergabe öffentlicher Aufträge steht. Entspricht ein ausschließliches Recht zur Weiterverwendung nicht dieser Verordnung, so sollte dieses ausschließliche Recht unwirksam sein.
- (14) Bereits vor dem Tag des Inkrafttretens dieser Verordnung bestehende und nunmehr verbotene Ausschließlichkeitsvereinbarungen und sonstige Praktiken oder Vereinbarungen, die die Weiterverwendung von Daten im Besitz von öffentlichen Stellen betreffen und die zwar keine 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 30 Monaten nach Inkrafttreten dieser Verordnung beendet werden.
- (15) Diese Verordnung sollte Bedingungen für die Weiterverwendung geschützter Daten festlegen, die für öffentliche Stellen gelten, die nach nationalem Recht als dafür zuständig benannt werden, die Weiterverwendung zu erlauben oder zu verweigern, und die die Rechte und Pflichten in Bezug auf den Zugang zu solchen Daten unberührt lassen. Diese Bedingungen sollten nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt sein und den Wettbewerb nicht einschränken, wobei insbesondere der Zugang von KMU und Start-up-Unternehmen zu solchen Daten gefördert werden sollte. Die Bedingungen für die Weiterverwendung sollten so gestaltet werden, dass wissenschaftliche Forschung gefördert wird, so dass beispielsweise die bevorzugte Behandlung der wissenschaftlichen Forschung als nicht diskriminierend betrachtet werden sollte. Öffentliche Stellen, die die Weiterverwendung von Daten erlauben, sollten über die für den Schutz der Rechte und Interessen Dritter erforderlichen technischen Mittel verfügen und dazu befugt sein, die notwendigen Informationen vom Weiterverwender anzufordern. Die Bedingungen für die Weiterverwendung von Daten sollten sich auf das beschränken, was zur Wahrung der Rechte und Interessen Dritter 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 den öffentlichen Stellen hieraus ein unverhältnismäßig hoher Aufwand erwächst. Die Bedingungen mit der Wiederverwendung von Daten verbundenen Bedingungen sollten derart konzipiert sein, dass wirksame Vorkehrungen in Bezug auf den Schutz personenbezogener Daten sichergestellt sind. Vor der Übermittlung sollten personenbezogene Daten anonymisiert werden, sodass ausgeschlossen ist, dass die betroffenen Personen identifiziert werden können, und sollten Daten, die vertrauliche Geschäftsinformationen enthalten, so verändert werden, dass keine vertraulichen Informationen offengelegt werden. Wenn die Bereitstellung anonymisierter oder veränderter Daten nicht den Bedürfnissen des Weiterverwenders entspricht und wenn etwaige Anforderungen in Bezug auf die Durchführung einer Datenschutz-Folgenabschätzung und die Konsultation der Aufsichtsbehörde gemäß den Artikeln 35 und 36 der Verordnung (EU) 2016/679 erfüllt wurden und die Risiken für die Rechte und Interessen der betroffenen Personen minimal sind, könnte die Weiterverwendung der Daten in den Räumlichkeiten der öffentlichen Stelle oder der Fernzugriff zur Verarbeitung in einer sicheren Verarbeitungsumgebung erlaubt werden.

Dies könnte eine geeignete Regelung für die Weiterverwendung pseudonymisierter Daten sein. 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 im Datenschutzrecht eine Rechtsgrundlage gibt. Nicht personenbezogene Daten sollten nur übermittelt werden, wenn kein Grund zu der Annahme besteht, dass betroffene Personen anhand der Kombination nicht personenbezogener Datensätze identifiziert werden können. Dies sollte auch für pseudonymisierte Daten gelten, die ihren Status als personenbezogene Daten behalten. Im Falle der erneuten Identifizierung betroffener Personen sollte zusätzlich zur einer Verpflichtung, eine solche Datenschutzverletzung gemäß Verordnung (EU) 2016/679 einer Aufsichtsbehörde und der betroffenen Person mitzuteilen, auch eine Verpflichtung bestehen, diese Datenschutzverletzung der öffentlichen Stelle mitzuteilen. Gegebenenfalls sollten die öffentlichen Stellen die Weiterverwendung von Daten auf der Grundlage der Einwilligung betroffener Personen bzw. Erlaubnis von Dateninhabern zur Weiterverwendung ihrer Daten mit geeigneten technischen Mitteln erleichtern. In diesem Zusammenhang sollte die öffentliche Stelle die potenziellen Weiterverwender der Daten nach besten Kräften bei der Einholung dieser Einwilligung oder Erlaubnis unterstützen, indem sie technische Mechanismen schafft, mit denen Einwilligungs- oder Erlaubnisanfragen der Weiterverwender weitergeleitet werden können, soweit dies praktisch durchführbar ist. Dabei sollten keine Kontaktangaben weitergegeben werden, die es Weiterverwendern ermöglichen würden, betroffene Personen oder Dateninhaber direkt zu kontaktieren. Bei der Übermittlung einer Einwilligungs- oder Erlaubnisanfrage sollte die öffentliche Stelle sicherstellen, dass die betroffene Person oder der Dateninhaber unmissverständlich darüber informiert wird, dass sie die Einwilligung oder Erlaubnis ablehnen kann.

- (16) Um die Nutzung von Daten im Besitz von öffentlichen Stellen für Zwecke der wissenschaftlichen Forschung zu erleichtern und zu fördern, werden die öffentlichen Stellen angehalten, einen harmonisierten Ansatz und harmonisierte Verfahren zu entwickeln, um diese Daten für Zwecke der wissenschaftlichen Forschung im öffentlichen Interesse leicht zugänglich zu machen. Dies könnte unter anderem bedeuten, dass gestraffte Verwaltungsverfahren, eine standardisierte Datenformatierung, informative Metadaten zu Entscheidungen über Methodik und Datenerhebung sowie standardisierte Datenfelder geschaffen werden, die es ermöglichen, Datensätze von verschiedenen Datenquellen des öffentlichen Sektors zu Analysezwecken gegebenenfalls leicht zusammenzuführen. Ziel dieser Verfahren sollte es sein, öffentlich finanzierte und erstellte Daten für Zwecke der wissenschaftlichen Forschung im Einklang mit dem Grundsatz „so offen wie möglich, so geschlossen wie nötig“ zu fördern.
- (17) Rechte Dritter an geistigem Eigentum sollten von dieser Verordnung unberührt bleiben. Diese Verordnung sollte weder bestehende Rechte öffentlicher Stellen an geistigem Eigentum oder deren Inhaberschaft daran berühren noch die Ausübung dieser Rechte in irgendeiner Weise einschränken. Die sich aus dieser Verordnung ergebenden Verpflichtungen sollten nur insoweit gelten, als 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), dem Urheberrechtsvertrag der Weltorganisation für geistiges Eigentum (WCT) sowie dem Unionsrecht oder dem nationalen Recht über geistiges Eigentum vereinbar sind. Öffentliche Stellen sollten ihre Urheberrechte jedoch auf eine Weise ausüben, die eine Weiterverwendung erleichtert.
- (18) 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 Inhaber des Datenbankherstellerechts nach Artikel 7 Absatz 1 der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates<sup>(26)</sup> 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.

<sup>(26)</sup> 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).

- (19) Unternehmen und betroffene Personen sollten darauf vertrauen können, dass die Weiterverwendung von geschützten Daten bestimmter Kategorien, die sich im Besitz von Stellen 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 außerhalb des öffentlichen Sektors erfolgt, wie eine Anforderung, dass öffentliche Stellen sicherstellen, dass in allen Fällen, auch wenn Daten in Drittländer übertragen werden, die Rechte und Interessen natürlicher und juristischer Personen in vollem Umfang gewahrt werden, insbesondere im Hinblick auf personenbezogene Daten, sensible Geschäftsdaten und Rechte des geistigen Eigentums. Öffentliche Stellen sollten die Weiterverwendung von Informationen, die von Versicherungsunternehmen oder sonstigen Dienstleistern in e-Gesundheitsanwendungen gespeichert werden, zum Zwecke der Diskriminierung bei der Festlegung von Preisen nicht gestatten, da dies dem Grundrecht auf Zugang zur Gesundheitsfürsorge zuwiderlaufen würde.
- (20) Außerdem ist es zur Wahrung eines fairen Wettbewerbs und der offenen Marktwirtschaft von größter Bedeutung, geschützte nicht personenbezogene Daten, 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 Rechte oder Interessen der Dateninhaber sollte es möglich sein, nicht personenbezogene Daten, die nach Unionsrecht oder dem nationalen Recht vor unrechtmäßigem oder unbefugtem Zugriff zu schützen sind und die sich im Besitz öffentlicher Stellen befinden, nur dann in Drittländer zu übertragen, wenn angemessene Schutzvorkehrungen für die Nutzung der Daten getroffen wurden. Zu diesen angemessenen Schutzvorkehrungen sollte auch eine Bedingung gehören, dass öffentliche Stellen geschützte Daten nur dann an einen Weiterverwender übermitteln, wenn dieser Weiterverwender sich zum Schutz der Daten vertraglich verpflichtet. Ein Weiterverwender, der beabsichtigt, die geschützten Daten in ein 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.
- (21) Angemessene Schutzvorkehrungen sollten auch dann als umgesetzt gelten, wenn in dem Drittland, in das nicht personenbezogene Daten übertragen werden sollen, gleichwertige Maßnahmen bestehen, mit denen gewährleistet wird, dass für Daten ein ähnliches Schutzniveau gilt wie das, das auf der Grundlage des Unionsrechts vor allem im Hinblick auf den Schutz von Geschäftsgeheimnissen und der Rechte des geistigen Eigentums Anwendung findet. Wenn dies aufgrund der Vielzahl unionsweit gestellter Anträge auf Weiterverwendung nicht personenbezogener Daten in bestimmten Drittländern gerechtfertigt ist, sollte die Kommission in der Lage sein, hierzu durch Durchführungsrechtsakte zu erklären, dass ein Drittland ein Schutzniveau bietet, das im Wesentlichen dem durch Unionsrecht gewährten Schutzniveau gleichwertig ist. Die Kommission sollte auf der Grundlage der von den Mitgliedstaaten über den Europäischen Dateninnovationsrat bereitgestellten Informationen die Notwendigkeit solcher Durchführungsrechtsakte prüfen. Durch solche Durchführungsrechtsakte hätten öffentliche Stellen die Gewissheit, dass der Schutz von Daten im Besitz öffentlicher Stellen bei deren Weiterverwendung in dem betreffenden Drittland nicht gefährdet wäre. Bei der Bewertung des in dem betreffenden Drittland gewährten Schutzniveaus sollten insbesondere das einschlägige allgemeine und sektorale Recht berücksichtigt werden, auch solche, die sich auf die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit beziehen, sowie die strafrechtlichen Vorschriften in Bezug auf den Zugang zu und den Schutz von nicht personenbezogenen Daten und auf den etwaigen Zugang der öffentlichen Stellen des betreffenden Drittlands zu den übertragenen Daten; außerdem sollten das Vorhandensein und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden, die in dem betreffenden Drittland für die Einhaltung und Durchsetzung der Rechtsvorschriften, mit denen der Zugang zu solchen Daten geregelt wird, zuständig sind, die internationalen Verpflichtungen hinsichtlich des Datenschutzes 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 Datenvermittlungsdiensten in dem betreffenden Drittland wirksame Rechtsbehelfe zur Verfügung stehen. Solche Schutzvorkehrungen sollten daher auch das Bestehen durchsetzbarer Rechte und wirksamer Rechtsbehelfe umfassen. Diese Durchführungsrechtsakte sollten rechtliche Verpflichtungen oder vertragliche Vereinbarungen, die ein Weiterverwender zum Schutz nicht personenbezogener Daten, insbesondere von Industriedaten, bereits eingegangen ist, sowie das Recht öffentlicher Stellen unberührt lassen, Weiterverwender im Einklang mit dieser Verordnung zur Einhaltung der Bedingungen für die Weiterverwendung zu verpflichten.

- (22) Einige Drittländer erlassen Gesetze, Verordnungen und sonstige Rechtsakte, die auf die unmittelbare Übertragung nicht personenbezogener Daten oder den unmittelbaren Zugang von Regierungsorganisationen zu diesen Daten, die in der Union der Kontrolle natürlicher oder juristischer Personen in der Gerichtsbarkeit von Mitgliedstaaten unterliegen, abzielen. Beschlüsse und Urteile von Gerichten in Drittländern oder Entscheidungen von Behörden in Drittländern, mit denen eine solche Übertragung oder ein solcher Zugang zu nicht personenbezogener Daten gefordert wird, sollten vollstreckbar sein, wenn sie sich auf ein völkerrechtliches Abkommen, etwa ein Rechtshilfe-

abkommen, stützen, das zwischen dem betreffenden Drittland und der Union oder einem Mitgliedstaat besteht. In einigen Fällen kann es dazu kommen, dass die sich aus einem Gesetz eines Drittlands ergebende Verpflichtung zur Übertragung nicht personenbezogener Daten oder zur Gewährung des Zugangs zu diesen Daten mit der Verpflichtung zum Schutz dieser Daten nach Unionsrecht oder nationalem Recht kollidiert, insbesondere im Hinblick auf den Schutz der Grundrechte der Einzelpersonen oder der grundlegenden Interessen eines Mitgliedstaats im Zusammenhang mit der nationalen Sicherheit oder der Landesverteidigung sowie auf den Schutz sensibler Geschäftsdaten und der Rechte des geistigen Eigentums, darunter auch vertragliche Vertraulichkeitspflichten nach einem solchen Gesetz. Besteht kein völkerrechtliches Abkommen zur Regelung dieser Fragen, so sollte die Übertragung von oder der Zugang zu nicht personenbezogenen Daten insbesondere nur dann erlaubt werden, wenn festgestellt wurde, dass das Rechtssystem des betreffenden Drittlands die Begründung und Verhältnismäßigkeit der Entscheidung oder des Urteils sowie die hinreichende Bestimmtheit des gerichtlichen Beschlusses oder des Urteils vorschreibt und dem Adressaten die Möglichkeit einräumt, seinen begründeten Einwand einem zuständigen Gericht des Drittlands, das befugt ist, die einschlägigen rechtlichen Interessen des Bereitstellers der Daten gebührend zu berücksichtigen, zur Überprüfung vorzulegen.

Darüber hinaus sollten öffentliche Stellen, natürliche oder juristische Personen, denen das Recht auf Weiterverwendung von Daten gewährt wurde, Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistischen Organisationen bei der Unterzeichnung von vertraglichen Vereinbarungen mit sonstigen privaten Parteien sicherstellen, dass der Zugriff durch Drittländer auf in der Union gespeicherte nicht personenbezogene Daten oder deren Übertragung in Drittländer nur im Einklang mit dem Unionsrecht und dem nationalen Recht des entsprechenden Mitgliedstaats erfolgt.

- (23) Das Vertrauen in die Datenwirtschaft kann nur weiter gestärkt werden, wenn die Schutzvorkehrungen, mit denen die Kontrolle über die strategischen und sensiblen Daten der Bürgerinnen und Bürger, des öffentlichen Sektors und der Unternehmen der Union sichergestellt wird, umgesetzt werden und das Recht, die Werte und die Standards der Union, unter anderem in Bezug auf die Sicherheit, den Datenschutz und den Verbraucherschutz, gewährt werden. 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 Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen 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. Zu diesem Zweck sollte sichergestellt werden, dass öffentliche Stellen, natürliche oder juristische Personen, denen das Recht auf Weiterverwendung von Daten gewährt wurde, Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen alle einschlägigen technischen Standards, Verhaltenskodizes und Zertifizierungen auf Unionsebene einhalten.
- (24) Zum Aufbau von Vertrauen in die Weiterverwendungsmechanismen ist es möglicherweise notwendig, im Einklang mit völkerrechtlichen Verpflichtungen strengere Bedingungen an bestimmte Arten nicht personenbezogener Daten, zu knüpfen die im Hinblick auf die Übertragung in Drittländer in besonderen künftigen Gesetzgebungsakten der Union als hochsensibel eingestuft werden können, wenn diese Übertragung Ziele des Gemeinwohls der Union gefährden könnte. So könnten im Gesundheitsbereich bestimmte Datensätze, die sich im Besitz von öffentlichen Gesundheitseinrichtungen, wie beispielsweise Krankenhäusern, befinden, als hochsensible Gesundheitsdaten gelten. Andere einschlägige Sektoren erfassen die Bereiche Verkehr, Energie, Umwelt oder Finanzen. Um hier unionsweit einheitlich vorzugehen, sollte im Unionsrecht, beispielsweise im Zusammenhang mit dem europäischen Gesundheitsdatenraum oder anderem sektorspezifischem Recht, festgelegt werden, welche nicht personenbezogenen öffentlichen Daten als hochsensibel gelten. Diese 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 der Union notwendig sein, wie etwa für den Schutz der öffentlichen Gesundheit, der Sicherheit, der Umwelt, der guten Sitten, der Verbraucher sowie der Privatsphäre und personenbezogener Daten. Diese 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 hinsichtlich 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 diese Bedingungen zum Schutz öffentlicher Interessen auch Beschränkungen in Bezug auf die Übertragung der Daten in Drittländer enthalten.
- (25) Öffentliche Stellen sollten Gebühren für die Weiterverwendung von Daten erheben können, aber auch eine Weiterverwendung zu ermäßigten Gebühren oder eine kostenlose Weiterverwendung erlauben können, beispielsweise für bestimmte Kategorien der Weiterverwendung, etwa für nichtkommerzielle Zwecke, für Zwecke der wissenschaftlichen Forschung oder durch KMU, Start-up-Unternehmen, die Zivilgesellschaft und Bildungseinrichtungen, um so Anreize für die Weiterverwendung der Daten in Forschung und Innovation zu schaffen und unter Beachtung der 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 erheben. In diesem besonderen Zusammenhang sollten die Zwecke der wissenschaftlichen Forschung – unabhängig von der

organisatorischen oder finanziellen Struktur der betreffenden Forschungseinrichtung – jegliche Art von Forschungszweck umfassen, mit Ausnahme der Forschung, die von einem Unternehmen mit dem Ziel der Entwicklung, Verbesserung oder Optimierung von Produkten oder Dienstleistungen betrieben wird. Diese Gebühren sollten transparent und nichtdiskriminierend sein, in einem angemessenen Verhältnis zu den entstandenen Kosten stehen und den Wettbewerb nicht beschränken. Eine Liste der Kategorien von Weiterverwendern, von denen eine ermäßigte oder keine Gebühr erhoben wird, sollte zusammen mit den Kriterien für die Erstellung dieser Liste öffentlich zugänglich gemacht werden.

- (26) Um die Weiterverwendung von Daten besonderer Kategorien im Besitz öffentlicher Stellen Anreize zu schaffen, sollten die Mitgliedstaaten eine zentrale Informationsstelle einrichten, die als Anlaufstelle für diejenigen dient, die die Weiterverwendung von solchen Daten beabsichtigen. Die Informationsstelle sollte sektorübergreifend angelegt sein und erforderlichenfalls sektorale Regelungen ergänzen. Die zentrale Informationsstelle sollte Anfragen oder Anträge in Bezug auf die Weiterverwendung auf automatischem Wege übermitteln können. Beim Übermittlungsprozess sollte für ausreichende menschliche Aufsicht gesorgt sein. Zu diesem Zweck könnten bereits vorhandene praktische Strukturen wie offene Datenportale genutzt werden. Die zentrale Informationsstelle sollte über eine Bestandsliste verfügen, die einen Überblick über alle verfügbaren Datenressourcen, gegebenenfalls einschließlich der bei sektoralen, regionalen oder lokalen Informationsstellen verfügbaren Datenressourcen, und einschlägige Informationen mit einer Beschreibung der verfügbaren Daten enthält. Ferner sollten die Mitgliedstaaten zuständige Stellen benennen, einrichten oder deren Einrichtung erleichtern, um öffentliche Stellen, die die Weiterverwendung geschützter Daten bestimmter Kategorien erlauben, zu unterstützen. Ihre Aufgaben könnten auch die Gewährung des Zugangs zu Daten umfassen, sofern ihnen hierzu auf der Grundlage des sektoralen Unionsrechts oder des nationalen Rechts der Auftrag erteilt wurde. Diese zuständigen Stellen sollten öffentliche Stellen mit moderner Technik unterstützen, etwa Technik zur optimalen Strukturierung und Speicherung der Daten, damit die Daten – insbesondere über Anwendungsprogrammierschnittstellen – leicht zugänglich, interoperabel, übertragbar und durchsuchbar werden, wobei bewährte Verfahren für die Datenverarbeitung sowie bestehende Regulierungs- und Technikstandards und sichere Datenverarbeitungsumgebungen zu berücksichtigen sind, die es ermöglichen, Daten unter Wahrung des Datenschutzes und der Privatsphäre zu analysieren.

Die zuständigen Stellen sollten aufgrund von Anweisungen der öffentlichen Stellen tätig werden. Solche Unterstützungsstrukturen könnten die betroffenen Personen und die Dateninhaber beim Einwilligungsmanagement oder Erlaubnismanagement für die Weiterverwendung unterstützen, wenn beispielsweise für bestimmte Bereiche der wissenschaftlichen Forschung die Einwilligung und Erlaubnis unter der Voraussetzung gegeben wird, dass anerkannte Standards der Ethik für die wissenschaftliche Forschung eingehalten werden. Die zuständigen Stellen sollten keine Aufsichtsfunktion haben, die gemäß der Verordnung (EU) 2016/679 Aufsichtsbehörden vorbehalten ist. Unbeschadet der Aufsichtsbefugnisse der Datenschutzbehörden sollte die Datenverarbeitung unter der Verantwortung der für das Datenregister zuständigen öffentlichen Stelle erfolgen, bei der es sich auch weiterhin und sofern es personenbezogene Daten betrifft, um einen Datenverantwortlichen im Sinne der Verordnung (EU) 2016/679 handelt. Die Mitgliedstaaten sollten eine oder mehrere zuständige Stellen benennen können, die für verschiedene Sektoren zuständig sind. Unter Umständen könnten die internen Dienste öffentlicher Stellen auch als zuständige Stellen fungieren. Eine zuständige Stelle könnte eine öffentliche Stelle sein, die gegebenenfalls andere öffentliche Stellen bei der Erteilung der Erlaubnis zur Weiterverwendung unterstützt, oder eine öffentliche Stelle, die die Weiterverwendung selbst erlaubt. Zur Unterstützung anderer öffentlicher Stellen sollte auch gehören, sie auf Anfrage über bewährte Verfahren zur Erfüllung der Anforderungen dieser Verordnung zu informieren, also etwa in Bezug auf die technischen Mittel zur Schaffung einer sicheren Verarbeitungsumgebung oder zur Gewährleistung der Privatsphäre und der Vertraulichkeit, wenn der Zugang zur Weiterverwendung von Daten im Rahmen des Anwendungsbereichs dieser Verordnung gewährt wird.

- (27) Datenvermittlungsdienste dürften eine Schlüsselrolle in der Datenwirtschaft spielen, insbesondere durch die Unterstützung und Förderung freiwilliger Verfahren zur gemeinsamen Datennutzung zwischen Unternehmen oder die Erleichterung zur gemeinsamen Datennutzung im Zusammenhang mit den im Unionsrecht oder im nationalen Recht festgelegten Verpflichtungen –. Sie könnten zu Akteuren werden, die den Austausch erheblicher Mengen einschlägiger Daten erleichtern. Anbieter von Datenvermittlungsdiensten, bei denen es sich auch um öffentliche Stellen handeln kann und die Dienste anbieten, die die verschiedenen Akteure miteinander verbinden, können zur effizienten Bündelung von Daten sowie zur Erleichterung des bilateralen Datenaustauschs beitragen. Spezialisierte Datenvermittlungsdienste, die von betroffenen Personen, Dateninhabern und Datennutzern unabhängig sind, könnten bei der Entstehung neuer, von Akteuren mit beträchtlicher Marktmacht unabhängiger datengetriebener Ökosysteme eine unterstützende Rolle spielen und dabei Unternehmen aller Größenordnungen – insbesondere KMU und Start-up-Unternehmen mit eingeschränkten finanziellen, rechtlichen oder administrativen Möglichkeiten – einen nichtdiskriminierenden Zugang zur Datenwirtschaft ermöglichen. Dies wird insbesondere im Zusammenhang mit der Schaffung gemeinsamer europäischer Datenräume, also zweck- oder sektorspezifischer oder auch sektorübergreifender interoperabler Rahmen mit gemeinsamen Normen und Praktiken für die gemeinsame Nutzung oder Verarbeitung von Daten – unter anderem zur Entwicklung neuer Produkte und Dienste, für die wissenschaftliche Forschung oder für Initiativen der Zivilgesellschaft – von Bedeutung sein. Zu den Datenvermittlungsdiensten könnten auch die zwei- oder mehrseitige gemeinsame Datennutzung oder die Einrichtung von Plattformen oder Datenbanken zur gemeinsamen Datennutzung oder -verwendung sowie die Einrichtung einer speziellen Infrastruktur für die Vernetzung von betroffenen Personen, Dateninhabern und Datennutzern gehören.

- (28) Diese Verordnung sollte für Dienste gelten, deren Ziel darin besteht, mit technischen, rechtlichen oder sonstigen Mitteln geschäftliche Beziehungen zur gemeinsamen Datennutzung, auch zur Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern auf der einen und Datennutzern auf der anderen Seite herzustellen. Bieten Unternehmen oder sonstige Stellen eine Vielzahl von datenbezogenen Diensten an, so sollten nur diejenigen Tätigkeiten, die unmittelbar die Bereitstellung von Datenvermittlungsdiensten betreffen, unter diese Verordnung fallen. Die Bereitstellung von Cloud-Speicher, Analysediensten, Software zur gemeinsamen Datennutzung, von Internetbrowsern oder Browser-Plug-ins oder von E-Mail-Diensten sollte nicht als Datenvermittlungsdienst im Sinne dieser Verordnung gelten, sofern mit diesen Diensten betroffenen Personen oder Dateninhabern ausschließlich technische Werkzeuge zur gemeinsamen Datennutzung mit anderen bereitgestellt werden, die Bereitstellung dieser Werkzeuge aber weder darauf abzielt, zwischen Dateninhabern und Datennutzern eine geschäftliche Beziehung herzustellen, noch dem Anbieter von Datenvermittlungsdiensten ermöglicht, Informationen über die Herstellung geschäftlicher Beziehungen zum Zwecke der gemeinsamen Datennutzung zu erlangen. Beispiele für Datenvermittlungsdienste schließen Datenmarktplätze ein, auf denen Unternehmen anderen Daten zugänglich machen könnten, Orchestrierer von Ökosystemen zur gemeinsamen Datennutzung, die allen Interessierten, etwa im Zusammenhang mit gemeinsamen europäischen Datenräumen, offen stehen, sowie Datenbestände, die von mehreren natürlichen oder juristischen Personen gemeinsam erstellt werden, um dann allen Interessierten Lizenzen für die Nutzung dieser Datenbestände zu erteilen, die so gestaltet sind, dass alle beitragenden Teilnehmer eine Gegenleistung für ihren Beitrag erhalten würden.

Dies würde Dienste ausschließen, die Daten von Dateninhabern einholen und aggregieren, anreichern oder umwandeln, um deren Wert erheblich zu steigern, und Lizenzen für die Nutzung der sich daraus ergebenden Daten an die Datennutzer vergeben, ohne eine geschäftliche Beziehung zwischen Dateninhabern und Datennutzern herzustellen. Dies würde auch Dienste ausschließen, die ausschließlich von einem Dateninhaber genutzt werden, um die Verwendung von den im Besitz dieses Dateninhabers befindlichen Daten zu ermöglichen, oder die von mehreren juristischen Personen in einer geschlossenen Gruppe, auch im Rahmen von Lieferanten- oder Kundenbeziehungen oder vertraglich festgelegten Formen der Zusammenarbeit, genutzt werden, insbesondere wenn deren Hauptziel darin besteht, die Funktionen von mit dem Internet der Dinge verbundenen Objekten und Geräten sicherzustellen.

- (29) Dienste, die auf die Vermittlung urheberrechtlich geschützter Inhalte ausgerichtet sind, beispielsweise Diensteanbieter für das Teilen von Online-Inhalten gemäß der Definition in Artikel 2 Nummer 6 der Richtlinie (EU) 2019/790, sollten nicht unter diese Verordnung fallen. „Bereitsteller konsolidierter Datenträger“ im Sinne von Artikel 2 Absatz 1 Nummer 35 der Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates <sup>(27)</sup> und „Kontoinformationsdienstleister“ im Sinne von Artikel 4 Nummer 19 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates <sup>(28)</sup> sollten für die Zwecke dieser Verordnung nicht als Anbieter von Datenvermittlungsdiensten gelten. Diese Verordnung sollte nicht für Dienste gelten, die von öffentlichen Stellen angeboten werden, um die Weiterverwendung entweder von geschützten Daten im Besitz von öffentlicher Stellen im Einklang mit dieser Verordnung oder die Verwendung jeglicher anderer Daten zu ermöglichen, sofern diese Dienste nicht darauf abzielen, Geschäftsbeziehungen herzustellen. Die in dieser Verordnung geregelten datenaltruistischen Organisationen sollten nicht als Anbieter von Datenvermittlungsdiensten gelten, sofern diese Dienste keine Geschäftsbeziehungen zwischen potenziellen Datennutzern einerseits und betroffenen Personen und Dateninhabern, die Daten für altruistische Zwecke zugänglich machen, andererseits herstellen. Sonstige Dienste, mit denen keine Geschäftsbeziehungen hergestellt werden sollen, wie Archive zur Ermöglichung der Weiterverwendung von wissenschaftlichen Forschungsdaten im Einklang mit den Grundsätzen des offenen Zugangs, sollten nicht als Datenvermittlungsdienste im Sinne der vorliegenden Verordnung gelten.

- (30) Zu einer besonderen Kategorie von Datenvermittlungsdiensten gehören Anbieter von Diensten, die ihre Dienste betroffenen Personen anbieten. Diese Anbieter von Datenvermittlungsdiensten wollen die Handlungsfähigkeit betroffener Personen und insbesondere die Kontrolle von Einzelpersonen in Bezug auf die ihn betreffenden Daten verbessern. Diese Anbieter unterstützen Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679, insbesondere in Bezug auf die Erteilung oder den Widerruf 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 Datenverarbeitung Verantwortlichen auf einen anderen zu übertragen. In diesem Zusammenhang ist es wichtig, dass das Geschäftsmodell dieser Anbieter sicherstellt, dass keine falschen Anreize bestehen, die Einzelpersonen dazu bewegen, solche Dienste in Anspruch zu nehmen, um mehr sie betreffende Daten für die Verarbeitung zur Verfügung zu stellen, als im Interesse der Einzelpersonen liegt. Dies könnte die Beratung von Einzelpersonen über die mögliche 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 „persönlichen Datenraum“ zusammenzustellen,

<sup>(27)</sup> Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABL L 173 vom 12.6.2014, S. 84).

<sup>(28)</sup> 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).

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. Solche „persönlichen Datenräume“ könnten statische personenbezogene Daten wie Name, Anschrift oder Geburtsdatum sowie dynamische Daten enthalten, die von Einzelpersonen zum Beispiel bei der Nutzung eines Online-Dienstes oder eines mit dem Internet der Dinge verbundenen Objekts generiert werden. Sie könnten auch zur Speicherung von geprüften Identitätsangaben, wie Reisepassnummer oder Sozialversicherungsdaten, sowie als Berechtigungsnachweise wie Führerscheine, Diplome oder Bankkontodaten verwendet werden.

- (31) Datengenossenschaften sind bestrebt, eine Reihe von Zielen zu erreichen, insbesondere die Position von Einzelpersonen bei der sachkundigen Entscheidung vor der Einwilligung zur Datennutzung zu stärken, die Geschäftsbedingungen von Datennutzerorganisationen im Zusammenhang mit der Datennutzung in einer Weise zu beeinflussen, die den einzelnen Mitgliedern der Gruppe bessere Wahlmöglichkeiten bietet, oder mögliche Lösungen zu ermitteln, wenn einzelne Mitglieder einer Gruppe unterschiedliche Standpunkte zu der Frage vertreten, 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 persönliche Rechte der betroffenen Personen sind und dass die betroffenen Personen nicht auf diese Rechte verzichten können. Datengenossenschaften könnten auch ein nützliches Instrument für Ein-Personen-Unternehmen und KMU darstellen, die in Bezug auf das Wissen über die Weitergabe von Daten häufig mit Einzelpersonen vergleichbar sind.
- (32) Um das Vertrauen in diese Datenvermittlungsdienste zu stärken, insbesondere in Bezug auf die Nutzung von Daten und die Einhaltung der von den betroffenen Personen und den Dateninhabern auferlegten Bedingungen, ist es erforderlich, einen Rechtsrahmen auf Unionsebene zu schaffen, in dem stark harmonisierte Anforderungen an die vertrauenswürdige Erbringung solcher Datenvermittlungsdienste festgelegt werden und der von den zuständigen nationalen Behörden umgesetzt wird. Dieser Rahmen wird dazu beitragen, dass betroffene Personen und Dateninhaber sowie Datennutzer eine bessere Kontrolle über den Zugang zu ihren Daten und deren Nutzung im Einklang mit dem Unionsrecht haben. Die Kommission könnte auch darauf hinwirken und den Weg dafür bereiten, dass auf Unionsebene unter Einbeziehung der einschlägigen Interessenträger Verhaltenskodizes, insbesondere zur Interoperabilität, entwickelt werden. Sowohl bei der Datenweitergabe zwischen Unternehmen als auch zwischen Unternehmen und Verbrauchern sollten die Anbieter von Datenvermittlungsdiensten 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 Datenvermittlungsdiensten könnten auch eine spezifische technische Infrastruktur für die Vernetzung von betroffenen Personen und Dateninhabern mit Datennutzern bereitstellen. In diesem Zusammenhang ist es von besonderer Bedeutung, diese Infrastruktur so zu gestalten, dass KMU und Start-up-Unternehmen nicht auf technische oder sonstige Hindernisse stoßen, wenn sie an der Datenwirtschaft teilnehmen wollen.

Datenvermittlungsdienste sollten Dateninhabern oder betroffenen Personen insbesondere zur Erleichterung des Datenaustauschs, z. B. durch vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung anbieten dürfen. Diese Werkzeuge und Dienste sollten jedoch nur auf ausdrücklichen Antrag oder mit der Zustimmung des Dateninhabers oder der betroffenen Person verwendet werden; und in diesem Zusammenhang angebotene Werkzeuge Dritter sollten Daten zu keinen anderen Zwecken verwenden. Gleichzeitig sollten Anbieter von Datenvermittlungsdiensten die ausgetauschten Daten anpassen dürfen, um auf Wunsch des Datennutzers deren Nutzbarkeit für den Datennutzer zu verbessern oder die Interoperabilität, beispielsweise zur Konvertierung der Daten in bestimmte Formate zu verbessern.

- (33) Es ist wichtig, dass ein durch Wettbewerb geprägtes Umfeld für die gemeinsame Datennutzung ermöglicht wird. Ein Schlüsselement zur Verbesserung des Vertrauens in die Datenvermittlungsdienste und zur Stärkung der Kontrolle über diese Dienste durch die Dateninhaber, betroffenen Personen und Datennutzer ist die Neutralität der Anbieter der Datenvermittlungsdienste in Bezug auf die zwischen Dateninhabern oder betroffenen Personen und Datennutzern weitergegebenen Daten. Es ist daher notwendig, dass Anbieter von Datenvermittlungsdiensten bei den Transaktionen lediglich als Mittler tätig werden und die weitergegebenen Daten nicht für andere Zwecke verwenden. Die kommerziellen Bedingungen, einschließlich der Preisgestaltung, für die Bereitstellung der Datenvermittlungsdienste sollten nicht davon abhängig sein, ob ein potenzieller Dateninhaber oder Datennutzer andere Dienstleistungen, wie etwa Speicherdienste, Datenanalytik, künstliche Intelligenz oder sonstige datenbasierte Anwendungen, die von demselben Anbieter von Datenvermittlungsdiensten oder von einer mit ihm verbundenen Einrichtung angeboten werden, in Anspruch nimmt, und wenn dies der Fall ist, in welchem Umfang der Dateninhaber oder Datennutzer diese anderen Dienste nutzt. Dies erfordert auch eine strukturelle Trennung des Datenvermittlungsdienstes von allen anderen erbrachten Diensten, um Interessenkonflikte zu vermeiden. Dies bedeutet, dass der Datenvermittlungsdienst von einer juristischen Person erbracht werden sollte, die von den anderen Tätigkeiten dieses Anbieters von Datenvermittlungsdiensten getrennt ist. Jedoch sollten die Anbieter von Datenvermittlungsdiensten die von den Dateninhabern bereitgestellten Daten zur Verbesserung ihrer Datenvermittlungsdienste verwenden können.

Auf ausdrücklichen Antrag oder mit der Zustimmung der betroffenen Person oder des Dateninhabers sollten Anbieter von Datenvermittlungsdiensten Dateninhabern, betroffenen Personen oder Datennutzern ihre Werkzeuge oder die Werkzeuge Dritter zur Verfügung stellen können, um die Datenweitergabe, etwa durch Werkzeuge zur Konvertierung oder Pflege von Daten, zu erleichtern. Mit den in diesem Zusammenhang zur Verfügung gestellten

Werkzeugen Dritter sollten Daten ausschließlich zu mit den Datenvermittlungsdiensten verbundenen Zwecken verwendet werden. Anbieter von Datenvermittlungsdiensten, die die Datenweitergabe zwischen Einzelpersonen als betroffenen Personen und juristischen Personen als Datennutzer vermitteln, sollten darüber hinaus treuhänderische Pflichten gegenüber den Einzelpersonen haben, damit sichergestellt ist, dass sie im besten Interesse der betroffenen Personen handeln. Haftungsfragen in Bezug auf alle materiellen und immateriellen Schäden und Nachteile infolge eines Verhaltens des Anbieters von Datenvermittlungsdiensten könnten in den entsprechenden Verträgen auf der Grundlage der nationalen Haftungsregelungen geregelt werden.

- (34) Damit der Binnenmarkt reibungslos funktionieren kann, sollten Anbieter von Datenvermittlungsdiensten angemessene Maßnahmen ergreifen, um die Interoperabilität innerhalb eines Sektors und zwischen verschiedenen Sektoren sicherzustellen. Zu diesen angemessenen Maßnahmen könnte gehören, dass die bestehenden, allgemein verwendeten Standards des Sektors, in dem der Anbieter von Datenvermittlungsdiensten tätig ist, eingehalten werden. Der Europäische Dateninnovationsrat sollte gegebenenfalls der Einführung zusätzlicher Industriestandards den Weg ebnen. Anbieter von Datenvermittlungsdiensten sollten die vom Europäischen Dateninnovationsrat festgelegten Maßnahmen für die Interoperabilität zwischen Datenvermittlungsdiensten rechtzeitig umsetzen.
- (35) Die vorliegende Verordnung sollte die Verpflichtung der Anbieter von Datenvermittlungsdiensten zur Einhaltung der Verordnung (EU) 2016/679 und die Verantwortung der Aufsichtsbehörden, die Einhaltung dieser Verordnung sicherzustellen, unberührt lassen. Verarbeiten Anbieter von Datenvermittlungsdiensten personenbezogene Daten, so sollte diese Verordnung nicht den Schutz personenbezogener Daten berühren. Handelt es sich bei den Anbietern von Datenvermittlungsdiensten um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter im Sinne der Verordnung (EU) 2016/679, so sind sie an die Bestimmungen der genannten Verordnung gebunden.
- (36) Von Anbietern von Datenvermittlungsdiensten wird erwartet, dass sie über Verfahren und Maßnahmen verfügen, um Sanktionen bei betrügerischen oder missbräuchlichen Praktiken in Bezug auf Parteien, die über ihre Datenvermittlungsdienste Zugang zu erlangen versuchen, zu verhängen, unter anderem durch Maßnahmen wie den Ausschluss von Datennutzern, die gegen die Geschäftsbedingungen oder geltendes Recht verstoßen.
- (37) Die Anbieter von Datenvermittlungsdiensten sollten auch Maßnahmen ergreifen, um die Einhaltung des Wettbewerbsrechts sicherzustellen, und über entsprechende Verfahren verfügen. Dies gilt insbesondere dann, wenn die gemeinsame Datennutzung es den Unternehmen ermöglicht, Kenntnis der Marktstrategien ihrer tatsächlichen oder potenziellen Wettbewerber zu erlangen. Zu den sensiblen wettbewerbsrelevanten Informationen gehören in der Regel Informationen über Kunden, künftige Preise, Produktionskosten, Mengen, Umsätze, Verkäufe oder Kapazitäten.
- (38) Es sollte ein Anmeldeverfahren für Datenvermittlungsdienste eingeführt werden, damit sichergestellt ist, dass die Daten-Governance auf der Grundlage einer vertrauenswürdigen Datenweitergabe in der Union erfolgt. Die Vorteile eines vertrauenswürdigen Umfelds ließen sich am besten dadurch erreichen, dass eine Reihe von Anforderungen an die Erbringung von Datenvermittlungsdiensten geknüpft würde, ohne dass jedoch eine ausdrückliche Entscheidung oder ein Verwaltungsakt der zuständigen Behörde für die Erbringung solcher Datenvermittlungsdienste erforderlich wäre. Durch das Anmeldeverfahren sollten keine unnötigen Hindernisse für KMU, Start-up-Unternehmen und Organisationen der Zivilgesellschaft entstehen, und es sollte dem Grundsatz der Nichtdiskriminierung folgen.
- (39) Um eine wirksame grenzüberschreitende Erbringung von Dienstleistungen zu unterstützen, sollte der Anbieter von Datenvermittlungsdiensten aufgefordert werden, eine Anmeldung nur an die für Datenvermittlungsdienste 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 Angabe der in dieser Verordnung genannten Informationen ergänzt werden. Nach der entsprechenden Anmeldung sollte der Anbieter von Datenvermittlungsdiensten in der Lage sein, den Betrieb ohne weitere Anmeldepflichten in jedem Mitgliedstaat aufzunehmen.
- (40) Das in dieser Verordnung festgelegte Anmeldeverfahren sollte spezifische zusätzliche Vorschriften für die Erbringung von Datenvermittlungsdiensten, die aufgrund sektorspezifischer Rechtsvorschriften gelten, unberührt lassen.
- (41) Die Hauptniederlassung eines Anbieters von Datenvermittlungsdiensten in der Union sollte seine Hauptverwaltung in der Union sein. Zur Bestimmung der Hauptniederlassung eines Anbieters von Datenvermittlungsdiensten in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Verwaltungstätigkeiten sein. Die Tätigkeiten eines Anbieters von Datenvermittlungsdiensten sollten gemäß dem nationalen Recht des Mitgliedstaats erfolgen, in dem sich seine Hauptniederlassung befindet.

- (42) Um zu gewährleisten, dass die Anbieter von Datenvermittlungsdiensten diese Verordnung einhalten, sollten sie ihre Hauptniederlassung in der Union haben. Bietet ein Anbieter von Datenvermittlungsdiensten, der keine Niederlassung in der Union hat, Dienste in der Union an, so sollte er stattdessen einen gesetzlichen Vertreter benennen. Die Benennung eines gesetzlichen Vertreters ist in solchen Fällen notwendig, da solche Anbieter von Datenvermittlungsdiensten personenbezogene Daten sowie vertrauliche Geschäftsdaten verarbeiten, weshalb die Einhaltung dieser Verordnung durch die Anbieter von Datenvermittlungsdiensten eng überwacht werden muss. Um festzustellen, ob ein solcher Anbieter von Datenvermittlungsdiensten in der Union Dienste anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Datenvermittlungsdienste anzubieten. Die bloße Zugänglichkeit der Website oder einer E-Mail-Adresse und anderer Kontaktdaten des Anbieters von Datenvermittlungsdiensten in der Union oder die Verwendung einer Sprache, die in dem Drittland, in dem der Anbieter von Datenvermittlungsdiensten niedergelassen ist, allgemein gebräuchlich ist, sollte hierfür kein ausreichender Anhaltspunkt sein. Jedoch könnten 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 Sprache zu bestellen, oder die Erwähnung von Nutzern in der Union darauf hindeuten, dass der Anbieter von Datenvermittlungsdiensten beabsichtigt, in der Union Dienste anzubieten.

Ein benannter gesetzlicher Vertreter sollte im Auftrag des Anbieters von Datenvermittlungsdiensten handeln, und es sollte der für die Anbieter von Datenvermittlungsdiensten zuständigen Behörden möglich sein, sich zusätzlich zu einem oder statt an einen Anbieter von Datenvermittlungsdiensten an den gesetzlichen Vertreter zu wenden, auch um im Falle eines Verstoßes ein Durchsetzungsverfahren einzuleiten, wenn ein nicht in der Union niedergelassener Anbieter von Datenvermittlungsdiensten die Vorschriften nicht einhält. Der Anbieter von Datenvermittlungsdiensten sollte den gesetzlichen Vertreter benennen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen in seinem Auftrag zu handeln.

- (43) Damit betroffene Personen und Dateninhaber in der Union anerkannte Anbieter von Datenvermittlungsdiensten ohne Weiteres erkennen können und dadurch ihr Vertrauen in in der Union anerkannte Anbieter von Datenvermittlungsdiensten wächst, sollte zusätzlich zu der Bezeichnung „in der Union anerkannter Anbieter von Datenvermittlungsdiensten“ ein in der gesamten Union wiedererkennbares, gemeinsames Logo eingeführt werden.
- (44) Die für Datenvermittlungsdienste zuständigen Behörden, die für die Überwachung der Einhaltung der Anforderungen dieser Verordnung durch die Anbieter von Datenvermittlungsdiensten benannt wurden, sollten auf der Grundlage ihrer Kapazitäten und ihres Fachwissens in Bezug auf den horizontalen oder sektoralen Datenaustausch ausgewählt werden. Sie sollten bei der Wahrnehmung ihrer Aufgaben von allen Anbietern von Datenvermittlungsdiensten unabhängig sowie transparent und unparteiisch sein. Die Mitgliedstaaten sollten der Kommission die Namen jener benannten, für Datenvermittlungsdienste zuständigen Behörden mitteilen. Die Befugnisse und Zuständigkeiten der benannten zuständigen Behörden sollten die Befugnisse der Datenschutzbehörden unberührt lassen. Insbesondere in Bezug auf Fragen, die eine Prüfung der Einhaltung der Verordnung (EU) 2016/679 erfordern, sollte die für Datenvermittlungsdienste zuständige Behörde gegebenenfalls um eine Stellungnahme oder einen Beschluss der gemäß der genannten Verordnung zuständigen Aufsichtsbehörde ersuchen.
- (45) Die Nutzung von Daten für Ziele von allgemeinem Interesse, die von betroffenen Personen auf der Grundlage ihrer sachkundigen Einwilligung freiwillig oder – wenn es sich um nicht personenbezogene Daten handelt – von Dateninhabern bereitgestellt werden, birgt ein großes Potenzial. Zu diesen Zielen gehören die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die bessere Erbringung öffentlicher Dienstleistungen oder bessere staatliche Entscheidungsfindung. Die Unterstützung der wissenschaftlichen Forschung sollte ebenfalls als Ziel von allgemeinem Interesse betrachtet werden. Ziel dieser Verordnung sollte es sein, zur Entstehung von ausreichend großen Datenbeständen beizutragen, die auf der Grundlage von Datenaltruismus bereitgestellt werden, um Datenanalysen und maschinelles Lernen auch grenzüberschreitend in der Union ermöglichen. Um dieses Ziel zu erreichen, sollten die Mitgliedstaaten organisatorische oder technische Vorkehrungen oder beides treffen können, mit denen der Datenaltruismus erleichtert würde. Zu solchen Vorkehrungen könnte gehören, dass betroffenen Personen oder Dateninhabern leicht verwendbare Werkzeuge zur Verfügung stehen, mit denen sie die Einwilligung oder Erlaubnis zur altruistischen Verwendung ihrer Daten erteilen können, dass Sensibilisierungskampagnen veranstaltet werden oder die zuständigen Behörden einen strukturierten Austausch dazu führen, wie staatliche Maßnahmen wie die Verbesserung des Verkehrs, der öffentlichen Gesundheit und der Bekämpfung des Klimawandels von Datenaltruismus profitieren können. Zu diesem Zweck sollten die Mitgliedstaaten auch nationale Strategien für Datenaltruismus festlegen können. Die betroffenen Personen sollten eine Entschädigung nur für diejenigen Kosten erhalten können, die ihnen durch die Bereitstellung ihrer Daten für Ziele von allgemeinem Interesse entstehen.
- (46) Es wird erwartet, dass die Eintragung anerkannter datenaltruistischer Organisationen und die Verwendung des Labels „in der Union anerkannte datenaltruistische Organisation“ zur Einrichtung von Datenarchiven führt. Die Eintragung in einem Mitgliedstaat wäre unionsweit gültig, und sollte die grenzüberschreitende Datennutzung innerhalb der Union und die Entstehung von Datenbeständen, die mehrere Mitgliedstaaten abdecken, erleichtern. Dateninhaber 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 Erfüllung der Anforderungen dieser

Verordnung durch diese eingetragenen Einrichtungen sollte für Vertrauen darin sorgen, dass die für altruistische Zwecke bereitgestellten Daten dem allgemeinen Interesse dienen. Dieses Vertrauen sollte sich insbesondere aus einem Niederlassungsort oder einem gesetzlichen Vertreter in der Union sowie aus der Anforderung ergeben, dass anerkannte datenaltruistische Organisationen keinen Erwerbszweck verfolgen, aus Transparenzanforderungen und aus spezifischen Vorkehrungen zum Schutz der Rechte und Interessen der betroffenen Personen und Unternehmen.

Weitere Schutzvorkehrungen sollten umfassen, dass einschlägige Daten in einer von anerkannten datenaltruistischen Organisationen betriebenen sicheren Verarbeitungsumgebung verarbeitet werden können, dass mithilfe von Aufsichtsmechanismen wie Ethikräten oder -gremien, einschließlich Vertretern der Zivilgesellschaft, sichergestellt wird, dass der für die Verarbeitung Verantwortliche hohe wissenschaftliche Ethikstandards und den Schutz der Grundrechte einhält, dass wirksame und klar kommunizierte technische Mittel vorhanden sind, um die Einwilligung auf der Grundlage der Informationspflichten des Auftragsverarbeiters 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. Die Eintragung als anerkannte datenaltruistische Organisation sollte keine Voraussetzung für die Ausübung datenaltruistischer Tätigkeiten sein. Die Kommission sollte im Wege delegierter Rechtsakte ein Regelwerk erstellen, das in enger Zusammenarbeit mit datenaltruistischen Organisationen und einschlägigen Interessenträgern erstellt wird. Die Einhaltung dieses Regelwerks sollte eine Voraussetzung für die Eintragung als anerkannte datenaltruistische Organisation sein.

- (47) Damit betroffene Personen und Dateninhaber anerkannte datenaltruistische Organisationen ohne Weiteres erkennen können und dadurch ihr Vertrauen in diese Anbieter wächst, sollte ein in der gesamten Union wiedererkennbares, gemeinsames Logo eingeführt werden. Das gemeinsame Logo sollte zusammen mit einem QR-Code mit Link zum öffentlichen Unionsregister der anerkannten datenaltruistischen Organisationen erscheinen.
- (48) Diese Verordnung sollte die Einrichtung, Organisation und Funktionsweise von Einrichtungen, die sich nach nationalem Recht dem Datenaltruismus verschreiben, unberührt lassen und sich auf die Anforderung stützen, dass die Tätigkeiten einer Organisation ohne Erwerbszweck in einem Mitgliedstaat nach nationalem Recht rechtmäßig sein müssen.
- (49) Diese Verordnung sollte die Einrichtung, Organisation und Funktionsweise von Einrichtungen, die keine öffentlichen Stellen sind und im Bereich der gemeinsamen Nutzung von Daten und Inhalten auf der Grundlage von freien Lizenzen tätig sind und damit zur Schaffung von gemeinsamen, für alle zugänglichen Ressourcen beitragen, unberührt lassen. Dazu sollten offene, kollaborative Plattformen zum Wissensaustausch, frei zugängliche wissenschaftliche und akademische Archive, Plattformen zur Entwicklung von Open-Source-Software und Aggregationsplattformen für Open-Access-Inhalte gehören.
- (50) Anerkannte datenaltruistische Organisationen sollten einschlägige Daten direkt bei natürlichen und juristischen Personen erheben oder von Dritten erhobene Daten verarbeiten können. Datenaltruistische Organisationen könnten die erhobenen Daten zu selbst festgelegten Zwecken verarbeiten oder könnten gegebenenfalls die Verarbeitung zu diesen Zwecken durch Dritte erlauben. Handelt es sich bei den anerkannten datenaltruistischen Organisationen um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter gemäß der Verordnung (EU) 2016/679, so sollten sie die genannte Verordnung einhalten. 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 der Verordnung (EU) 2016/679, die den Anforderungen an eine rechtmäßige Einwilligung gemäß den Artikeln 7 und 8 der genannten Verordnung entsprechen sollte. Gemäß der Verordnung (EU) 2016/679 könnten 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. Für nicht personenbezogene Daten sollten die Nutzungsbeschränkungen in der vom Dateninhaber erteilten Erlaubnis aufgeführt sein.
- (51) Die für die Registrierung datenaltruistischer Organisationen zuständigen Behörden, die benannt wurden, um die Einhaltung der Anforderungen dieser Verordnung durch anerkannte datenaltruistische Organisationen zu überwachen, sollten auf der Grundlage ihrer Kapazitäten und ihres Fachwissens ausgewählt werden. Sie sollten bei der Wahrnehmung ihrer Aufgaben von allen anerkannten datenaltruistischen Organisationen unabhängig sowie transparent und unparteiisch sein. Die Mitgliedstaaten sollten der Kommission die Namen dieser für die Registrierung datenaltruistischer Organisationen benannten zuständigen Behörden mitteilen. Die Befugnisse und Zuständigkeiten der für die Registrierung datenaltruistischer Organisationen benannten zuständigen Behörden sollten die Befugnisse der Datenschutzbehörden unberührt lassen. Insbesondere in Bezug auf Fragen, die eine Prüfung der Einhaltung der Verordnung (EU) 2016/679 erfordern, sollte die für die Registrierung datenaltruistischer Organisationen zuständige Behörde gegebenenfalls um eine Stellungnahme oder einen Beschluss der gemäß der genannten Verordnung zuständigen Aufsichtsbehörde ersuchen.

- (52) Um insbesondere im Zusammenhang mit Daten, die altruistisch für die wissenschaftliche Forschung und für statistische Zwecke zur Verfügung gestellt werden das Vertrauen in das Verfahren der Einwilligung und des Widerrufs zu fördern und für mehr Rechtssicherheit und Nutzerfreundlichkeit darin zu sorgen, 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 sollte auch die Erteilung und den Widerruf der Einwilligung erleichtern und 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 modular aufgebaut sein, damit es an bestimmte Sektoren und für verschiedene Zwecke angepasst werden kann.
- (53) Zur erfolgreichen Umsetzung des Rahmens für die Daten-Governance sollte ein Europäischer Dateninnovationsrat in Form einer Expertengruppe eingerichtet werden. Der Europäischer Dateninnovationsrat sollte sich aus Vertretern der für Datenvermittlungsdienste zuständigen Behörden sowie den für die Registrierung datenaltruistischer Organisationen aller Mitgliedstaaten, des Europäischen Datenschutzausschusses, des Europäischen Datenschutzbeauftragten, der Agentur der Europäischen Union für Cybersicherheit (ENISA), der Kommission, dem KMU-Beauftragten der EU oder einem vom Netz der KMU-Beauftragten benannten Vertreter und anderen Vertretern von maßgeblichen Stellen in bestimmten Sektoren und von Stellen mit spezifischen Fachkenntnissen zusammensetzen. Der Europäische Dateninnovationsrat sollte aus einer Reihe von Untergruppen bestehen, einschließlich einer Untergruppe für die Einbeziehung von Interessenträgern die sich aus einschlägigen Vertretern der Wirtschaft zusammensetzen, wie Gesundheit, Umwelt, Landwirtschaft, Verkehr, Energie, industrielle Fertigung, Medien, Kultur- und Kreativbranche und Statistik und gegebenenfalls Vertretern der Forschung, der Wissenschaft, der Zivilgesellschaft, von Normungsorganisationen, einschlägigen gemeinsamen europäischen Datenräumen und anderen einschlägigen Interessenträger und Dritten, gegebenenfalls von Stellen mit spezifischen Fachkenntnissen wie nationalen statistischen Ämtern.
- (54) Unter Berücksichtigung der Normungsarbeit in bestimmten Sektoren oder Bereichen sollte der Europäische Dateninnovationsrat 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 befolgt und europäische und internationale Normen und Spezifikationen, auch im Rahmen der Multi-Stakeholder-Plattform der EU für die IKT-Normung, sowie die Kernvokabulare und die CEF-Bausteine, nutzt. Die Arbeiten an der technischen Normung könnten 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 ermöglichen – insbesondere bei der Klärung, welche Normen und Praktiken sektorspezifisch und welche sektorübergreifend sind, sowie bei der diesbezüglichen Differenzierung. Der Europäische Dateninnovationsrat 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 Europäische Dateninnovationsrat die Kommission in Absprache mit dem Europäischen Datenschutzausschuss bei der Entwicklung des Einwilligungsformulars für Datenaltruismus unterstützen. Durch Unterbreitung von Leitlinien für gemeinsame europäische Datenräume sollte der Europäische Dateninnovationsrat die Entwicklung einer funktionierenden europäischen Datenwirtschaft auf der Grundlage dieser Datenräume, wie in der europäischen Datenstrategie dargelegt, unterstützen.
- (55) Die Mitgliedstaaten sollten Vorschriften über anzuwendende Sanktionen bei Verstößen gegen diese Verordnung festlegen und sollten alle Maßnahmen ergreifen, die sicherstellen, dass diese durchgeführt werden. Die Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein. Große Diskrepanzen zwischen den Vorschriften über Sanktionen könnten zur Verzerrung des Wettbewerbs im digitalen Binnenmarkt führen. Die Harmonisierung dieser Vorschriften könnte in dieser Hinsicht von Vorteil sein.
- (56) Um für eine wirksame Durchsetzung dieser Verordnung zu sorgen und sicherzustellen, dass Anbieter von Datenvermittlungsdiensten und Einrichtungen, die eine Eintragung als anerkannte datenaltruistische Organisation anstreben, vollständigen und grenzüberschreitenden Online-Zugang zu den Anmelde- und Eintragsverfahren haben und diese vollständig online abwickeln können, sollten diese Verfahren im Rahmen des einheitlichen digitalen Zugangstors angeboten werden, das gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates<sup>(29)</sup> eingerichtet wurde. Diese Verfahren sollten in die im Anhang II der Verordnung (EU) 2018/1724 enthaltene Liste der Verfahren aufgenommen werden.
- (57) Die Verordnung (EU) 2018/1724 sollte daher entsprechend geändert werden.

<sup>(29)</sup> Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (Abl. L 295 vom 21.11.2018, S. 1).

- (58) Um die Wirksamkeit dieser Verordnung sicherzustellen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um diese Verordnung zu ergänzen, indem in besonderen Gesetzgebungsakten der Union besondere Bedingungen für die Übertragung bestimmter als hochsensibel geltender Kategorien nicht personenbezogener Daten in Drittländer festgelegt werden und indem ein Regelwerk für anerkannte datenaltuistische Organisationen ausgearbeitet wird, das von diesen Organisationen einzuhalten ist, das informationsbezogene, technische und Sicherheitsanforderungen sowie Kommunikationsfahrpläne und Interoperabilitätsnormen enthält. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung<sup>(30)</sup> 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.
- (59) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse zur Unterstützung der öffentlichen Stellen und der Weiterverwender bei der Einhaltung der Bedingungen für die Weiterverwendung gemäß dieser Verordnung durch Bereitstellung von Mustervertragsklauseln für die Übertragung nicht personenbezogener Daten durch Weiterverwender in ein Drittland, zur Erklärung der der Rechts-, Aufsichts- und Durchsetzungsmechanismen eines Drittlands, die im Wesentlichen dem durch das Unionsrecht gewährleisteten Schutz gleichwertig sind, zur Ausgestaltung des gemeinsamen Logos für Anbieter von Datenvermittlungsdiensten und zur Ausgestaltung des gemeinsamen Logos datenaltuistischer Organisationen, sowie zur Entwicklung des europäischen Einwilligungssformulars für Datenaltuismus übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates<sup>(31)</sup> ausgeübt werden.
- (60) Diese Verordnung sollte die Anwendung der Wettbewerbsvorschriften, insbesondere der Artikel 101 und 102 AEUV unberührt lassen. Die in dieser Verordnung vorgesehenen Vorschriften dürfen nicht dazu verwendet werden, den Wettbewerb entgegen den Vorschriften des AEUV einzuschränken. Dies betrifft insbesondere die Vorschriften für den Austausch sensibler wettbewerbsrelevanter Informationen zwischen tatsächlichen oder potenziellen Wettbewerbern durch Datenvermittlungsdienste.
- (61) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und haben am 10. März 2021 ihre Stellungnahme abgegeben.
- (62) Leitprinzipien dieser Verordnung sind die Achtung der Grundrechte und die Wahrung der Grundsätze, die insbesondere in der Charta der Grundrechte der Europäischen Union anerkannt sind, darunter die Achtung der Privatsphäre, der Schutz personenbezogener Daten, die unternehmerische Freiheit, das Eigentumsrecht und die Integration von Menschen mit Behinderungen. Bezüglich Letzterer sollten die öffentlichen Stellen und Dienste gemäß dieser Verordnung gegebenenfalls die Richtlinien (EU) 2016/2102<sup>(32)</sup> und (EU) 2019/882<sup>(33)</sup> des Europäischen Parlaments und des Rates einhalten. Darüber hinaus sollte im Zusammenhang mit Informations- und Kommunikationstechnologie dem Konzept „Design für alle“ Rechnung getragen werden; dabei handelt es sich um bewusste und systematische Bemühungen um die Anwendung von Grundsätzen, Methoden und Werkzeugen zur Verbreitung eines universellen Designs bei computerbezogenen Technologien – auch bei internetbasierten Technologien –, mit dem nachträgliche Anpassungen oder spezielle Designs hinfällig werden.
- (63) Da die Ziele dieser Verordnung, nämlich die Weiterverwendung von Daten bestimmter Datenkategorien, die im Besitz öffentlicher Stellen sind, innerhalb der Union und die Schaffung eines ein Anmelde- und Aufsichtsrahmens für die Erbringung von Datenvermittlungsdiensten sowie eines Rahmens für die freiwillige Eintragung von Einrichtungen, die Daten für altruistische Zwecke zur Verfügung stellen und eines Rahmens für die Einsetzung eines Europäischen Dateninnovationsrats, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder wegen der Wirkungen auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzips tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus —

<sup>(30)</sup> ABl. L 123 vom 12.5.2016, S. 1.

<sup>(31)</sup> 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).

<sup>(32)</sup> Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen (ABl. L 327 vom 2.12.2016, S. 1).

<sup>(33)</sup> Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019, S. 70).

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 Datenvermittlungsdiensten;
- c) ein Rahmen für die freiwillige Eintragung von Einrichtungen, die für altruistische Zwecke zur Verfügung gestellte Daten erheben und verarbeiten und
- d) ein Rahmen für die Einsetzung eines Europäischen Dateninnovationsrats.

(2) Diese Verordnung begründet weder eine Verpflichtung für öffentliche Stellen, die Weiterverwendung von Daten zu erlauben, noch befreit sie öffentliche Stellen von ihren Geheimhaltungspflichten nach dem Unionsrecht oder dem nationalen Recht.

Von dieser Verordnung unberührt bleiben

- a) besondere Bestimmungen des Unionsrechts oder des nationalen Rechts über den Zugang zu bestimmten Kategorien von Daten oder deren Weiterverwendung, insbesondere in Bezug auf die Zugangsgewährung zu amtlichen Dokumenten und deren Offenlegung, und
- b) die nach dem Unionsrecht oder dem nationalen Recht geltenden Verpflichtungen öffentlicher Stellen, die Weiterverwendung von Daten zu erlauben, oder die Anforderungen in Bezug auf die Verarbeitung nicht personenbezogener Daten.

Müssen öffentliche Stellen, Anbieter von Datenvermittlungsdiensten oder anerkannte Einrichtungen, die Datenaltruismus-Dienste erbringen, aufgrund sektorspezifischen Unionsrechts oder nationalen Rechts bestimmte zusätzliche technische, administrative oder organisatorische Anforderungen einhalten, einschließlich durch Genehmigungs- oder Zertifizierungsverfahren, so finden auch diese Bestimmungen des sektorspezifischen Unionsrechts oder nationalen Rechts Anwendung. Etwaige spezifische zusätzliche Anforderungen müssen nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein.

(3) Das Unionsrecht und das nationale Recht über den Schutz personenbezogener Daten gelten für alle personenbezogenen Daten, die im Zusammenhang mit der vorliegenden Verordnung verarbeitet werden. Insbesondere gilt die vorliegende Verordnung unbeschadet der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinien 2002/58/EG und (EU) 2016/680, einschließlich im Hinblick auf die Befugnisse der Aufsichtsbehörden. Im Fall eines Konflikts zwischen der vorliegenden Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem entsprechend diesem Unionsrecht erlassenen nationalen Recht soll das einschlägige Unionsrecht bzw. das nationale Recht über den Schutz personenbezogener Daten Vorrang haben. Die vorliegende Verordnung schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, noch berührt es die in den Verordnungen (EU) 2016/679 oder (EU) 2018/1725 oder den Richtlinien 2002/58/EG oder (EU) 2016/680 festgelegten Rechte und Pflichten.

(4) Die Anwendung des Wettbewerbsrechts bleibt von dieser Verordnung unberührt.

(5) Diese Verordnung lässt die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit unberührt.

## 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. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;
4. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten sind;
5. „Einwilligung“ eine Einwilligung im Sinne des Artikels 4 Nummer 11 der Verordnung (EU) 2016/679;
6. „Erlaubnis“, dass Datennutzern das Recht auf Verarbeitung nicht personenbezogener Daten eingeräumt wird;
7. „betroffene Person“ eine betroffene Person im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;
8. „Dateninhaber“ eine juristische Person, einschließlich öffentlichen Stellen und internationalen Organisationen oder natürlichen Person, die in Bezug auf die betreffenden Daten keine betroffene Person ist, welche nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten personenbezogenen Daten oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben;
9. „Datennutzer“ eine natürliche oder juristische Person, die rechtmäßig Zugang zu bestimmten personenbezogenen oder nicht personenbezogenen Daten hat und im Fall personenbezogener Daten, unter anderem nach der Verordnung (EU) 2016/679, berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen;
10. „gemeinsame Datennutzung“ die entgeltliche oder unentgeltliche Bereitstellung von Daten durch eine betroffene Person oder einen Dateninhaber an einen Datennutzer für die gemeinschaftliche oder individuelle Nutzung dieser Daten auf der Grundlage freiwilliger Vereinbarungen, des Unionsrechts oder des nationalen Rechts, sowohl direkt als auch über einen Mittler, etwa im Rahmen von gebührenpflichtigen oder gebührenfreien offenen oder kommerziellen Lizenzen;
11. „Datenvermittlungsdienst“ einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen, und die zumindest folgendes nicht umfassen:
  - a) Dienste, in deren Rahmen Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden, um deren Wert erheblich zu steigern, und Lizenzen für die Nutzung der resultierenden Daten an die Datennutzer vergeben werden, ohne eine Geschäftsbeziehung zwischen Dateninhabern und Datennutzern herzustellen;
  - b) Dienste, deren Schwerpunkt auf der Vermittlung urheberrechtlich geschützter Inhalte liegt;
  - c) Dienste, die ausschließlich von einem Dateninhaber genutzt werden, um die Verwendung von im Besitz dieses Dateninhabers befindlichen Daten zu ermöglichen, oder die von mehreren juristischen Personen in einer geschlossenen Gruppe, einschließlich Lieferanten- oder Kundenbeziehungen oder vertraglich festgelegter Kooperationen, genutzt werden, insbesondere wenn deren Hauptziel darin besteht, Funktionen von Gegenständen und Geräten im Zusammenhang mit dem Internet der Dinge sicherzustellen;
  - d) Datenvermittlungsdienste, die von öffentlichen Stellen ohne die Absicht der Herstellung von Geschäftsbeziehungen angeboten werden;
12. „Verarbeitung“ die Verarbeitung im Sinne von Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 im Hinblick auf personenbezogene Daten oder Artikel 3 Nummer 2 der Verordnung (EU) 2018/1807 im Hinblick auf nicht personenbezogene Daten;
13. „Zugang“ die Datennutzung im Einklang mit bestimmten technischen, rechtlichen oder organisatorischen Anforderungen, ohne dass Daten hierzu zwingend übertragen oder heruntergeladen werden müssen;
14. „Hauptniederlassung“ einer juristischen Person den Ort, an dem sich ihre Hauptverwaltung in der Union befindet;

15. „Dienste von Datengenossenschaften“ Datenvermittlungsdienste, die von einer Organisationsstruktur angeboten werden, welche sich aus betroffenen Personen, Ein-Personen-Unternehmen oder KMU, die in dieser Struktur Mitglied sind, zusammensetzt, und deren Hauptzwecke in der Unterstützung ihrer Mitglieder bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten bestehen, unter anderem beim Treffen einer sachkundigen Entscheidung vor der Einwilligung zur Datenverarbeitung, beim Meinungsaustausch über die den Interessen ihrer Mitglieder im Zusammenhang mit ihren Daten am besten entsprechenden Zwecke und Bedingungen der Datenverarbeitung und beim Aushandeln der Bedingungen der Datenverarbeitung im Namen der Mitglieder, bevor die Erlaubnis zur Verarbeitung nicht personenbezogener Daten erteilt oder in die Verarbeitung personenbezogener Daten eingewilligt wird;
16. „Datenaltruismus“ die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse;
17. „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;
18. „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, unterstehen hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften oder Einrichtungen, oder 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;
19. „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;
20. „sichere Verarbeitungsumgebung“ die physische oder virtuelle Umgebung und die organisatorischen Mittel, mit denen die Einhaltung der Anforderungen des Unionsrechts, wie der Verordnung (EU) 2016/679, insbesondere im Hinblick auf die Rechte der betroffenen Personen, der Rechte des geistigen Eigentums und der geschäftlichen und statistischen Vertraulichkeit, der Integrität und der Verfügbarkeit, sowie des geltenden Unionsrechts und des nationalen Rechts gewährleistet wird und die es der Einrichtung, die die sichere Verarbeitungsumgebung bereitstellt, ermöglicht, alle Datenverarbeitungsvorgänge zu bestimmen und zu beaufsichtigen, darunter auch das Anzeigen, Speichern, Herunterladen und Exportieren von Daten und das Berechnen abgeleiteter Daten mithilfe von Rechenalgorithmen;
21. „gesetzlicher 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 Datenvermittlungsdiensten oder einer Einrichtung, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus für Ziele von allgemeinem Interesse zur Verfügung gestellte Daten erhebt, zu handeln, und an die sich die für die Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung datenaltruistischer Organisationen zuständigen Behörden hinsichtlich der Verpflichtungen nach dieser Verordnung ausschließlich oder zusätzlich zu den betreffenden Anbietern von Datenvermittlungsdiensten bzw. den betreffenden Einrichtungen, wenden auch um gegen einen nicht in der Union niedergelassenen Anbieter von Datenvermittlungsdiensten oder eine nicht in der Union niedergelassene Einrichtung, der bzw. die die Vorschriften nicht einhält, Durchsetzungsverfahren einzuleiten.

## 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, einschließlich Betriebsgeheimnissen, Berufsgeheimnissen, Unternehmensgeheimnissen;
- b) statistische Geheimhaltung,
- c) der Schutz geistigen Eigentums Dritter oder
- d) der Schutz personenbezogener Daten, soweit diese Daten nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024 fallen.

(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 im Besitz öffentlicher Stellen sind und aus Gründen der öffentlichen Sicherheit, der Landesverteidigung oder der nationalen Sicherheit geschützt sind, oder
- 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) Dieses Kapitel berührt nicht:

- a) Das Unionsrecht und das nationale Recht oder völkerrechtliche Übereinkünfte, denen die Union oder die Mitgliedstaaten beigetreten sind, in Bezug auf den Schutz der in Absatz 1 genannten Datenkategorien und
- b) das Unionsrecht und das nationale Recht über den Zugang zu Dokumenten.

## 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, die andernfalls nicht möglich gewesen wären.

(3) Ein ausschließliches Recht nach Absatz 2 wird durch einen Verwaltungsakt oder eine vertragliche Vereinbarung gemäß dem geltenden Unionsrecht oder dem nationalen Recht sowie im Einklang mit den Grundsätzen der Transparenz, der Gleichbehandlung und der Nichtdiskriminierung gewährt.

(4) Die Dauer des ausschließlichen Rechts auf Weiterverwendung von Daten darf 12 Monate nicht überschreiten. Wird ein Vertrag abgeschlossen, so ist dessen Dauer die gleiche wie die des ausschließlichen Rechts.

- (5) Die Gewährung eines ausschließlichen Rechts nach den Absätzen 2, 3 und 4, einschließlich der Begründung, warum die Gewährung eines solchen Rechts erforderlich ist, ist transparent und wird in einer Form, die dem einschlägigen Unionsrecht für die Vergabe öffentlicher Aufträge entspricht, im Internet öffentlich zugänglich gemacht.
- (6) Vereinbarungen oder andere Praktiken, die unter das in Absatz 1 genannte Verbot fallen und die in den Absätzen 2 und 3 festgelegten Bedingungen nicht erfüllen, die aber vor dem 23. Juni 2022 bereits bestanden haben, werden zum Ende des anwendbaren Vertrags, auf jeden Fall aber zum 24. Dezember 2024 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 und das Verfahren für die Beantragung einer solchen Weiterverwendung über die zentrale Informationsstelle nach Artikel 8 öffentlich zugänglich. Bei der Gewährung oder Verweigerung des Zugangs zur Weiterverwendung können sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

Die Mitgliedstaaten stellen sicher, dass die öffentlichen Stellen über die notwendigen Ressourcen verfügen und den vorliegenden Artikel einhalten.

(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, transparent, verhältnismäßig und objektiv gerechtfertigt sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen.

(3) Öffentliche Stellen sorgen gemäß dem Unionsrecht und dem nationalen Recht dafür, dass die Daten geschützt bleiben. Sie können folgende Anforderungen vorschreiben:

- a) Den Zugang zur Weiterverwendung von Daten nur zu gewähren, wenn die öffentliche Stelle oder die zuständige Stelle nach Eingang des Antrags auf Weiterverwendung sichergestellt hat, dass die Daten
  - i) im Falle personenbezogener Daten anonymisiert wurden und
  - ii) im Falle von vertraulichen Geschäftsinformationen, einschließlich Geschäftsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte, nach einer anderen Methode der Offenlegungskontrolle verändert, aggregiert oder aufbereitet wurden,
- b) der Zugang zu den Daten und deren Weiterverwendung erfolgt durch Fernzugriff in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten sicheren Verarbeitungsumgebung,
- c) der Zugang zu den Daten und deren Weiterverwendung erfolgt unter Einhaltung hoher Sicherheitsstandards innerhalb der physischen Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, sofern ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden.

(4) Die öffentlichen Stellen erlegen im Falle einer erlaubten Weiterverwendung gemäß Absatz 3 Buchstaben b und c Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird. Die öffentliche Stelle behält sich das Recht vor, das Verfahren, die Mittel und die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung zu überprüfen, um die Integrität des Datenschutzes zu wahren, und sie behält sich das Recht vor, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen Dritter gefährden. Die Entscheidung, die Verwendung der Ergebnisse zu verbieten, muss für den Weiterverwender verständlich und transparent sein.

(5) Sofern im nationalen Recht für die Weiterverwendung von Daten gemäß Artikel 3 Absatz 1 keine besonderen Schutzvorkehrungen bezüglich geltender Geheimhaltungspflichten vorgesehen sind, macht die öffentliche Stelle die Nutzung der gemäß Absatz 3 des vorliegenden Artikels bereitgestellten Daten davon abhängig, ob der Weiterverwender einer Geheimhaltungspflicht nachkommt, wonach ihm die Offenlegung von Informationen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, untersagt ist, wenn dadurch die Rechte und Interessen Dritter verletzt würden. Weiterverwendern ist es untersagt, betroffene Personen, auf die sich die Daten beziehen, erneut zu identifizieren, und sie ergreifen technische und operative Maßnahmen, um eine erneute Identifizierung zu verhindern und der öffentlichen Stelle etwaige Datenschutzverletzungen, die zu einer erneuten Identifizierung der betroffenen Personen führen könnten, mitzuteilen. Im Falle der unbefugten Weiterverwendung nicht personenbezogener Daten unterrichtet der Weiterverwender unverzüglich, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristischen Personen, deren Rechte und Interessen beeinträchtigt werden könnten.

(6) Kann die Weiterverwendung von Daten gemäß den in den Absätzen 3 und 4 des vorliegenden Artikels festgelegten Verpflichtungen nicht erlaubt werden und es keine andere Rechtsgrundlage für die Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, bemüht sich die öffentliche Stelle, gemäß dem Unionsrecht und dem nationalen Recht, nach besten Kräften, mögliche Weiterverwender dabei zu unterstützen, die Einwilligung der betroffenen Personen oder die Erlaubnis der Dateninhaber einzuholen, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, sofern dies ohne einen unverhältnismäßig hohen Aufwand für die öffentliche Stelle machbar ist. In den Fällen, in denen die öffentliche Stelle eine solche Unterstützung leistet, kann 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 den Bestimmungen des Unionsrechts oder des nationalen Rechts über die geschäftliche oder die statistische Geheimhaltung als vertraulich angesehen, so stellen die öffentlichen Stellen sicher, dass die vertraulichen Daten infolge der Erlaubnis einer solchen Weiterverwendung nicht offengelegt werden, es sei denn, die Weiterverwendung ist gemäß Absatz 6 zulässig.

(9) Beabsichtigt ein Weiterverwender nach Artikel 3 Absatz 1 geschützte nicht personenbezogene Daten in ein Drittland zu übertragen, so hat er die öffentliche Stelle zum Zeitpunkt der Beantragung der Weiterverwendung solcher Daten von seiner Absicht, solche Daten zu übertragen, und dem Zweck dieser Übertragung zu unterrichten. Im Falle einer Weiterverwendung gemäß Absatz 6 des vorliegenden Artikels unterrichtet der Weiterverwender, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristische Person, deren Rechte und Interessen beeinträchtigt werden können, über diese Absicht, den Zweck und die angemessenen Schutzvorkehrungen. Die öffentliche Stelle gestattet die Weiterverwendung nur, wenn die juristische Person die Erlaubnis für die Übertragung erteilt.

(10) Öffentliche Stellen übermitteln nicht personenbezogene vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten nur dann an einen Weiterverwender, der beabsichtigt, diese Daten in ein nicht gemäß Absatz 12 benanntes Drittland zu übertragen, wenn der Weiterverwender sich vertraglich dazu verpflichtet,

- a) die gemäß den Absätzen 7 und 8 auferlegten Verpflichtungen auch nach der Übertragung der Daten in das Drittland weiterhin zu erfüllen und
- b) die Zuständigkeit der Gerichte des Mitgliedstaats der übermittelnden öffentlichen Stelle für alle Streitigkeiten im Zusammenhang mit der Einhaltung der Absätze 7 und 8 anzuerkennen.

(11) Öffentliche Stellen bieten den Weiterverwendern gegebenenfalls und im Rahmen ihrer Möglichkeiten Beratung und Unterstützung, indem sie den in Absatz 10 des vorliegenden Artikels genannten Verpflichtungen nachkommen.

Zur Unterstützung der öffentlichen Stellen und der Weiterverwender kann die Kommission Durchführungsrechtsakte mit Mustervertragsklauseln für die Erfüllung der in Absatz 10 des vorliegenden Artikels genannten Verpflichtungen erlassen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 33 Absatz 3 genannten Prüfverfahren erlassen.

(12) Wenn dies aufgrund der Vielzahl unionsweit gestellter Anträge auf Weiterverwendung nicht personenbezogener Daten in bestimmten Drittländern gerechtfertigt ist, kann die Kommission 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 gemäß dem in Artikel 33 Absatz 3 genannten Prüfverfahren erlassen.

(13) Nach besonderen Gesetzgebungsakten der Union können bestimmte Kategorien nicht personenbezogener Daten, die im Besitz öffentlicher Stellen sind, für die Zwecke dieses Artikels als hochsensibel gelten, wenn die Übertragung dieser Daten in Drittländer Ziele des Gemeinwohls der Union, beispielsweise in den Bereichen Sicherheit und öffentliche Gesundheit, gefährden könnte oder die Gefahr einer erneuten Identifizierung anhand nicht personenbezogener, anonymisierter Daten birgt. Wird ein solcher Rechtsakt erlassen, so erlässt die Kommission gemäß Artikel 32 delegierte Rechtsakte zur Ergänzung dieser Verordnung durch Festlegung besonderer Bedingungen für die Übertragung dieser Daten in Drittländer.

Diese besonderen Bedingungen richten sich nach der Art der Kategorien der nicht personenbezogenen Daten, die in dem besonderen Gesetzgebungsakt der Union aufgeführt werden, und den Gründen, aus denen diese Kategorien als hochsensibel gelten, wobei sie die Risiken einer erneuten Identifizierung anhand anonymisierter Daten berücksichtigen. Sie sind nichtdiskriminierend und auf das erforderliche Maß zur Erreichung der in diesem Gesetzgebungsakt der Union festgelegten Ziele des Gemeinwohls der Union beschränkt; sie stehen im Einklang mit den internationalen Verpflichtungen der Union.

Wenn dies nach besonderen Gesetzgebungsakt der Union gemäß Unterabsatz 1 erforderlich ist, können diese besonderen Bedingungen 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.

(14) 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 10, 12 und 13 erfüllen.

#### 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) Gemäß Absatz 1 erhobene Gebühren müssen transparent, nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen den Wettbewerb nicht einschränken.

(3) Öffentliche Stellen müssen gewährleisten, dass alle Gebühren auch 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, so ergreifen sie Maßnahmen, um – gemäß den Vorschriften über staatliche Beihilfen – Anreize für die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu nichtkommerziellen Zwecken wie der wissenschaftlichen Forschung und durch KMU und Start-up-Unternehmen zu schaffen. In diesem Zusammenhang können öffentliche Stellen die Daten insbesondere KMU, Start-up-Unternehmen, der Zivilgesellschaft und Bildungseinrichtungen auch gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung stellen. Öffentliche Stellen können zu diesem Zweck eine Liste der Kategorien von Weiterverwendern aufstellen, denen Daten für die Weiterverwendung gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung gestellt werden. Diese Liste wird zusammen mit den Kriterien, die bei ihrer Aufstellung verwendet wurden, veröffentlicht.

(5) Gebühren werden aus den Kosten abgeleitet, die mit der Durchführung des Antragsverfahrens auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien verbunden sind, und auf die für das Folgende erforderlichen Kosten beschränkt:

- a) die Vervielfältigung, Bereitstellung und Verbreitung der Daten,
- b) die Freigabe der Urheberrechte,
- c) die Anonymisierung oder sonstigen Aufbereitung personenbezogener oder vertraulicher Geschäftsinformationen gemäß Artikel 5 Absatz 3,
- d) die Instandhaltung einer sicheren Verarbeitungsumgebung,
- e) der Erwerb des Rechts auf Erlaubnis der Weiterverwendung gemäß diesem Kapitel von Dritten außerhalb des öffentlichen Sektors und
- f) der Unterstützung von Weiterverwendern bei der Einholung der Einwilligung der betroffenen Personen und der Erlaubnis der Dateninhaber, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten.

(6) Die Kriterien und die Methode für die Gebührenberechnung werden von den Mitgliedstaaten festgelegt und veröffentlicht. Die öffentliche Stelle veröffentlicht eine Beschreibung der wichtigsten Kostenarten und die Regeln der Kostenzuweisung.

#### Artikel 7

##### Zuständige Stellen

(1) Für die Durchführung der in diesem Artikel genannten Aufgaben benennt jeder Mitgliedstaat eine oder mehrere zuständige Stellen, die für bestimmte Sektoren zuständig sein können, welche die öffentlichen Stellen, die Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien gewähren oder verweigern, unterstützen. Die Mitgliedstaaten können entweder eine oder mehrere neue zuständige Stellen einrichten oder sich auf bestehende öffentliche Stellen oder interne Dienste öffentlicher Stellen stützen, die die in dieser Verordnung festgelegten Bedingungen erfüllen.

(2) Die zuständigen Stellen können nach dem Unionsrecht oder dem nationalen Recht, wenn darin eine solche Zugangsgewährung vorgesehen ist, befugt werden, den Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu gewähren. In den Fällen, in denen sie den Zugang zur Weiterverwendung gewähren oder verweigern, finden die Artikel 4, 5, 6 und 9 auf diese zuständigen Stellen Anwendung.

(3) Die zuständigen Stellen müssen zur Erfüllung der ihnen übertragenen Aufgaben über angemessene rechtliche, finanzielle, technische und personelle Mittel, einschließlich der erforderlichen technischen 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.

(4) 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) Beratung und technische Unterstützung bei der bestmöglichen Strukturierung und Speicherung von Daten, um diese Daten leicht zugänglich zu machen;
- c) Leistung technischer Unterstützung bei der Pseudonymisierung und Sicherstellung, dass die Datenverarbeitung in einer Weise erfolgt, bei der die Privatsphäre, die Vertraulichkeit, die Integrität und die Zugänglichkeit in Bezug auf die Informationen in den Daten, deren Weiterverwendung erlaubt wird, effektiv gewahrt bleiben; dazu gehören auch Techniken zur Anonymisierung, Generalisierung, Unterdrückung und Randomisierung personenbezogener Daten oder andere dem Stand der Technik entsprechende Methoden zur Wahrung der Privatsphäre sowie die Löschung vertraulicher Geschäftsinformationen, wie Handelsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte;
- d) gegebenenfalls Unterstützung der öffentlichen Stellen, um Weiterverwender bei der Einholung der Einwilligung der betroffenen Personen zur Weiterverwendung oder der Erlaubnis der Dateninhaber entsprechend ihrer besonderen Festlegungen zu unterstützen, auch im Hinblick auf das Hoheitsgebiet, in dem die Datenverarbeitung stattfinden soll, und Unterstützung der öffentlichen Stellen bei der Einrichtung technischer Mechanismen, mit denen Einwilligungsanfragen oder die Erlaubnis der Weiterverwender übermittelt werden können, soweit dies praktikabel ist;
- e) Unterstützung öffentlicher Stellen bei der Beurteilung, ob die von einem Weiterverwender nach Artikel 5 Absatz 10 eingegangenen vertragliche Zusagen angemessen sind.

(5) Jeder Mitgliedstaat teilt der Kommission bis zum 24. September 2023 die Namen der nach Absatz 1 benannten zuständigen Stellen mit. Jeder Mitgliedstaat teilt der Kommission auch alle späteren Änderungen des Namens dieser benannten zuständigen Stellen mit.

#### Artikel 8

##### Zentrale Informationsstellen

(1) Die Mitgliedstaaten gewährleisten, dass alle einschlägigen Informationen in Bezug auf die Anwendung der Artikel 5 und 6 über eine zentrale Informationsstelle erhältlich und leicht zugänglich sind. Als Informationsstelle können die Mitgliedstaaten entweder eine neue Stelle oder Organisation einrichten oder eine vorhandene Stelle oder Organisation benennen. Die zentrale Informationsstelle kann mit sektoralen, regionalen oder lokalen Informationsstellen verknüpft sein. Die Funktionen der zentralen Informationsstelle können automatisiert werden, sofern die öffentliche Stelle für angemessene Unterstützung sorgt.

(2) Die zentrale Informationsstelle ist befugt, Anfragen oder Anträge in Bezug auf die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien entgegenzunehmen, und übermittelt diese – sofern möglich und angebracht durch automatisierte Verfahren – an die zuständigen öffentlichen Stellen oder gegebenenfalls an die in Artikel 7 Absatz 1 genannten zuständigen Stellen. Die zentrale Informationsstelle stellt auf elektronischem Wege eine durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Datenressourcen, gegebenenfalls einschließlich der bei sektoralen, regionalen oder lokalen Informationsstellen verfügbaren Datenressourcen, und einschlägige Informationen mit einer Beschreibung der verfügbaren Daten bereit, die mindestens das Datenformat und den Datenumfang und die Bedingungen für ihre Weiterverwendung umfasst.

(3) Die zentrale Informationsstelle kann einen gesonderten, vereinfachten und gut dokumentierten Informationskanal für KMU und Start-up-Unternehmen einrichten, der auf deren Bedarf und Kapazitäten mit Blick auf die Beantragung der Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien abstellt.

(4) Die Kommission richtet ein europaweites zentrales Zugangsportalein, über das ein durchsuchbares elektronisches Verzeichnis der bei den zentralen nationalen Informationsstellen verfügbaren Daten sowie weitere Informationen darüber bereitgestellt werden, wie über die zentralen nationalen Informationsstellen Daten angefordert werden können.

#### Artikel 9

### Verfahren für Anträge auf Weiterverwendung

(1) Sofern nicht gemäß dem nationalen Recht kürzeren Fristen festgelegt sind, treffen die zuständigen öffentlichen Stellen oder die in Artikel 7 Absatz 1 genannten zuständigen Stellen eine Entscheidung über den Antrag auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien innerhalb von zwei Monaten nach Eingang des Antrags.

Bei außergewöhnlich umfangreichen und komplexen Anträgen auf Weiterverwendung kann diese Frist von zwei Monaten um bis zu 30 Tage verlängert werden. In solchen Fällen teilen die zuständigen öffentlichen Stellen oder die in Artikel 7 Absatz 1 genannten zuständigen Stellen dem Antragsteller möglichst bald mit, dass für die Durchführung des Verfahrens mehr Zeit benötigt wird, zusammen mit den Gründen für die Verzögerung.

(2) Jede natürliche oder juristische Person, die von einer Entscheidung gemäß Absatz 1 direkt betroffen ist, hat in dem Mitgliedstaat, in dem die betreffende Stelle ihren Sitz hat, einen wirksamen Rechtsbehelfsanspruch. Dieser Rechtsbehelfsanspruch ist durch das nationale Recht geregelt und umfasst die Möglichkeit der Überprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis, wie die nationale Wettbewerbsbehörde, die für den Zugang zu Dokumenten zuständige Behörde, die gemäß der Verordnung (EU) 2016/679 errichtete Aufsichtsbehörde oder ein nationales Gericht, deren Entscheidungen für die betreffende öffentliche Stelle oder die zuständige Stelle bindend sind.

#### KAPITEL III

### Anforderungen an Datenvermittlungsdienste

#### Artikel 10

### Datenvermittlungsdienste

Die Erbringung der folgenden Datenvermittlungsdienste erfolgt gemäß Artikel 12 und unterliegt einem Anmeldeverfahren:

- a) Vermittlungsdienste zwischen Dateninhabern und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu diesen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen, sowie die Einrichtung anderer spezieller Infrastrukturen für die Vernetzung von Dateninhabern mit Datennutzern gehören;
- b) Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, oder natürlichen Personen, die nicht personenbezogene Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung dieser Dienste, sowie insbesondere Ermöglichung der Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte betroffener Personen;
- c) Dienste von Datengenossenschaften.

*Artikel 11***Anmeldung der Anbieter von Datenvermittlungsdiensten**

(1) Jeder Anbieter von Datenvermittlungsdiensten, der beabsichtigt, die in Artikel 10 genannten Datenvermittlungsdienste zu erbringen, muss sich bei der für Datenvermittlungsdienste zuständigen Behörde anmelden.

(2) Unbeschadet unionsrechtlicher Bestimmungen zur Regelung grenzübergreifender Schadenersatzklagen und damit zusammenhängender Verfahren gilt für die Zwecke dieser Verordnung, dass ein Anbieter von Datenvermittlungsdiensten, der in mehreren Mitgliedstaaten niedergelassen ist, der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem er seine Hauptniederlassung hat.

(3) Ein Anbieter von Datenvermittlungsdiensten, der nicht in der Union niedergelassen ist, aber die in Artikel 10 genannten Datenvermittlungsdienste in der Union anbietet, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in denen diese Dienste angeboten werden.

Um die Einhaltung dieser Verordnung sicherzustellen, beauftragt der Anbieter der Datenvermittlungsdienste den gesetzlichen Vertreter, neben ihm oder an seiner Stelle für Datenvermittlungsdienste zuständigen Behörden oder betroffenen Personen und Dateninhabern bei Fragen im Zusammenhang mit den erbrachten Datenvermittlungsdiensten als Anlaufstelle zu dienen. Der gesetzliche Vertreter arbeitet mit den für Datenvermittlungsdienste zuständigen Behörden zusammen und legt ihnen auf Verlangen umfassend dar, welche Maßnahmen und Vorkehrungen der Anbieter von Datenvermittlungsdiensten getroffen hat, um die Einhaltung dieser Verordnung sicherzustellen.

Es gilt, dass der Anbieter von Datenvermittlungsdiensten der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem sich der gesetzliche Vertreter befindet. Die Benennung eines gesetzlichen Vertreters durch den Anbieter von Datenvermittlungsdiensten erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Anbieter von Datenvermittlungsdiensten.

(4) Sobald er die Anmeldung vorgenommen hat, kann der Anbieter von Datenvermittlungsdiensten gemäß Absatz 1 die Tätigkeit unter den in diesem Kapitel festgelegten Bedingungen aufnehmen.

(5) Die in Absatz 1 genannte Anmeldung berechtigt den Anbieter von Datenvermittlungsdiensten zur Erbringung von Datenvermittlungsdiensten in allen Mitgliedstaaten.

(6) Die in Absatz 1 genannte Anmeldung muss folgende Angaben enthalten:

- a) den Namen des Anbieters von Datenvermittlungsdiensten,
- b) den Rechtsstatus, die Rechtsform, die Eigentümerstruktur, die relevanten Tochtergesellschaften und, sofern der Anbieter von Datenvermittlungsdiensten in einem Handelsregister oder einem anderen vergleichbaren öffentlichen nationalen Register eingetragen ist, die Registernummer des Anbieters von Datenvermittlungsdiensten,
- c) die Anschrift der Hauptniederlassung des Anbieters von Datenvermittlungsdiensten in der Union, falls zutreffend, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gesetzlichen Vertreters,
- d) eine öffentliche Website mit vollständigen und aktuellen Informationen über den Anbieter von Datenvermittlungsdiensten und seine Tätigkeiten, einschließlich mindestens der Informationen gemäß den Buchstaben a, b, c und f,
- e) die Kontaktpersonen und Kontaktangaben des Anbieters von Datenvermittlungsdiensten,
- f) eine Beschreibung des Datenvermittlungsdienstes, den der Anbieter von Datenvermittlungsdiensten zu erbringen beabsichtigt, und Angaben dazu, unter welche der in Artikel 10 genannten Kategorien dieser Datenvermittlungsdienst fällt,
- g) den voraussichtlichen Tag der Aufnahme der Tätigkeit, falls dies ein anderer als der Tag der Anmeldung ist.

(7) Die für Datenvermittlungsdienste zuständige Behörde stellt sicher, dass das Anmeldeverfahren nichtdiskriminierend ist und zu keinen Wettbewerbsverzerrungen führt.

(8) Auf Antrag des Anbieters von Datenvermittlungsdiensten gibt die für Datenvermittlungsdienste zuständige Behörde innerhalb einer Woche nach einer ordnungsgemäß und vollständig abgeschlossenen Anmeldung eine standardisierte Erklärung ab, in der sie bestätigt, dass der Anbieter von Datenvermittlungsdiensten die in Absatz 1 genannte Anmeldung vorgenommen hat und dass die Anmeldung die in Absatz 6 genannten Informationen enthält.

(9) Auf Antrag des Anbieters von Datenvermittlungsdiensten bestätigt die für Datenvermittlungsdienste zuständige Behörde, dass der Anbieter von Datenvermittlungsdiensten die Anforderungen dieses Artikels und des Artikels 12 erfüllt. Nach Erhalt einer solchen Bestätigung kann der Anbieter von Datenvermittlungsdiensten bei der schriftlichen und mündlichen Kommunikation den das Label „in der Union anerkannter Anbieter von Datenvermittlungsdiensten“ führen und ein gemeinsames Logo verwenden.

Damit in der Union anerkannte Anbieter von Datenvermittlungsdiensten in der gesamten Union leicht erkennbar sind, legt die Kommission im Wege von Durchführungsrechtsakten die Ausgestaltung eines gemeinsamen Logos fest. In der Union anerkannte Anbieter von Datenvermittlungsdiensten verwenden das gemeinsame Logo deutlich gut sichtbar auf jeder mit ihren Datenvermittlungsdiensten verbundenen Online- und Offline-Veröffentlichung.

Die Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

(10) Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede neue Anmeldung unverzüglich auf elektronischem Wege mit. Die Kommission führt ein Register aller Anbieter von Datenvermittlungsdiensten, die ihre Dienste in der Union erbringen, und aktualisiert dieses Register regelmäßig. Die Informationen gemäß Absatz 6 Buchstaben a, b, c, d, f und g werden in einem öffentlichen Register veröffentlicht.

(11) Die für Datenvermittlungsdienste zuständige Behörde kann nach Maßgabe des nationalen Rechts Gebühren für die Anmeldung erheben. Diese Gebühren sind verhältnismäßig und objektiv und beruhen auf den Verwaltungskosten, die durch die Überwachung der Einhaltung der Vorschriften und andere Marktkontrolltätigkeiten der für Datenvermittlungsdienste zuständigen Behörden in Bezug auf Anmeldungen von Anbietern von Datenvermittlungsdiensten entstehen. Im Falle von KMU und Start-up-Unternehmen kann die für Datenvermittlungsdienste zuständige Behörde eine ermäßigte Anmeldegebühr verlangen oder auf die Gebühr verzichten.

(12) Anbieter von Datenvermittlungsdiensten teilen der für Datenvermittlungsdienste zuständigen Behörde jede Änderung der gemäß Absatz 6 übermittelten Angaben innerhalb von 14 Tagen ab dem Tag der Änderung mit.

(13) Stellt ein Anbieter von Datenvermittlungsdiensten seine Tätigkeiten ein, so meldet er dies der nach den Absätzen 1, 2 und 3 bestimmten für Datenvermittlungsdienste zuständigen Behörde innerhalb von 15 Tagen.

(14) Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede der in den Absätzen 12 und 13 genannten Abmeldung unverzüglich auf elektronischem Wege mit. Die Kommission aktualisiert das öffentliche Register der Anbieter von Datenvermittlungsdiensten in der Union entsprechend.

## Artikel 12

### **Bedingungen für die Erbringung von Datenvermittlungsdiensten**

Die Erbringung von Datenvermittlungsdiensten nach Artikel 10 unterliegt folgenden Bedingungen:

- a) Der Anbieter von Datenvermittlungsdiensten verwendet die Daten, für die er Datenvermittlungsdienste erbringt, für keine anderen Zwecke, als sie den Datennutzern zur Verfügung zu stellen, und stellt die Datenvermittlungsdienste über eine gesonderte juristische Person bereit;
- b) die kommerziellen Bedingungen, einschließlich der Preisgestaltung, für die Erbringung von Datenvermittlungsdiensten für einen Dateninhaber oder Datennutzer sind nicht davon abhängig, ob der Dateninhaber oder Datennutzer andere Dienste desselben Anbieters von Datenvermittlungsdiensten oder eines verbundenen Unternehmens nutzt, und wenn dies der Fall ist, in welchem Umfang der Dateninhaber oder Datennutzer diese anderen Dienste nutzt;

- c) die Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zur Erbringung des Datenvermittlungsdienstes erhoben werden, einschließlich Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Datenvermittlungsdienst nutzenden Person hergestellt werden, werden nur für die Entwicklung dieses Datenvermittlungsdienstes verwendet, was die Nutzung von Daten für die Aufdeckung von Betrug oder im Interesse der Cybersicherheit umfassen kann, und sie sind den Dateninhabern auf Anfrage zur Verfügung zu stellen;
- d) der Anbieter von Datenvermittlungsdiensten ermöglicht den Austausch der Daten in dem Format, in dem er diese von einer betroffenen Person oder vom Dateninhaber erhält, wandelt die Daten nur in bestimmte Formate um, um die Interoperabilität innerhalb und zwischen Sektoren zu verbessern, oder wenn der Datennutzer dies verlangt, oder wenn das Unionsrecht dies vorschreibt oder wenn dies der Harmonisierung mit internationalen oder europäischen Datennormen dient und bietet betroffenen Personen oder Dateninhabern die Möglichkeit an, auf diese Umwandlungen zu verzichten („opt out“), sofern sie nicht durch das Unionsrecht vorgeschrieben sind;
- e) Datenvermittlungsdienste können ein Angebot zusätzlicher spezifischer Werkzeuge und Dienste für Dateninhaber oder betroffene Personen umfassen, insbesondere um den Datenaustausch zu erleichtern, z. B. vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung; diese Werkzeuge werden nur auf ausdrücklichen Antrag oder mit Zustimmung des Dateninhabers oder der betroffenen Person verwendet, und die in diesem Zusammenhang angebotenen Werkzeuge Dritter werden für keine anderen Zwecke verwendet;
- f) der Anbieter von Datenvermittlungsdiensten stellt sicher, dass das Verfahren für den Zugang zu seinem Dienst sowohl für betroffene Personen als auch für Dateninhaber sowie für Datennutzer – auch in Bezug auf die Preise und die Geschäftsbedingungen – fair, transparent und nichtdiskriminierend ist;
- g) der Anbieter von Datenvermittlungsdiensten verfügt über Verfahren, um betrügerische oder missbräuchliche Praktiken in Bezug auf Parteien zu verhindern, die über seine Datenvermittlungsdienste Zugang zu erlangen suchen;
- h) der Anbieter von Datenvermittlungsdiensten gewährleistet im Falle seiner Insolvenz eine angemessene Weiterführung der Erbringung seiner Datenvermittlungsdienste und richtet, sofern dieser Datenvermittlungsdienst die Speicherung von Daten sicherstellt, Mechanismen ein, die es Dateninhabern und Datennutzern ermöglichen, Zugang zu ihren Daten zu erhalten, diese zu übertragen oder abzurufen und im Fall der Erbringung von Datenvermittlungsdiensten zwischen betroffenen Personen und Datennutzern, ihre Rechte auszuüben;
- i) der Anbieter von Datenvermittlungsdiensten trifft geeignete Maßnahmen, um unter anderem mithilfe von allgemein verwendeten offenen Standards in dem Sektor, in dem der Anbieter von Datenvermittlungsdiensten tätig ist, die Interoperabilität mit anderen Datenvermittlungsdiensten zu gewährleisten;
- j) der Anbieter von Datenvermittlungsdiensten 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 oder des nationalen Rechts des jeweiligen Mitgliedstaats rechtswidrig sind;
- k) die Dateninhaber werden vom Anbieter von Datenvermittlungsdiensten im Falle einer unbefugten Übertragung, des unbefugten Zugriffs oder der unbefugten Nutzung der von ihm geteilten nicht personenbezogenen Daten unverzüglich unterrichtet;
- l) der Anbieter von Datenvermittlungsdiensten trifft die notwendigen Maßnahmen, um ein angemessenes Sicherheitsniveau bei der Speicherung, Verarbeitung und Übermittlung nicht personenbezogener Daten zu gewährleisten, und der Anbieter von Datenvermittlungsdiensten stellt ferner das höchste Sicherheitsniveau bei der Speicherung und Übermittlung sensibler wettbewerbsrelevanter Informationen sicher;
- m) der Anbieter von Datenvermittlungsdiensten, der Dienste für betroffene Personen anbietet, handelt bei der Erleichterung der Rechtausübung durch die betroffenen Personen im besten Interesse der betroffenen Personen; insbesondere informiert und –soweit erforderlich – berät er betroffene Personen in prägnanter, transparenter, verständlicher und leicht zugänglicher Weise über die beabsichtigte Nutzung der Daten durch Datennutzer und die üblichen Geschäftsbedingungen für solche Nutzungen, bevor die betroffenen Personen ihre Einwilligung erteilen;
- n) stellt ein Anbieter von Datenvermittlungsdiensten Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit, so gibt er gegebenenfalls das Hoheitsgebiet des Drittlandes an, in dem die Datennutzung stattfinden soll, und stellt den betroffenen Personen Werkzeuge zur Erteilung und zum Widerruf der Einwilligung sowie Dateninhabern Werkzeuge zur Erteilung und zum Widerruf der Erlaubnis zur Verarbeitung von Daten zur Verfügung;
- o) der Anbieter von Datenvermittlungsdiensten führt ein Protokoll über die Datenvermittlungstätigkeit.

### Artikel 13

#### Zuständige Behörden für Datenvermittlungsdienste

- (1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden für die Wahrnehmung der Aufgaben im Zusammenhang mit dem Anmeldeverfahren für Datenvermittlungsdienste, und teilt der Kommission bis zum 24. September 2023 die Namen dieser zuständigen Behörden mit. Jeder Mitgliedstaat teilt der Kommission auch alle späteren Änderungen der Namen dieser zuständigen Behörden mit.
- (2) Die für Datenvermittlungsdienste zuständigen Behörden müssen den Anforderungen des Artikels 26 genügen.
- (3) Die Befugnisse der für Datenvermittlungsdienste zuständigen Behörden lassen die Befugnisse der Datenschutzbehörden, der nationalen Wettbewerbsbehörden, der für Cybersicherheit zuständigen Behörden und anderer einschlägiger Fachbehörden unberührt. Nach Maßgabe ihrer jeweiligen Befugnisse im Rahmen des Unionsrechts und des nationalen Rechts begründen diese Behörden eine enge Zusammenarbeit, tauschen Informationen aus, die für die Wahrnehmung ihrer Aufgaben in Bezug auf Anbieter von Datenvermittlungsdiensten erforderlich sind, und bemühen sich darum, dass die Entscheidungen, die bei der Anwendung der Verordnung getroffen werden, konsistent sind.

### Artikel 14

#### Überwachung der Einhaltung

- (1) Die für Datenvermittlungsdienste zuständigen Behörden überwachen und beaufsichtigen die Einhaltung der Anforderungen dieses Kapitels durch die Anbieter von Datenvermittlungsdiensten. Auf Antrag einer natürlichen oder juristischen Person kann die für Datenvermittlungsdienste zuständige Behörde auch die Einhaltung der Rechtsvorschriften durch Anbieter von Datenvermittlungsdiensten überwachen und beaufsichtigen.
- (2) Die für Datenvermittlungsdienste zuständigen Behörden sind befugt, von den Anbietern von Datenvermittlungsdiensten oder ihren gesetzlichen Vertretern alle Informationen anzufordern, die nötig sind, um die Einhaltung der Anforderungen dieses Kapitels zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und mit Gründen versehen sein.
- (3) Stellt die für Datenvermittlungsdienste zuständige Behörde fest, dass ein Anbieter von Datenvermittlungsdiensten gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies dem betreffenden Anbieter von Datenvermittlungsdiensten mit und gibt ihm Gelegenheit, innerhalb von 30 Tagen nach Erhalt der Mitteilung dazu Stellung zu nehmen.
- (4) Die für Datenvermittlungsdienste zuständige Behörde ist befugt, die Beendigung des in Absatz 3 genannten Verstoßes innerhalb einer angemessenen Frist oder im Fall eines schwerwiegenden Verstoßes unverzüglich zu verlangen, und ergreift angemessene und verhältnismäßige Maßnahmen, um die Einhaltung sicherzustellen. In dieser Hinsicht müssen die für Datenvermittlungsdienste zuständigen Behörden gegebenenfalls dazu befugt sein,
  - a) im Rahmen von Verwaltungsverfahren abschreckende Geldstrafen, die Zwangsgelder und Zwangsgelder mit Rückwirkung umfassen können, zu verhängen gerichtliche Verfahren zur Verhängung von Geldbußen einzuleiten, oder beides zu tun;
  - b) eine Verschiebung des Beginns oder eine Aussetzung der Erbringung des Datenvermittlungsdienstes bis zu den von der für Datenvermittlungsdienste zuständigen Behörde geforderten Änderungen seiner Bedingungen anzuordnen oder
  - c) die Einstellung der Bereitstellung des Datenvermittlungsdienstes anzuordnen, falls schwere oder wiederholte Verstöße trotz der vorherigen Mitteilung gemäß Absatz 3 nicht behoben wurden.

Die für Datenvermittlungsdienste zuständige Behörde fordert die Kommission auf, den Anbieter des Datenvermittlungsdienstes aus dem Register der Anbieter von Datenvermittlungsdiensten zu streichen, sobald sie die Einstellung der Bereitstellung von Datenvermittlungsdiensten gemäß Unterabsatz 1 Buchstabe c angeordnet hat.

Wenn ein Anbieter von Datenvermittlungsdiensten die Verstöße beseitigt, teilt dieser Anbieter von Datenvermittlungsdiensten dies erneut der für Datenvermittlungsdienste zuständigen Behörde mit. Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede erneute Mitteilung mit.

(5) Wenn ein Anbieter von Datenvermittlungsdiensten, der nicht in der Union niedergelassen ist, keinen gesetzlichen Vertreter benennt oder der gesetzliche Vertreter es versäumt, auf Verlangen der für Datenvermittlungsdienste zuständigen Behörde die erforderlichen Informationen vorzulegen, durch die die Einhaltung dieser Verordnung umfassend belegt wird, ist die für Datenvermittlungsdienste zuständige Behörde befugt, den Beginn der Erbringung des Datenvermittlungsdienstes zu verschieben oder diese auszusetzen, bis der gesetzliche Vertreter benannt wurde oder die erforderlichen Informationen vorgelegt wurden.

(6) Die für Datenvermittlungsdienste zuständigen Behörden teilen dem betreffenden Anbieter der Datenvermittlungsdienste unverzüglich die gemäß den Absätzen 4 und 5 auferlegten Maßnahmen, die Gründe dafür sowie die notwendigen Schritte zur Behebung der entsprechenden Mängel mit und setzen dem Anbieter von Datenvermittlungsdiensten eine angemessene Frist von höchstens 30 Tagen damit der Anbieter von Datenvermittlungsdiensten diesen Maßnahmen nachkommen kann.

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

Ersucht eine für Datenvermittlungsdienste zuständige Behörde in einem Mitgliedstaat um Unterstützung einer für Datenvermittlungsdienste zuständigen Behörde aus einem anderen Mitgliedstaat, so stellt sie ein begründetes Ersuchen. Die für Datenvermittlungsdienste zuständige Behörde antwortet dieses Ersuchen unverzüglich und innerhalb einer Frist, die der Dringlichkeit des Ersuchens angemessen ist.

Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe nach diesem Artikel ausgetauscht werden, dürfen nur zu den Zwecken verwendet werden, für die um sie ersucht wurde.

#### *Artikel 15*

### **Ausnahmen**

Dieses Kapitel gilt nicht für anerkannte datenaltruistische Organisationen und andere Einrichtungen ohne Erwerbszweck, soweit deren Tätigkeit darin besteht, für Ziele von allgemeinem Interesse Daten zu erheben, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus zur Verfügung gestellt werden, es sei denn, diese Organisationen und Einrichtungen sind bestrebt, Geschäftsbeziehungen zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern einerseits und Datennutzern andererseits herzustellen.

#### *KAPITEL IV*

### **Dataltruismus**

#### *Artikel 16*

### **Nationale Regelungen für Datenaltruismus**

Die Mitgliedstaaten können organisatorische oder technische Regelungen oder beides festlegen, um Datenaltruismus zu erleichtern. Hierzu können die Mitgliedstaaten nationale Strategien für Datenaltruismus festlegen. Diese nationalen Strategien können insbesondere dazu dienen, betroffene Personen dabei zu unterstützen, sie betreffende personenbezogene Daten im Besitz öffentlicher Stellen freiwillig für den Datenaltruismus zur Verfügung zu stellen, und die erforderlichen Informationen festzulegen, die betroffenen Personen in Bezug auf die Weiterverwendung ihrer Daten im allgemeinen Interesse zur Verfügung gestellt werden müssen.

Entwickelt ein Mitgliedstaat solche nationalen Strategien, so teilt er dies der Kommission mit.

#### Artikel 17

### Öffentliche Register der anerkannten datenaltuistischen Organisationen

- (1) Jede für die Registrierung von datenaltuistischen Organisationen zuständige Behörde führt ein öffentliches nationales Register der anerkannten datenaltuistischen Organisationen und aktualisiert dieses regelmäßig.
- (2) Die Kommission pflegt zu Informationszwecken ein öffentliches Unionsregister der anerkannten datenaltuistischen Organisationen. Sofern eine gemäß Artikel 18 im öffentlichen nationalen Register der anerkannten datenaltuistischen Organisationen eingetragene Einrichtung registriert ist, darf sie in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannte datenaltuistische Organisation“ und ein gemeinsames Logo verwenden.

Damit anerkannte datenaltuistische Organisationen in der gesamten Union leicht zu erkennen sind, legt die Kommission im Wege von Durchführungsrechtsakten die Ausgestaltung des gemeinsamen Logos fest. Anerkannte datenaltuistische Organisationen verwenden das gemeinsame Logo gut sichtbar auf jeder Online- und Offline-Veröffentlichung, die mit ihren datenaltuistischen Tätigkeiten in Zusammenhang steht. Das gemeinsame Logo erscheint gemeinsam mit einem QR-Code mit Link zum öffentlichen Unionsregister der anerkannten datenaltuistischen Organisationen.

Die Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

#### Artikel 18

### Allgemeine Eintragungsanforderungen

Um für eine Eintragung in ein öffentliches nationales Register anerkannter datenaltuistischer Organisationen infrage zu kommen, muss eine Einrichtung

- a) datenaltuistische Tätigkeiten durchführen;
- b) gemäß nationalem Recht Rechtspersönlichkeit haben, um gegebenenfalls gemäß dem nationalen Recht Ziele von allgemeinem Interesse zu erreichen;
- c) selbst ohne Erwerbszweck tätig sein und rechtlich unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln;
- d) die Datenaltuismus-Tätigkeiten über eine Struktur ausüben, die von ihren anderen Tätigkeiten funktionell getrennt ist;
- e) dem in Artikel 22 Absatz 1 genannten Regelwerk entsprechen, und zwar spätestens 18 Monate nach dem Tag des Inkrafttretens der delegierten Rechtsakte, auf die in jenem Absatz Bezuggenommen wird.

#### Artikel 19

### Eintragung anerkannter datenaltuistischer Organisationen

- (1) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt, kann einen Antrag auf Eintragung in das nationale öffentliche Register der anerkannten datenaltuistischen Organisationen in dem Mitgliedstaat stellen, in dem sie niedergelassen ist.
- (2) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt und in mehreren Mitgliedstaaten niedergelassen ist, kann einen Antrag zur Eintragung in das nationale öffentliche Register der anerkannten datenaltuistischen Organisationen in dem Mitgliedstaat beantragen, in dem sie ihre Hauptniederlassung hat.
- (3) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt, aber nicht in der Union niedergelassen ist, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in dem diese datenaltuistischen Dienste angeboten werden.

Um die Einhaltung dieser Verordnung sicherzustellen, beauftragt die Einrichtung den gesetzlichen Vertreter, neben ihr oder an ihrer Stelle für die Registrierung datenaltuistischer Organisationen den zuständigen Behörden oder betroffenen Personen und Dateninhabern bei Fragen im Zusammenhang mit diesen Einrichtungen als Anlaufstelle zu dienen. Der gesetzliche Vertreter arbeitet mit den für die Registrierung datenaltuistischer Organisationen zuständigen Behörden zusammen und legt ihnen auf Verlangen umfassend dar, welche Maßnahmen und Vorkehrungen die Einrichtung getroffen hat, um die Einhaltung dieser Verordnung sicherzustellen.

Die Einrichtung gilt als in der Zuständigkeit des Mitgliedstaats liegend, in dem der gesetzliche Vertreter niedergelassen ist. Die Einrichtung kann einen Antrag zur Registrierung in das nationale öffentliche Register der anerkannten datenaltuistischen Organisationen in diesem Mitgliedstaat beantragen. Die Benennung eines gesetzlichen Vertreters durch die Einrichtung erfolgt unbeschadet etwaiger rechtlicher Schritte gegen die Einrichtung.

(4) Der Eintragungsantrag gemäß den Absätzen 1, 2 und 3 muss folgende Angaben enthalten:

- a) den Namen der Einrichtung,
- b) Rechtsstatus, Rechtsform und, sofern die Einrichtung in einem öffentlichen nationalen Register eingetragen ist, Registernummer der Einrichtung,
- c) die Satzung der Einrichtung, falls zutreffend,
- d) die Einnahmequellen der Einrichtung,
- e) die Anschrift der Hauptniederlassung der Einrichtung in der Union, falls vorhanden, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gesetzlichen Vertreters,
- f) eine öffentliche Website mit vollständigen und aktuellen Informationen über die Einrichtung und ihre Tätigkeiten, einschließlich mindestens der Informationen gemäß den Buchstaben a, b, d, e und h,
- g) die Kontaktpersonen und Kontaktangaben der Einrichtung,
- h) die Ziele von allgemeinem Interesse, die sie mit der Erhebung der Daten fördern will,
- i) die Art der Daten, die die Einrichtung überprüfen oder verarbeiten will, sowie, im Fall von personenbezogenen Daten, die Kategorien von personenbezogenen Daten,
- j) alle sonstigen Nachweise, die belegen, dass die Anforderungen des Artikels 18 erfüllt werden.

(5) Nachdem die Einrichtung alle erforderlichen Informationen gemäß Absatz 4 übermittelt hat und die für die Registrierung datenaltuistischer Organisationen zuständige Behörde den Eintragungsantrag bewertet hat und zu dem Schluss gekommen ist, dass die Einrichtung die Anforderungen des Artikels 18 erfüllt, nimmt die Behörde innerhalb von 12 Wochen nach Eingang des Antrags auf Registrierung die Eintragung der Einrichtung in das öffentliche nationale Register der anerkannten datenaltuistischen Organisationen vor. Die Eintragung gilt in allen Mitgliedstaaten.

Die für die Registrierung von datenaltuistischen Organisationen zuständige Behörde teilt der Kommission jede Registrierung mit. Die Kommission nimmt diese Registrierung in das öffentliche Unionsregister der anerkannten datenaltuistischen Organisationen auf.

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

(7) Eine anerkannte datenaltuistische Organisation teilt der entsprechenden für die Registrierung von datenaltuistischen Organisationen zuständigen Behörde jede Änderung der gemäß Absatz 4 übermittelten Angaben innerhalb von 14 Tagen ab dem Tag der Änderung mit.

Die für die Registrierung datenaltuistischer Organisationen zuständigen Behörde teilt der Kommission unverzüglich jede solche Mitteilung auf elektronischem Wege mit. Auf der Grundlage einer solchen Meldung aktualisiert die Kommission unverzüglich das öffentliche Unionsregister der anerkannten datenaltuistischen Organisationen.

*Artikel 20***Transparenzanforderungen**

- (1) Eine anerkannte datenaltuistische Organisation führt vollständige und genaue Aufzeichnungen über Folgendes:
- alle natürlichen oder juristischen Personen, denen die Möglichkeit zur Verarbeitung der im Besitz dieser anerkannten datenaltuistischen Organisation befindlichen Daten gegeben wurde, sowie deren Kontaktdaten,
  - den Zeitpunkt oder die Dauer der Verarbeitung personenbezogener Daten oder der Nutzung nicht personenbezogener Daten,
  - den Zweck der Verarbeitung entsprechend der Erklärung der natürlichen oder juristischen Person, der die Möglichkeit zur Verarbeitung gegeben wurde,
  - etwaige Gebühren, die von den die Daten verarbeitenden natürlichen oder juristischen Personen gezahlt wurden.
- (2) Eine anerkannte datenaltuistische Organisation erstellt einen jährlichen Tätigkeitsbericht und übermittelt ihn der entsprechenden für die Eintragung von datenaltuistischen Organisationen zuständigen Behörde; dieser Bericht enthält mindestens Folgendes:
- Informationen über die Tätigkeiten der anerkannten datenaltuistischen Organisation,
  - eine Beschreibung, in welcher Weise die Zwecke von allgemeinem Interesse, zu denen die Daten gesammelt wurden, in dem betreffenden Geschäftsjahr gefördert wurden,
  - eine Liste aller natürlichen und juristischen Personen, denen erlaubt wurde, die in ihrem Besitz befindlichen Daten zu verarbeiten, einschließlich einer zusammenfassenden Beschreibung der Zwecke von allgemeinem Interesse, die mit dieser Datenverarbeitung 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,
  - gegebenenfalls eine Zusammenfassung der Ergebnisse der von der anerkannten datenaltuistischen Organisation erlaubten Datenverarbeitung,
  - Informationen über die Einnahmequellen der anerkannten datenaltuistischen Organisation, insbesondere alle Einnahmen aus der Zugänglichmachung der Daten, sowie über die Ausgaben.

*Artikel 21***Besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber im Hinblick auf ihre Daten**

- (1) Eine anerkannte datenaltuistische Organisation informiert betroffene Personen oder Dateninhaber vor der Verarbeitung ihrer Daten auf klare und leicht verständliche Weise über Folgendes:
- die Ziele von allgemeinem Interesse und gegebenenfalls den angegebenen, ausdrücklichen und rechtmäßigen Zweck der Verarbeitung personenbezogener Daten, für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt;
  - den Standort und die Ziele von allgemeinem Interesse, für die sie eine etwaige Verarbeitung in einem Drittland erlaubt, sofern die Verarbeitung von der anerkannten datenaltuistischen Organisation vorgenommen wird.
- (2) Die anerkannte datenaltuistische Organisation verwendet die Daten nicht für andere als die Ziele von allgemeinem Interesse, für die die betroffene Person oder der Dateninhaber die Verarbeitung erlaubt hat. Die anerkannte datenaltuistische Organisation darf keine irreführenden Vermarktungspraktiken verwenden, um Daten zu erhalten.
- (3) Die anerkannte datenaltuistische Organisation stellt Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit. Die anerkannte datenaltuistische Organisation stellt ferner Werkzeuge zum einfachen Widerruf einer solchen Einwilligung oder Erlaubnis zur Verfügung.
- (4) Die anerkannte datenaltuistische Organisation ergreift Maßnahmen, um ein angemessenes Sicherheitsniveau für die Speicherung und Verarbeitung der nicht personenbezogenen Daten sicherzustellen, die sie auf der Grundlage von Datenaltuismus erhoben hat.
- (5) Die Dateninhaber werden von der anerkannten datenaltuistischen Organisation im Falle einer unbefugten Übertragung, des unbefugten Zugriffs oder der unbefugten Nutzung der von ihm geteilten nicht personenbezogenen Daten unverzüglich unterrichtet.

(6) Ermöglicht die anerkannte datenaltuistische Organisation die Datenverarbeitung durch Dritte, einschließlich durch die Bereitstellung von Werkzeugen zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit, so gibt sie gegebenenfalls das Hoheitsgebiet des Drittlandes an, in denen die Datennutzung stattfinden soll.

#### Artikel 22

##### **Regelwerk**

(1) Die Kommission erlässt gemäß Artikel 32 delegierte Rechtsakte zur Ergänzung der vorliegenden Verordnung durch die Ausarbeitung eines Regelwerks, das Folgendes enthält:

- a) angemessene Informationsanforderungen, um sicherzustellen, dass betroffene Personen und Dateninhaber vor Erteilung einer Einwilligung oder Erlaubnis für Datenaltuismus ausreichend detaillierte, klare und transparente Informationen über die Datennutzung, die Werkzeuge zur Erteilung und zum Widerruf der Einwilligung oder Erlaubnis und über die Maßnahmen erhalten, die ergriffen werden, um einen Missbrauch der mit der datenaltuistischen Organisation ausgetauschten Daten zu verhindern,
- b) geeignete technische Anforderungen und Sicherheitsanforderungen, um ein angemessenes Sicherheitsniveau für die Speicherung und Verarbeitung von Daten sowie für die Werkzeuge zur Erteilung und zum Widerruf der Einwilligung oder der Erlaubnis,
- c) Kommunikationsfahrpläne, bei denen ein multidisziplinärer Ansatz verfolgt wird, um das Bewusstsein für Datenaltuismus, die Bezeichnung als „in der Union anerkannte datenaltuistische Organisation“ und das Regelwerk unter den einschlägigen Interessenträgern, insbesondere Dateninhabern und betroffenen Personen, die möglicherweise ihre Daten austauschen würden, zu schärfen,
- d) Empfehlungen zu einschlägigen Interoperabilitätsnormen.

(2) Das in Absatz 1 genannte Regelwerk wird in enger Zusammenarbeit mit datenaltuistischen Organisationen und einschlägigen Interessenträgern erstellt.

#### Artikel 23

##### **Für die Registrierung von datenaltuistischen Organisationen zuständige Behörden**

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für das öffentliche nationale Register der anerkannten datenaltuistischen Organisationen zuständig sind.

Die für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden müssen den Anforderungen gemäß Artikel 26 entsprechen.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen seiner für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden bis zum 24. September 2023 mit. Jeder Mitgliedstaat teilt der Kommission auch alle späteren Änderungen der Namen dieser zuständigen Behörden mit.

(3) Die für die Eintragung von datenaltuistischen Organisationen zuständige Behörde nimmt ihre Aufgaben in Bezug auf die Verarbeitung personenbezogener Daten in Zusammenarbeit mit der einschlägigen Datenschutzbehörde sowie mit den einschlägigen sektoralen Behörden desselben Mitgliedstaats wahr.

#### Artikel 24

##### **Überwachung der Einhaltung**

(1) Die für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden überwachen und beaufsichtigen die Einhaltung der in diesem Kapitel festgelegten Anforderungen durch die anerkannten datenaltuistischen Organisationen. Die für die Eintragung von datenaltuistischen Organisationen zuständige Behörde kann die Einhaltung der Rechtsvorschriften durch diese datenaltuistischen Organisationen auch auf Antrag einer natürlichen oder juristischen Person überwachen und beaufsichtigen.

(2) Die für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden sind befugt, von den anerkannten datenaltuistischen Organisationen alle Informationen zu verlangen, die nötig sind, um die Einhaltung der Anforderungen dieses Kapitels zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(3) Stellt die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde fest, dass eine anerkannte datenaltruistische Organisation gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies der anerkannten datenaltruistischen Organisation mit und gibt ihr Gelegenheit, innerhalb von 30 Tagen nach Erhalt der Meldung dazu Stellung zu nehmen.

(4) Die für die Registrierung von datenaltruistischen Organisationen 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 anerkannte datenaltruistische Organisation eine oder mehrere der Anforderungen dieses Kapitels auch dann nicht, nachdem sie von der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörde gemäß Absatz 3 davon unterrichtet wurde, so

- a) verliert sie ihr Recht, in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ zu führen,
- b) wird sie aus dem einschlägigen öffentlichen nationalen Register der anerkannten datenaltruistischen Organisationen und dem öffentlichen Unionsregister der anerkannten datenaltruistischen Organisationen gestrichen.

Jede Entscheidung gemäß Unterabsatz 1 Buchstabe a, die das Recht widerruft, die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ zu führen, wird durch die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde öffentlich zugänglich gemacht.

(6) Hat eine anerkannte datenaltruistische Organisation ihre Hauptniederlassung oder ihren gesetzlichen Vertreter in einem Mitgliedstaat, betätigt sich aber in anderen Mitgliedstaaten, so arbeiten die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder der gesetzliche Vertreter befindet, und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden für die Zwecke ihrer Tätigkeiten im Rahmen dieser Verordnung und begründete Ersuchen umfassen, die in diesem Artikel genannten Maßnahmen zu ergreifen.

Ersucht eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde in einem Mitgliedstaat um Unterstützung durch eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde in einem anderen Mitgliedstaat, so stellt sie ein begründetes Ersuchen. Nach einem solchen Ersuchen antwortet die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde unverzüglich und innerhalb eines Zeitrahmens, der der Dringlichkeit des Ersuchens angemessen ist.

Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe nach diesem Artikel ausgetauscht werden, dürfen nur zu den Zwecken des Ersuchens verwendet werden.

## Artikel 25

### **Europäisches Einwilligungsförmular für Datenaltruismus**

(1) Um die Erhebung von Daten auf der Grundlage des Datenaltruismus zu erleichtern, erlässt die Kommission nach Konsultation des Europäischen Datenschutzausschusses, unter Berücksichtigung der Empfehlungen des Europäischen Dateninnovationsrats sowie unter entsprechender Einbeziehung einschlägiger Interessenträger Durchführungsrechtsakte zur Festlegung und Ausarbeitung eines europäischen Einwilligungsförmulars für Datenaltruismus. Das Förmular ermöglicht das Einholen von Einwilligungen und Erlaubnissen in allen Mitgliedstaaten in einem einheitlichen Format. Diese Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

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

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

(4) Das Förmular ist leicht verständlich und wird in einer Form bereitgestellt, in der es auf Papier ausgedruckt werden kann, sowie in elektronischer, maschinenlesbarer Form.

## KAPITEL V

**Zuständige Behörden und Verfahrensvorschriften**

## Artikel 26

**Anforderungen an zuständige Behörden**

- (1) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden müssen von allen Anbietern von Datenvermittlungsdiensten und allen anerkannten datenaltruistischen Organisationen rechtlich getrennt und funktional unabhängig sein. Die Aufgaben der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden können von derselben Behörde wahrgenommen werden. Die Mitgliedstaaten können entweder eine oder mehrere neue Behörden für diese Zwecke errichten oder bereits vorhandene Behörden nutzen.
- (2) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden nehmen ihre Aufgaben unparteiisch, transparent, kohärent und rechtzeitig wahr. Bei der Wahrnehmung ihrer Aufgaben sorgen sie für einen fairen Wettbewerb und Diskriminierungsfreiheit.
- (3) Die oberste Leitungsebene und die Mitarbeiter, die für die Durchführung der in dieser Verordnung vorgesehenen einschlägigen Aufgaben der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden verantwortlich sind, dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der von ihnen bewerteten Dienste noch bevollmächtigter Vertreter einer dieser Parteien sein. Dies schließt die Verwendung von bewerteten Diensten, die für die Tätigkeit der für Datenvermittlungsdienste zuständigen Behörde und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörde nötig sind, oder die Verwendung solcher Dienste zum persönlichen Gebrauch nicht aus.
- (4) Die oberste Leitungsebene und die Mitarbeiter der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den ihnen übertragenen Bewertungstätigkeiten beeinträchtigen könnten.
- (5) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen 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 für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden eines Mitgliedstaats stellen der Kommission und den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden anderer Mitgliedstaaten auf begründeten Antrag und unverzüglich die Informationen zur Verfügung, die sie zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung benötigen. Sieht eine für Datenvermittlungsdienste zuständige Behörde oder eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde die verlangten Informationen nach den Bestimmungen des Unionsrechts und des nationalen Rechts über das Berufs- und Geschäftsgeheimnis als vertraulich an, so gewährleisten die Kommission und alle anderen für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden eine entsprechende vertrauliche Behandlung.

## Artikel 27

**Beschwerderecht**

- (1) Natürliche und juristische Personen haben das Recht, wegen aller in den Anwendungsbereich dieser Verordnung fallenden Angelegenheiten bei der jeweiligen, für die Datenvermittlungsdienste zuständigen Behörde, allein oder gegebenenfalls gemeinsam, Beschwerde gegen einen Anbieter von Datenvermittlungsdiensten oder bei der jeweiligen, für die Registrierung von datenaltruistischen Organisationen gegen eine anerkannte datenaltruistische Organisation einzulegen.

- (2) Die für Datenvermittlungsdienste zuständige Behörde und die für die Registrierung von datenaltuistischen Organisationen zuständige Behörde, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer
- a) über den Stand des Verfahrens und die getroffene Entscheidung und
  - b) über die Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 28.

#### Artikel 28

### **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 gegen rechtsverbindliche Entscheidungen gemäß Artikel 14 durch die für Datenvermittlungsdienste zuständigen Behörden in Bezug auf die Verwaltung, Kontrolle und Durchsetzung der Anmeldevorschriften für Anbieter von Datenvermittlungsdiensten und rechtsverbindliche Entscheidungen gemäß Artikel 19 und 24 durch die für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden in Bezug auf die Überwachung von anerkannten datenaltuistischen Organisationen.
- (2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats der für Datenvermittlungsdienste zuständigen Behörde und der für die Registrierung von datenaltuistischen Organisationen zuständigen Behörde, gegen die der allein oder gegebenenfalls gemeinsam von den Vertretern einer oder mehrerer natürlicher oder juristischer Personen eingelegte Rechtsbehelf gerichtet ist, eingeleitet.
- (3) Bleibt eine für Datenvermittlungsdienste zuständige Behörde oder eine für die Registrierung von datenaltuistischen Organisationen zuständige Behörde auf eine Beschwerde untätig, haben betroffene natürliche und juristische Personen gemäß dem nationalen Recht entweder Anspruch auf einen wirksamen gerichtlichen Rechtsbehelf oder Zugang zur Nachprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis.

#### KAPITEL VI

### **Europäischer Dateninnovationsrat**

#### Artikel 29

### **Europäischer Dateninnovationsrat**

- (1) Die Kommission setzt einen Europäischen Dateninnovationsrat ein, der die Form einer Expertengruppe hat und sich aus Vertretern der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden aller Mitgliedstaaten, des Europäischen Datenschutzausschusses, des Europäischen Datenschutzbeauftragten, der ENISA, der Kommission, dem KMU-Beauftragten der EU oder einem vom Netz der KMU-Beauftragten benannten Vertreter und anderen Vertretern von maßgeblichen Stellen in bestimmten Sektoren und von Stellen mit spezifischen Fachkenntnissen zusammensetzt. Bei der Ernennung einzelner Sachverständiger strebt die Kommission im Hinblick auf die Zusammensetzung der Expertengruppe ein ausgewogenes Geschlechterverhältnis und geografische Ausgewogenheit unter den Mitgliedern der Expertengruppe an.
- (2) Der Europäische Dateninnovationsrat besteht aus mindestens den drei folgenden Untergruppen:
- a) einer aus den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltuistischen Organisationen zuständigen Behörden zusammengesetzten Untergruppe für die Aufgaben gemäß Artikel 30 Buchstaben a, c, j und k,
  - b) einer Untergruppe für technische Beratungen zu Normung, Übertragbarkeit und Interoperabilität gemäß Artikel 30 Buchstaben f und g,

- c) einer Untergruppe für die Einbeziehung von Interessenträgern, der einschlägige Vertreter der Wirtschaft, der Forschung, der Wissenschaft, der Zivilgesellschaft, von Normungsgremien, einschlägigen gemeinsamen europäischen Datenräumen und andere einschlägige Interessenträger und Dritte angehören, die den Europäischen Dateninnovationsrat zu Aufgaben gemäß Artikel 30 Buchstaben d, e, f, g und h beraten.
- (3) Die Kommission führt den Vorsitz in den Sitzungen des Europäischen Dateninnovationsrats.
- (4) Der Europäische Dateninnovationsrat wird von einem Sekretariat unterstützt, das von der Kommission gestellt wird.

#### Artikel 30

### Aufgaben des Europäischen Dateninnovationsrats

Der Europäische Dateninnovationsrat 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 für die Bearbeitung von Anträgen auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien;
- b) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis für den unionsweiten Datenaltruismus;
- c) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden bei der Anwendung der Anforderungen, die jeweils für Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen gelten;
- d) Beratung und Unterstützung der Kommission bei der Entwicklung einheitlicher Leitlinien dazu, wie 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, optimal geschützt werden können;
- e) Beratung und Unterstützung der Kommission bei der Entwicklung einheitlicher Leitlinien zu Cybersicherheitsanforderungen beim Austausch und der Speicherung von Daten;
- f) Beratung der Kommission unter besonderer Berücksichtigung der Beiträge von Normungsgremien bei der Festlegung von Prioritäten für die Verwendung bzw. Entwicklung sektorübergreifender Normen für die Datennutzung und sektorübergreifende gemeinsame Datennutzung durch neue gemeinsame europäische Datenräume sowie für den sektorübergreifenden Vergleich und Austausch bewährter Verfahren in Bezug auf Sicherheitsanforderungen und Zugangsverfahren in bestimmten Sektoren, wobei sektorspezifische Normungstätigkeiten insbesondere bei der Klärung, welche Normen und Praktiken sektorspezifisch und welche sektorübergreifend sind, und bei der diesbezüglichen Differenzierung zu berücksichtigen sind;
- g) Unterstützung der Kommission unter besonderer Berücksichtigung der Beiträge von Normungsgremien bei ihren Bemühungen, einer Fragmentierung des Binnenmarkts und der Datenwirtschaft im Binnenmarkt entgegenzuwirken, indem die grenzüberschreitende und die sektorübergreifende Interoperabilität von Daten sowie von Diensten für die gemeinsame Datennutzung zwischen verschiedenen Sektoren und Bereichen auf der Grundlage bestehender europäischer, internationaler oder nationaler Normen verbessert wird, um unter anderem die Schaffung gemeinsamer europäischer Datenräume zu fördern;
- h) Unterbreitung von Leitlinien zu „gemeinsamen europäischen Datenräumen“, also zu zweck- oder sektorspezifischen oder auch sektorübergreifenden interoperablen Rahmen mit gemeinsamen Normen und Praktiken für die gemeinsame Nutzung oder Verarbeitung von Daten – unter anderem zur Entwicklung neuer Produkte und Dienste, für die wissenschaftliche Forschung oder für Initiativen der Zivilgesellschaft; solche gemeinsame Normen und Praktiken tragen geltenden Normen Rechnung, entsprechen den Wettbewerbsregeln und gewährleisten den nichtdiskriminierenden Zugang für alle Beteiligten, um die gemeinsame Datennutzung in der Union zu erleichtern und das Potenzial bereits vorhandener und künftiger Datenräume auszuschöpfen; dabei werden folgende Bereiche behandelt:
  - i) Verwendung und Entwicklung sektorübergreifender Normen für die Datennutzung und die sektorübergreifende gemeinsame Datennutzung, sektorübergreifender Vergleich und Austausch bewährter Verfahren in Bezug auf sektorale Sicherheitsanforderungen und Zugangsverfahren, wobei sektorspezifische Normungstätigkeiten insbesondere Klärung der Frage, welche Normen und Praktiken sektorspezifisch und welche sektorübergreifend sind, und bei der diesbezüglichen Differenzierung zu berücksichtigen sind,
  - ii) Anforderungen bezüglich der Beseitigung von Marktzutrittsbeschränkungen und der Vermeidung von Lock-in-Effekten im Interesse eines fairen Wettbewerbs und der Interoperabilität,

- iii) angemessener Schutz für rechtmäßige Datenübertragungen in Drittländer, einschließlich Schutzvorkehrungen gegen nach Unionsrecht verbotene Datenübertragungen,
  - iv) angemessene und nichtdiskriminierende Vertretung der einschlägigen Interessenträger bei der Verwaltung gemeinsamer europäischer Datenräume,
  - v) Einhaltung der gemäß dem Unionsrecht geltenden Cybersicherheitsanforderungen.
- i) Erleichterung der Zusammenarbeit zwischen den Mitgliedstaaten bezüglich der Festlegung harmonisierter Bedingungen für die Erlaubnis, binnenmarktweit im Besitz öffentlicher Stellen befindliche Kategorien von Daten gemäß Artikel 3 Absatz 1 wiederzuverwenden;
  - j) Erleichterung der Zusammenarbeit zwischen den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden mittels Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für einen effizienten Informationsaustausch über das Anmeldeverfahren für Anbieter von Datenvermittlungsdiensten und die Eintragung und Überwachung anerkannter datenaltruistischer Organisationen, einschließlich der Abstimmung über Gebühren und Sanktionen sowie der Erleichterung der Zusammenarbeit zwischen den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden beim internationalen Zugang zu Daten und internationale Datenübertragungen;
  - k) Beratung und Unterstützung der Kommission bei der Prüfung der Frage, ob die Durchführungsrechtsakte gemäß Artikel 5 Absätze 11 und 12 erlassen werden sollen;
  - l) Beratung und Unterstützung der Kommission bei der Entwicklung des europäischen Einwilligungsförmulars für Datenaltruismus gemäß Artikel 25 Absatz 1;
  - m) Beratung der Kommission bei der Verbesserung des internationalen Regelungsumfelds für nicht personenbezogene Daten einschließlich der Normung.

## KAPITEL VII

### **Internationaler Zugang und internationale Übertragung**

#### Artikel 31

### **Internationaler Zugang und internationale Übertragung**

- (1) Die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation ergreifen alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen, um die internationale Übertragung in der Union gespeicherter nicht personenbezogener Daten oder den Zugang von Regierungsorganisationen zu diesen Daten zu verhindern, wenn eine solche Übertragung oder ein solcher Zugang im Widerspruch zum Unionsrecht oder dem nationalen Recht des betreffenden Mitgliedstaats stünde; Absatz 2 oder Absatz 3 bleiben davon unberührt.
- (2) Entscheidungen und Urteile 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 II gewährt wurde, einem Anbieter von Datenvermittlungsdiensten oder einer anerkannten datenaltruistischen Organisationen die Übertragung von in der Union gespeicherten nicht personenbezogenen Daten im Anwendungsbereich dieser Verordnung oder der Zugang zu diesen Daten in der Union verlangt wird, werden nur dann anerkannt oder vollstreckbar, wenn sie auf eine in Kraft befindliche völkerrechtliche Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder auf eine solche Vereinbarung zwischen dem ersuchenden Drittland und einem Mitgliedstaat gestützt sind.
- (3) Wenn keine völkerrechtliche Übereinkunft gemäß Absatz 2 des vorliegenden Artikels besteht und eine Entscheidung oder ein Urteil eines Gerichts eines Drittlandes oder eine Entscheidung einer Verwaltungsbehörde eines Drittlands, mit der die Übertragung nicht personenbezogener Daten im Anwendungsbereich dieser Verordnung 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 II gewährt wurde, einen Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation gerichtet ist und die Befolgung einer solchen Entscheidung den Adressaten in Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats bringen würde, erfolgt die Übertragung dieser Daten an die Behörde des Drittlands oder die entsprechende Zugangsgewährung nur dann, wenn
- a) das Rechtssystem des Drittlands vorschreibt, dass die Entscheidung oder das Urteil zu begründen ist und verhältnismäßig sein muss, und weiter vorsieht, dass die Entscheidung oder das Urteil eine hinreichende Bestimmtheit aufweisen muss, indem z. B. darin eine hinreichende Bezugnahme auf bestimmte verdächtige Personen oder Rechtsverletzungen erfolgt,

- b) der begründete Einwand des Adressaten von einem zuständigen Gericht des Drittlands überprüft wird und
- c) das zuständige Gericht des Drittlands, das die Entscheidung oder das Urteil erlässt oder die Entscheidung einer Verwaltungsbehörde überprüft, nach dem Recht dieses Drittlands befugt ist, die einschlägigen rechtlichen Interessen des Bereitstellers der durch das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats geschützten Daten gebührend zu berücksichtigen.
- (4) Sind die in Absatz 2 oder 3 festgelegten Bedingungen nicht erfüllt, so überträgt die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation aufgrund einer vertretbaren Auslegung des Ersuchens nur die auf das Ersuchen hin zulässige Mindestmenge an Daten.
- (5) Bevor die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation dem Ersuchen einer Verwaltungsbehörde eines Drittlands auf Zugang zu den Daten eines Dateninhabers nachkommt, unterrichtet sie bzw. er den Dateninhaber über das Vorliegen dieses Ersuchens, es sei denn, das Ersuchen dient Strafverfolgungszwecken, und solange dies zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahme erforderlich ist.

## KAPITEL VIII

### *Delegierung und Ausschussverfahren*

#### *Artikel 32*

#### **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 13 und Artikel 22 Absatz 1 wird der Kommission auf unbestimmte Zeit ab dem 23. Juni 2022 übertragen.
- (3) Die Befugnisübertragung gemäß Artikel 5 Absatz 13 und Artikel 22 Absatz 1 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 13 und Artikel 22 Absatz 1 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 33*

#### **Ausschussverfahren**

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

- (2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 4 der Verordnung (EU) Nr. 182/2011.
- (3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

## KAPITEL IX

### **Schluss- und Übergangsbestimmungen**

#### Artikel 34

#### **Sanktionen**

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die für die Übertragung nicht personenbezogener Daten in Drittländer gemäß Artikel 5 Absatz 14 und Artikel 31 geltenden Verpflichtungen, die nach Artikel 11 für Anbieter von Datenvermittlungsdiensten geltende Mitteilungspflicht, die gemäß Artikel 12 für die Erbringung von Datenvermittlungsdiensten geltenden Bedingungen und die gemäß den Artikeln 18, 20, 21 und 22 für die Eintragung als anerkannte datenaltruistische Organisation geltenden Bedingungen zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. In ihren Sanktionsvorschriften tragen die Mitgliedstaaten den Empfehlungen des Europäischen Dateninnovationsrats Rechnung. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 24. September 2023 mit und melden ihr unverzüglich alle späteren diesbezüglichen Änderungen.

(2) Bei der Verhängung von Sanktionen aufgrund von Verstößen gegen diese Verordnung gegen Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen berücksichtigen die Mitgliedstaaten, gegebenenfalls die folgenden nicht erschöpfenden und indikativen Kriterien:

- a) Art, Schwere, Umfang und Dauer des Verstoßes;
- b) Maßnahmen, die der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation zur Minderung oder Behebung des durch den Verstoß bedingten Schadens ergreifen;
- c) frühere Verstöße des Anbieters von Datenvermittlungsdiensten oder der anerkannten datenaltruistischen Organisation;
- d) die durch den Verstoß bedingten finanziellen Gewinne oder Verluste des Anbieters von Datenvermittlungsdiensten oder der anerkannten datenaltruistischen Organisation, sofern diese Gewinne oder Verluste zuverlässig festgestellt werden können;
- e) sonstige erschwerende oder mildernde Umstände im jeweiligen Fall.

#### Artikel 35

#### **Bewertung und Überprüfung**

Bis zum 24. September 2025 führt die Kommission eine Bewertung dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über ihre wichtigsten Ergebnisse. Dem Bericht werden, soweit erforderlich, Gesetzgebungsvorschläge beigelegt.

Dabei wird in dem Bericht insbesondere Folgendes bewertet:

- a) Anwendung und Funktionsweise der von den Mitgliedstaaten gemäß Artikel 34 festgelegten Sanktionsvorschriften;
- b) Grad der Einhaltung dieser Verordnung durch die gesetzlichen Vertreter von Anbietern von Datenvermittlungsdiensten und anerkannten datenaltruistischen Organisationen, die nicht in der Union niedergelassen sind, und Grad der Durchsetzbarkeit von verhängten Sanktionen gegen diese Anbieter und Organisationen;
- c) Art der gemäß Kapitel IV eingetragenen datenaltruistischen Organisationen und ein Überblick über die mit der gemeinsamen Datennutzung verfolgten Zwecke von allgemeinem Interesse, um diesbezüglich klare Kriterien festzulegen.

Die Mitgliedstaaten übermitteln der Kommission alle zur Ausarbeitung dieses Berichts erforderlichen Informationen.

*Artikel 36*

**Änderung der Verordnung (EU) 2018/1724**

In der Tabelle in Anhang II der Verordnung (EU) 2018/1724 erhält der Eintrag „Gründung, Führung und Schließung eines Unternehmens“ folgende Fassung:

Lebensereignisse	Verfahren	Erwartete Ergebnisse, gegebenenfalls vorbehaltlich einer Bewertung des Antrags durch die zuständige Behörde gemäß nationalen Rechtsvorschriften
Gründung, Führung und Schließung eines Unternehmens	Meldung einer Geschäftstätigkeit, Zulassung zur Ausübung einer Geschäftstätigkeit, Änderung einer Geschäftstätigkeit und Einstellung einer Geschäftstätigkeit ausgenommen Insolvenz- oder Liquidationsverfahren, ausgenommen der erstmaligen Eintragung einer Geschäftstätigkeit in das Unternehmens-Register, und ausgenommen Eintragungen im Rahmen des Verfahrens zur Gründung von — oder späteren Anmeldungen oder Einreichungen von Meldungen von — Gesellschaften oder Unternehmen im Sinne von Artikel 54 Absatz 2 AEUV	Bestätigung des Eingangs der Meldung oder Änderung einer Geschäftstätigkeit oder des Antrags auf Genehmigung der Geschäftstätigkeit
	Registrierung eines Arbeitgebers (einer natürlichen Person) bei obligatorischen Versorgungs- und Versicherungssystemen	Registrierung von Beschäftigten bei obligatorischen Versorgungs- und Versicherungssystemen
	Registrierung von Beschäftigten bei obligatorischen Versorgungs- und Versicherungssystemen	Bestätigung der Registrierung oder Sozialversicherungs-Kennnummer
	Einreichung einer Körperschaftsteuererklärung	Bestätigung des Eingangs der Erklärung
	Meldung an die Sozialversicherungssysteme bei Beendigung des Vertrags mit einem Beschäftigten, ausgenommen bei Verfahren zur kollektiven Beendigung von Arbeitnehmerverträgen	Bestätigung des Eingangs der Meldung
	Zahlung von Sozialbeiträgen für Beschäftigte	Empfangs- oder andere Art der Bestätigung der Zahlung der Sozialbeiträge für Beschäftigte
	Anmeldung eines Anbieters von Datenvermittlungsdiensten	Bestätigung des Eingangs der Anmeldung
	Eintragung als in der Union anerkannte datenaltruistische Organisation	Bestätigung der Eintragung

*Artikel 37*

**Übergangsregelung**

Einrichtungen, die am 23. Juni 2022 die in Artikel 10 genannten Datenvermittlungsdienste bereits erbringen, müssen den in Kapitel III festgelegten Verpflichtungen ab dem 24. September 2025 nachkommen.

*Artikel 38***Inkrafttreten und Geltung**

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

Sie gilt ab dem 24. September 2023.

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

Geschehen zu Brüssel am 30. Mai 2022.

*Im Namen des Europäischen Parlaments*

*Die Präsidentin*

R. METSOLA

*Im Namen des Rates*

*Der Präsident*

B. LE MAIRE

---