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

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Digitalisierung der Wirtschaft beschleunigt sich. Die Informations- und Kommunikationstechnologie ist nicht länger ein besonderer Wirtschaftszweig, sondern bildet die Grundlage aller modernen innovativen Wirtschaftssysteme und Gesellschaften. Elektronische Daten nehmen in diesen Systemen eine zentrale Stellung ein und können eine große Wertschöpfung schaffen, wenn sie analysiert oder mit Dienstleistungen und Produkten kombiniert werden. Gleichzeitig kommen mit der raschen Entwicklung der Datenwirtschaft und neuer Technologien wie der künstlichen Intelligenz, Produkten und Diensten im Zusammenhang mit dem Internet der Dinge, autonomer Systeme und 5G neue rechtliche Fragen bezüglich des Zugangs zu und der Weiterverwendung von Daten, der Haftung, der Ethik und der Solidarität auf. Es sollte erwogen werden, in Haftungsfragen insbesondere durch die Einführung von Regeln für die Selbstregulierung und anderen bewährten Verfahren unter Berücksichtigung von Empfehlungen, Beschlüssen und Maßnahmen, die entlang der gesamten Wertschöpfungskette der Datenverarbeitung ohne menschliches Eingreifen getroffen werden, tätig zu werden. Dies könnte auch geeignete Mechanismen für die Klärung von Haftungsfragen, die Übertragung von Verantwortlichkeiten zwischen kooperierenden Diensten, für Versicherungen und für Audits umfassen.

(2) Daten-Wertschöpfungsketten bestehen aus unterschiedlichen Datenaktivitäten: Datenerzeugung und -erhebung, Datenaggregation und -organisation, Datenverarbeitung, Datenanalyse, -vermarktung und -verbreitung, Datennutzung und -weiterverwendung. Das wirksame und effiziente Funktionieren der Datenverarbeitung ist das tragende Glied jeder Daten-Wertschöpfungskette. Das wirksame und effiziente Funktionieren der Datenverarbeitung und die Entwicklung der Datenwirtschaft in der Union werden jedoch beeinträchtigt, insbesondere durch zwei Arten von Hindernissen für die Datenmobilität und für den Binnenmarkt: die von den Behörden der Mitgliedstaaten eingeführten Datenlokalisierungsauflagen und das Modell der Anbieterabhängigkeit (vendor-lock-in) im privaten Bereich.

(3) Die Niederlassungsfreiheit und die Dienstleistungsfreiheit nach dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) gelten auch für Datenverarbeitungsdienste. Die Erbringung solcher Dienste wird jedoch durch bestimmte nationale, regionale oder lokale Anforderungen, wonach die Daten in einem bestimmten Gebiet zu speichern sind, behindert und bisweilen sogar verhindert.

(4) Solche Hindernisse, die den freien Verkehr von Datenverarbeitungsdiensten wie auch das Niederlassungsrecht der Diensteanbieter beeinträchtigen, gehen auf Anforderungen im Recht der Mitgliedstaaten zurück, wonach sich die Daten zwecks Datenverarbeitung in einem bestimmten geografischen Gebiet oder Hoheitsgebiet befinden müssen. Daneben gibt es andere Vorschriften und Verwaltungspraktiken, die eine gleichartige Wirkung haben, weil sie ganz bestimmte Anforderungen enthalten, die es erschweren, die Daten außerhalb eines bestimmten geografischen Gebiets oder Hoheitsgebiets innerhalb der Union zu verarbeiten, beispielsweise eine vorgeschriebene Nutzung von technischen Anlagen, die in einem bestimmten Mitgliedstaat zertifiziert oder genehmigt worden sind. Die Wahlmöglichkeiten der Marktteilnehmer und des öffentlichen Sektors bezüglich des Standorts der Datenverarbeitung werden durch rechtliche Unsicherheiten bezüglich der Reichweite rechtmäßiger oder unrechtmäßiger Datenlokalisierungsauflagen weiter eingeschränkt. Diese Verordnung schränkt die Freiheit von Unternehmen, Verträge abzuschließen, in denen festgelegt wird, an welchem Ort Daten sich befinden sollen, in keiner Weise ein. Durch diese Verordnung soll lediglich diese Freiheit gewährleistet werden, indem sichergestellt wird, dass ein beliebiger Ort innerhalb der Union vereinbart werden kann.

([1]) ABl. C 227 vom 28.6.2018, S. 78.

([2]) Standpunkt des Europäischen Parlaments vom 4. Oktober 2018 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 6. November 2018.

(5) Gleichzeitig wird die Mobilität der Daten in der Union auch durch private Beschränkungen behindert, nämlich durch rechtliche, vertragliche und technische Probleme, die es den Nutzern von Datenverarbeitungsdiensten erschweren oder unmöglich machen, ihre Daten von einem Diensteanbieter zu einem anderen oder zurück in ihre eigene Informationstechnologie (IT)-Systeme zu übertragen, wenn beispielsweise ihr Vertrag mit einem Diensteanbieter endet.

(6) Das Zusammenspiel dieser Hindernisse hat zu einer Mangel an Wettbewerb zwischen Anbietern von Cloud-Diensten in der Union, zu verschiedenen Problemen im Zusammenhang mit der Anbieterabhängigkeit und zu einer äußerst eingeschränkten Datenmobilität geführt. Außerdem haben Vorgaben zur Datenlokalisierung dazu geführt, dass die Möglichkeiten von Unternehmen aus dem Forschungs- und Entwicklungsbereich eingeschränkt sind, mit Hochschulen und anderen Forschungseinrichtungen zusammenzuarbeiten, um die Innovationskraft zu stärken.

(7) Aus Gründen der Rechtssicherheit und der Notwendigkeit gleicher Wettbewerbsbedingungen innerhalb der Union ist ein einheitliches Regelwerk für alle Marktteilnehmer ein zentrales Element für das Funktionieren des Binnenmarktes. Um Handelshemmnisse und Wettbewerbsverzerrungen aufgrund divergierender nationaler Rechtsvorschriften zu beseitigen und das Entstehen neuer möglicher Handelshemmnisse und beträchtlicher Wettbewerbsverzerrungen zu vermeiden, ist es notwendig, einheitliche und in allen Mitgliedstaaten geltende Vorschriften zu erlassen.

(8) Die vorliegende Verordnung lässt den Rechtsrahmen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, für die Achtung der Privatsphäre und für den Schutz personenbezogener Daten in der elektronischen Kommunikation und insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([1]) und die Richtlinien (EU) 2016/680 ([2]) und 2002/58/EG ([3]) des Europäischen Parlaments und des Rates unberührt.

(9) Das wachsende Internet der Dinge, künstliche Intelligenz und maschinelles Lernen stellen bedeutende Quellen für nicht-personenbezogene Daten dar, zum Beispiel durch ihren Einsatz in automatisierten industriellen Produktionsprozessen. Konkrete Beispiele für nicht-personenbezogene Daten umfassen aggregierte und anonymisierte Datensätze für Big-Data-Analysen, Daten im Zusammenhang mit der Präzisionslandwirtschaft, die dabei helfen können, den Einsatz von Pestiziden und Wasser zu überwachen und zu optimieren, oder Daten zum Wartungsbedarf von Industriemaschinen. Ist es durch technologische Neuentwicklungen möglich, anonymisierten Daten wieder in personenbezogene Daten umzuwandeln, müssen diese Daten als personenbezogene Daten behandelt werden, und die Verordnung (EU) 2016/679 muss entsprechend gelten.

(10) Nach der Verordnung (EU) 2016/679 dürfen die Mitgliedstaaten den freien Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder einschränken noch verbieten. Die vorliegende Verordnung legt denselben Grundsatz des freien Verkehrs innerhalb der Union für nicht-personenbezogene Daten fest, außer wenn eine Einschränkung oder ein Verbot aus Gründen der öffentlichen Sicherheit gerechtfertigt ist. Die Verordnung (EU) 2016/679 und die vorliegende Verordnung bilden ein kohärentes Regelwerk, das auf den freien Verkehr verschiedener Arten von Daten ausgerichtet ist. Zudem wird mit dieser Verordnung nicht vorgeschrieben, dass verschiedene Arten von Daten getrennt zu speichern sind.

(11) Zur Schaffung eines Rahmens für den freien Verkehr nicht-personenbezogener Daten in der Union sowie zur Schaffung der Grundlage für die Entwicklung der Datenwirtschaft und die Verbesserung der Wettbewerbsfähigkeit der Industrie in der Union ist es notwendig, einen klaren, umfassenden und vorhersehbaren Rechtsrahmen für die Verarbeitung von Daten, die keine personenbezogenen Daten sind, im Binnenmarkt festzulegen. Mit einem grundsatzorientierten, die Zusammenarbeit zwischen den Mitgliedstaaten sowie die Selbstregulierung umfassenden Ansatz sollte dafür gesorgt werden, dass dieser Rahmen hinreichend flexibel ist, um mit den sich weiterentwickelnden Bedürfnissen der Nutzer, Diensteanbieter und nationalen Behörden in der Union Schritt zu halten. Um Überschneidungen mit bestehenden Mechanismen und somit höhere Belastungen sowohl für Mitgliedstaaten als auch Unternehmen zu vermeiden, sollten keine ausführlichen technischen Vorschriften erlassen werden.

(12) Diese Verordnung sollte keine Datenverarbeitungsprozesse im Rahmen von Tätigkeiten betreffen, die nicht in den Geltungsbereich des Unionsrechts fallen. Insbesondere ist darauf hinzuweisen, dass die nationale Sicherheit nach Artikel 4 des Vertrags über die Europäische Union (EUV) in die ausschließliche Zuständigkeit der einzelnen Mitgliedstaaten fällt.

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

([2]) 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).

([3]) 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).

(13) Dem freien Datenverkehr innerhalb der Union wird eine entscheidende Bedeutung dabei zukommen, datengetriebenes Wachstum und Innovationen zu generieren. Behörden und Einrichtungen des öffentlichen Rechts der Mitgliedstaaten ziehen ebenso wie Unternehmen und Verbraucher Nutzen aus einer größeren Auswahl an Anbietern datenbezogener Dienste, wettbewerbsfähigeren Preisen und der effizienteren Erbringung von Diensten für die Bürger. Angesichts der großen Datenmengen, die die Behörden und Einrichtungen des öffentlichen Rechts verarbeiten, ist es von größter Bedeutung, dass sie mit gutem Beispiel vorangehen, indem sie Datenverarbeitungsdienste einführen, und auf Datenlokalisierungsauflagen verzichten, wenn sie Datenverarbeitungsdienste nutzen. Deshalb sollte die vorliegende Verordnung auch für Behörden und Einrichtungen des öffentlichen Rechts gelten. In diesem Zusammenhang sollte der in dieser Verordnung geregelte Grundsatz des freien Verkehrs nicht-personenbezogener Daten auch für allgemeine und einheitliche Verwaltungspraktiken und andere Datenlokalisierungsauflagen bei der Vergabe öffentlicher Aufträge gelten, unbeschadet der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([1]).

(14) Wie im Fall der Richtlinie 2014/24/EU lässt die vorliegende Verordnung Rechts- und Verwaltungsvorschriften, die sich auf die interne Organisation der Mitgliedstaaten beziehen und die Übertragung von Befugnissen und Zuständigkeiten für die Datenverarbeitung zwischen Behörden und Einrichtungen des öffentlichen Rechts ohne eine vertragliche Vergütung unter Privatrechtssubjekten zu regeln, sowie Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die die Wahrnehmung dieser Befugnisse und Zuständigkeiten regeln, unberührt. Zwar sind die Behörden und Einrichtungen des öffentlichen Recht angehalten, den wirtschaftlichen und sonstigen Nutzen einer Auslagerung an externe Diensteanbieter zu erwägen, es kann für sie jedoch auch berechtigte Gründe dafür geben, bestimmte Dienste selbst zu erbringen oder Leistungen zu internalisieren. Deshalb werden die Mitgliedstaaten mit dieser Verordnung nicht verpflichtet, Leistungen in Auftrag zu geben oder zu externalisieren, die sie selbst erbringen oder auf anderem Wege als durch die Vergabe öffentlicher Aufträge organisieren möchten.

(15) Diese Verordnung sollte auf natürliche und juristische Personen Anwendung finden, die Datenverarbeitungsdienste für Nutzer erbringen, die in der Union wohnhaft oder niedergelassen sind, einschließlich Anbieter, die Datenverarbeitungsdienste in der Union bereitstellen, ohne eine Niederlassung in der Union zu haben. Diese Verordnung sollte deshalb nicht für die Datenverarbeitungsdienste außerhalb der Union und die auf die betreffenden Daten bezogenen Datenlokalisierungsauflagen gelten.

(16) In dieser Verordnung werden keine Vorschriften für die Bestimmung des anwendbaren Rechts in Handelssachen aufgestellt; somit lässt sie die Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates ([2]) unberührt. Insbesondere unterliegt ein Dienstleistungsvertrag grundsätzlich dem Recht des Landes, in dem der Diensteanbieter seinen gewöhnlichen Aufenthalt hat, soweit das auf einen Vertrag anwendbare Recht nicht nach der genannten Verordnung festgelegt wurde.

(17) Diese Verordnung sollte für die Datenverarbeitung im weitesten Sinne gelten und die Verwendung aller Arten von IT-Systemen erfassen, unabhängig davon, ob diese sich in den Räumlichkeiten des Nutzers befinden oder an einen Diensteanbieter ausgelagert werden. Sie sollte die Datenverarbeitung in unterschiedlichen Intensitätsstufen erfassen, von der Datenspeicherung (Infrastructure-as-a-Service — IaaS) bis zur Verarbeitung von Daten auf Plattformen (Platform-as-a-Service — PaaS) oder in Anwendungen (Software-as-a-Service — SaaS).

(18) Datenlokalisierungsauflagen sind ein eindeutiges Hindernis, das der Dienstleistungsfreiheit in Bezug auf Datenverarbeitungsdienste in der Union sowie auch dem Binnenmarkt entgegensteht. Sie sollten daher an sich verboten werden, soweit sie nicht aus Gründen der öffentlichen Sicherheit im Sinne des Unionsrechts, insbesondere Artikel 52 AEUV, gerechtfertigt sind und dem in Artikel 5 des EUV verankerten Grundsatz der Verhältnismäßigkeit entsprechen. Um dem Grundsatz des freien grenzüberschreitenden Verkehrs nicht-personenbezogener Daten Geltung zu verschaffen, eine rasche Beseitigung bestehender Datenlokalisierungsauflagen zu bewirken und aus betrieblichen Gründen die Verarbeitung von Daten an mehreren Standorten in der Union zu ermöglichen, und da diese Verordnung Maßnahmen vorsieht, die die Verfügbarkeit von Daten für ordnungspolitische Kontrollzwecke gewährleisten, sollten sich die Mitgliedstaaten für die Begründung von Datenlokalisierungsauflagen nur auf die öffentliche Sicherheit berufen können.

(19) Der Begriff der öffentlichen Sicherheit im Sinne von Artikel 52 AEUV und gemäß der Auslegung durch den Gerichtshof bezieht sich sowohl auf die innere als auch die äußere Sicherheit eines Mitgliedstaats sowie auf Fragen der Sicherheit der Bevölkerung, um insbesondere die Untersuchung, Aufdeckung und Verfolgung von Straftaten zu erleichtern. Er setzt die Existenz einer tatsächlichen erheblichen Gefahr voraus, die ein Grundinteresse der Gesellschaft berührt, wie eine Bedrohung für das Funktionieren der Institutionen, der grundlegenden öffentlichen Dienstleistungen und das Überleben der Bevölkerung sowie die Gefahr einer erheblichen Störung der Außenbeziehungen, der friedlichen Koexistenz der Nationen oder eine Bedrohung der militärischen Interessen. Gemäß dem Grundsatz der Verhältnismäßigkeit sollten Datenlokalisierungsauflagen, die aus Gründen der öffentlichen Sicherheit gerechtfertigt sind, zur Erreichung der damit verfolgten Ziele geeignet sein und nicht über das dafür Notwendige hinausgehen.

([1]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

([2]) Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I) (ABl. L 177 vom 4.7.2008, S. 6).

(20) Um die wirksame Anwendung des Grundsatzes des freien grenzüberschreitenden Verkehrs nicht-personenbezogener Daten sicherzustellen und das Entstehen neuer Hindernisse für ein reibungsloses Funktionieren des Binnenmarktes zu verhindern, sollten die Mitgliedstaaten der Kommission alle Entwürfe von Vorschriften umgehend mitteilen, die neue Datenlokalisierungsauflagen einführen oder bestehende Datenlokalisierungsauflagen ändern. Diese Entwürfe von Vorschriften sollten gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([1]) übermittelt und geprüft werden.

(21) Darüber hinaus sollten die Mitgliedstaaten zur Beseitigung möglicher bereits bestehender Hindernisse während eines Übergangszeitraums von 24 Monaten ab dem Zeitpunkt der Anwendung dieser Verordnung eine Überprüfung bestehender allgemeiner Rechts- und Verwaltungsvorschriften, in denen Datenlokalisierungsauflagen geregelt sind, durchführen und der Kommission sämtliche dieser Datenlokalisierungsauflagen, die sie für mit dieser Verordnung vereinbar halten, samt einer Begründung mitteilen. Damit sollte die Kommission in der Lage sein, die Rechtmäßigkeit etwaiger verbleibender Datenlokalsierungsauflagen zu prüfen. Die Kommission sollte gegebenenfalls in der Lage sein, dem betreffenden Mitgliedstaat Anmerkungen zu übermitteln. Solche Anmerkungen könnten eine Empfehlung enthalten, die Datenlokalisierungsauflage zu ändern oder aufzuheben.

(22) Die in dieser Verordnung geregelte Pflicht, der Kommission bestehende Datenlokalisierungsauflagen und Entwürfe von Vorschriften mitzuteilen, sollte für regulatorische Datenlokalisierungsauflagen und Entwürfe von Vorschriften allgemeiner Art gelten, nicht aber für Entscheidungen, die sich an bestimmte natürliche oder juristische Personen richten.

(23) Um sicherzustellen, dass durch Rechts- und Verwaltungsvorschriften geregelte Datenlokalisierungsauflagen in den Mitgliedstaaten für natürliche und juristische Personen, wie z. B. für Diensteanbieter und Nutzer von Datenverarbeitungsdiensten, transparent sind, sollten die Mitgliedstaaten die Informationen über solche Auflagen bei einer nationalen einheitlichen Online-Informationsstelle veröffentlichen und regelmäßig auf den neuesten Stand bringen. Alternativ sollten die Mitgliedstaaten einer zentralen Informationsstelle, die gemäß einem anderen Rechtsakt der Union eingerichtet wurde, aktuelle Informationen über solche Auflagen liefern. Um natürliche und juristische Personen angemessen über die in der Union bestehenden Datenlokalisierungsauflagen zu informieren, sollten die Mitgliedstaaten der Kommission die Adressen dieser einheitlichen Informationsstellen mitteilen. Die Kommission sollte diese Angaben zusammen mit einer regelmäßig aktualisierten konsolidierten Liste aller in den Mitgliedstaaten geltenden Datenlokalisierungsauflagen, einschließlich zusammenfassender Informationen über diese Auflagen, auf ihrer eigenen Website veröffentlichen.

(24) Datenlokalisierungsauflagen sind häufig auf ein mangelndes Vertrauen in eine grenzüberschreitende Datenverarbeitung zurückzuführen, weil angenommen wird, dass Daten den zuständigen Behörden der Mitgliedstaaten für deren Zwecke wie Überprüfungen und Audits zu Regulierungs- und Aufsichtszwecken nicht zur Verfügung stünden. Dieses mangelnde Vertrauen lässt sich nicht allein dadurch überwinden, dass Vertragsbestimmungen, mit denen der rechtmäßige Datenzugang der zuständigen Behörden in Ausübung ihrer amtlichen Pflichten unterbunden wird, für nichtig erklärt werden. Deshalb sollte diese Verordnung eindeutig festlegen, dass die Befugnisse der zuständigen Behörden, gemäß dem Unionsrecht oder nationalem Recht Zugang zu Daten zu verlangen oder zu erhalten, unberührt bleiben und dass den zuständigen Behörden der Zugang zu den Daten nicht mit der Begründung verweigert werden darf, dass die Daten in einem anderen Mitgliedstaat verarbeitet werden. Die zuständigen Behörden könnten funktionale Anforderungen festlegen, um den Datenzugang zu unterstützen, wie beispielsweise die Anforderung, dass Systembeschreibungen in dem betreffenden Mitgliedstaat aufbewahrt werden müssen.

(25) Natürliche oder juristische Personen, die verpflichtet sind, zuständigen Behörden Daten zur Verfügung zu stellen, können solchen Verpflichtungen dadurch nachkommen, dass sie den zuständigen Behörden einen wirksamen und zeitnahen elektronischen Zugang zu den Daten gewähren und garantieren, und zwar unabhängig von dem Mitgliedstaat, in dessen Gebiet die Daten verarbeitet werden. Ein solcher Zugang kann durch konkrete Geschäftsbestimmungen in Verträgen zwischen der natürlichen oder juristischen Person, die zur Zugangsgewährung verpflichtet ist, und dem Diensteanbieter gewährleistet werden.

(26) Kommt eine natürliche oder juristische Person, die zur Datenübermittlung verpflichtet ist, dieser Verpflichtung nicht nach, so sollte die zuständige Behörde die zuständigen Behörden in anderen Mitgliedstaaten um Amtshilfe ersuchen können. In solchen Fällen sollten die zuständigen Behörden die besonderen Instrumente der Zusammenarbeit nutzen, die je nach Sachlage im Unionsrecht oder in internationalen Abkommen etwa für den

([1]) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Bereich der polizeilichen Zusammenarbeit, der justiziellen Zusammenarbeit in Zivil- und Strafsachen oder der Zusammenarbeit in Verwaltungsangelegenheiten vorgesehen sind, z. B. im Rahmenbeschluss 2006/960/JI des Rates ([1]), der Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates ([2]), dem Übereinkommen des Europarats über Computerkriminalität ([3]), der Verordnung (EG) Nr. 1206/2001 des Rates ([4]), der Richtlinie 2006/112/EG des Rates ([5]) und der Verordnung (EU) Nr. 904/2010 des Rates ([6]). In Ermangelung solcher besonderen Kooperationsmechanismen sollten die zuständigen Behörden untereinander zusammenarbeiten, um den Zugang zu den gewünschten Daten über benannte einheitliche Anlaufstellen zu gewähren.

(27) Beinhaltet ein Amtshilfeersuchen die Erlangung des Zugangs zu Räumlichkeiten einer natürlichen oder juristischen Person, einschließlich Datenverarbeitungsanlagen und -mittel, durch die ersuchte Behörde, so muss ein solcher Zugang im Einklang mit dem Unionsrecht oder dem nationalen Verfahrensrecht stehen und unter anderem dem Erfordernis einer vorherigen richterlichen Genehmigung genügen.

(28) Diese Verordnung sollte Nutzern nicht den Versuch ermöglichen, geltendes nationales Recht zu umgehen. Deshalb sollte sie regeln, dass die Mitgliedstaaten wirksame, verhältnismäßige und abschreckende Sanktionen gegen Nutzer verhängen, die die zuständigen Behörden daran hindern, in Ausübung ihrer amtlichen Pflichten nach Unionsrecht und nach nationalem Recht auf ihre Daten zuzugreifen. In dringenden Fällen, in denen ein Nutzer sein Recht missbraucht, sollten die Mitgliedstaaten die Möglichkeit haben, strikt verhältnismäßige einstweilige Maßnahmen zu verhängen. Erfordern einstweilige Maßnahmen eine Relokalisierung von Daten über einen Zeitraum von mehr als 180 Tagen nach der Relokalisierung, so würde das bedeuten, dass über einen wesentlichen Zeitraum gegen den Grundsatz des freien Datenverkehrs verstoßen wird; deshalb sollten solche Maßnahmen der Kommission mitgeteilt werden, damit geprüft werden kann, ob sie mit dem Unionsrecht vereinbar sind.

(29) Die Möglichkeit der unbehinderten Übertragung von Daten ist ein Schlüsselfaktor, um die Auswahlmöglichkeiten der Nutzer und einen wirksamen Wettbewerb auf den Märkten der Datenverarbeitungsdienste zu fördern. Die tatsächlichen oder vermeintlichen Schwierigkeiten bei der grenzüberschreitenden Übertragung von Daten untergraben auch das Vertrauen beruflicher Nutzer in grenzüberschreitende Angebote und dadurch ihr Vertrauen in den Binnenmarkt. Während das geltende Unionsrecht einzelnen Verbraucher zugute kommt, wird es Nutzern, die im Rahmen ihres Gewerbes oder Berufes tätig werden, nicht erleichtert, die Möglichkeit des Wechsels zwischen Diensteanbietern in Anspruch zu nehmen. Einheitliche technische Anforderungen in der gesamten Union, sei es in Bezug auf technische Vereinheitlichung, gegenseitige Anerkennung oder freiwillige Vereinheitlichung, tragen ebenfalls zur Entwicklung eines wettbewerbsfähigen Binnenmarktes für Datenverarbeitungsdienste bei.

(30) Damit sie alle Vorteile des wettbewerbsorientierten Umfelds für sich nutzen können, sollten berufliche Nutzer in die Lage versetzt werden, sich sachkundig zu entscheiden und die einzelnen Bestandteile verschiedener Datenverarbeitungsdienste, die im Binnenmarkt angeboten werden, leicht zu vergleichen, auch bezüglich der Geschäftsbedingungen für die Übertragung von Daten bei Beendigung eines Vertrags. Um mit dem Innovationspotenzial des Marktes Schritt zu halten und die Erfahrungen und die Sachkenntnis der Diensteanbieter und beruflichen Nutzer von Datenverarbeitungsdiensten zu berücksichtigen, sollten die Einzelheiten und betrieblichen Anforderungen für die Übertragung von Daten von den Marktteilnehmern mittels Selbstregulierung festgelegt werden; die Kommission sollte die Selbstregulierung mit Verhaltensregeln der Union, die auch Mustergeschäftsbedingungen enthalten können, fördern, erleichtern und überwachen.

(31) Um wirksam zu sein und den Anbieterwechsel und die Datenübertragung einfacher zu machen, sollten solche Verhaltensregeln umfassend sein und mindestens die zentralen Aspekte, die beim Prozess der Datenübertragung wichtig sind, abdecken, wie die Prozesse, die für die Datensicherungen benutzt werden und den Ort der Datensicherung, die verfügbaren Datenformate und Datenträger, die erforderliche IT-Konfiguration und die Mindestnetzbandbreite, die Vorlaufzeit vor Beginn des Übertragungsprozesses und die Zeitspanne, in der die Daten für eine Übertragung verfügbar bleiben, sowie die Garantien für den Zugang zu den Daten im Falle der Insolvenz des Diensteanbieters. Aus den Verhaltensregeln sollte eindeutig hervorgehen, dass eine Anbieterabhängigkeit kein akzeptables Geschäftsgebaren ist; sie sollten vertrauensfördernde Technologien vorsehen und regelmäßig aktualisiert werden, um mit den technischen Entwicklungen Schritt zu halten. Die Kommission sollte dafür sorgen, dass alle relevanten Interessenträger, darunter Verbände von kleinen und mittelständischen Unternehmen (im Folgenden „KMU“) und Startups, Nutzer und Anbieter von Cloud-Diensten, in den Konsultationsprozess einbezogen werden. Die Kommission sollte die Entwicklung und die Wirksamkeit der Umsetzung solcher Verhaltensregeln evaluieren.

([1]) Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89).

([2]) Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (ABl. L 130 vom 1.5.2014, S. 1).

([3]) Übereinkommen des Europarats über Computerkriminalität, SEV-Nr. 185.

([4]) Verordnung (EG) Nr. 1206/2001 des Rates vom 28. Mai 2001 über die Zusammenarbeit zwischen den Gerichten der Mitgliedstaaten auf dem Gebiet der Beweisaufnahme in Zivil- oder Handelssachen (ABl. L 174 vom 27.6.2001, S. 1).

([5]) Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem (ABl. L 347 vom 11.12.2006, S. 1).

([6]) Verordnung (EU) Nr. 904/2010 des Rates vom 7. Oktober 2010 über die Zusammenarbeit der Verwaltungsbehörden und die Betrugsbekämpfung auf dem Gebiet der Mehrwertsteuer (ABl. L 268 vom 12.10.2010, S. 1).

(32) Wenn eine zuständige Behörde eines Mitgliedstaats einen anderen Mitgliedstaat um Amtshilfe ersucht, um gemäß dieser Verordnung Zugang zu Daten zu erlangen, so sollte sie über eine benannte einheitliche Anlaufstelle einen ordnungsgemäß begründeten Antrag an die einheitliche Anlaufstelle des betreffenden Mitgliedstaats richten, der eine schriftliche Darlegung der Gründe und der Rechtsgrundlagen für das Zugangsbegehren enthalten sollte. Die einheitliche Anlaufstelle, die vom Mitgliedstaat, um dessen Amtshilfe ersucht wird, benannt wurde, sollte die Übermittlung des Antrags an die jeweils zuständige Behörde in dem ersuchten Mitgliedstaat ermöglichen. Im Interesse einer wirksamen Zusammenarbeit sollte die Behörde, der ein Antrag zugeleitet wird, unverzüglich die beantrage Amtshilfe leisten oder mitteilen, welche Schwierigkeiten sie hatte, dem Antrag nachzukommen bzw. die Gründe nennen, warum sie den Antrag ablehnt.

(33) Durch die Stärkung des Vertrauens in eine grenzüberschreitende Datenverarbeitung sollte die Neigung von Marktteilnehmern und öffentlichen Stellen verringert werden, Datenlokalisierung stellvertretend für Datensicherheit zu verwenden. Außerdem sollten dadurch die Unternehmen mehr Rechtssicherheit in Bezug auf die Einhaltung anwendbarer Sicherheitsanforderungen erhalten, wenn sie ihre Datenverarbeitungstätigkeiten an Diensteanbieter, auch solche in anderen Mitgliedstaaten, auslagern.

(34) Bestehende Sicherheitsanforderungen an die Datenverarbeitung, die auf der Grundlage des Unionsrechts oder nationalen Rechts in begründeter und verhältnismäßiger Weise sowie im Einklang mit dem Unionsrecht in dem Mitgliedstaat gelten, in dem die natürlichen oder juristischen Personen, deren Daten betroffen sind, ihren Wohnsitz oder ihre Niederlassung haben, sollten auch auf die Verarbeitung dieser Daten in einem anderen Mitgliedstaat weiterhin Anwendung finden. Diese natürlichen oder juristischen Personen sollten derartige Anforderungen entweder selbst oder aber durch Vertragsklauseln in ihren Verträgen mit den Diensteanbietern erfüllen können.

(35) Auf nationaler Ebene festgelegte Sicherheitsanforderungen sollten notwendig sein und in einem angemessenen Verhältnis zu den Risiken für die Sicherheit der Datenverarbeitung stehen, für die das nationale Recht gilt, in dem diese Anforderungen festgelegt sind.

(36) Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates [1] enthält rechtliche Bestimmungen zur Anhebung des allgemeinen Niveaus der Cybersicherheit in der Union. Datenverarbeitungsdienste gehören zu den von dieser Richtlinie erfassten digitalen Diensten. Nach jener Richtlinie müssen die Mitgliedstaaten sicherstellen, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ermitteln und ergreifen, um die Risiken für die Sicherheit der von ihnen genutzten Netz- und Informationssysteme zu beherrschen. Diese Maßnahmen sollten ein dem Risiko angemessenes Schutzniveau gewährleisten und der Sicherheit der Systeme und Anlagen, der Bewältigung von Sicherheitsvorfällen, dem Betriebskontinuitätsmanagement, der Überwachung, Audits und Erprobung sowie der Einhaltung der internationalen Normen Rechnung tragen. Diese Elemente sollten von der Kommission in gemäß jener Richtlinie zu erlassenen Durchführungsrechtsakten weiter präzisiert werden.

(37) Die Kommission sollte einen Bericht über die Umsetzung dieser Verordnung vorlegen, um insbesondere festzustellen, ob angesichts der Entwicklung der Technologie und der Märkte Änderungsbedarf besteht. In diesem Bericht sollte insbesondere diese Verordnung, vor allem ihre Anwendung auf Datensätze, die aus personenbezogenen und nicht-personenbezogenen Daten bestehen, und die Anwendung der Ausnahme zugunsten der öffentlichen Sicherheit evaluiert werden. Bevor diese Verordnung Anwendung findet, sollte die Kommission zudem informierende Leitlinien darüber veröffentlichen, wie Datensätze, die sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen, zu behandeln sind, damit Unternehmen einschließlich KMU das Verhältnis zwischen dieser Verordnung und der Verordnung (EU) 2016/679 besser verstehen und um sicherzustellen, dass beide Verordnungen eingehalten werden.

(38) Diese Verordnung steht insbesondere mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen im Einklang und sollte in Übereinstimmung mit diesen Grundrechten und Grundsätzen ausgelegt und angewandt werden; dazu zählen die Rechte auf Schutz personenbezogener Daten, auf Freiheit der Meinungsäußerung und Informationsfreiheit und auf unternehmerische Freiheit.

(39) Da das Ziel dieser Verordnung, nämlich den freien Verkehr von Daten, die keine personenbezogenen Daten sind, in der Union zu gewährleisten, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das zur Verwirklichung dieses Ziels erforderliche Maß hinaus —

[1] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

Diese Verordnung zielt darauf ab, den freien Verkehr von Daten, die keine personenbezogenen Daten sind, in der Union zu gewährleisten, indem sie Vorschriften über Datenlokalisierungsauflagen, die Verfügbarkeit von Daten für zuständige Behörden und die Übertragung von Daten für berufliche Nutzer festlegt.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für die Verarbeitung elektronischer Daten, die keine personenbezogenen Daten sind, in der Union, die

a) als eine Dienstleistung für Nutzer erfolgt, die in der Union wohnhaft oder niedergelassen sind, ungeachtet dessen, ob der Diensteanbieter in der Union niedergelassen ist oder nicht; oder

b) von einer natürlichen oder juristischen Person, die in der Union wohnhaft oder niedergelassen ist, für ihren eigenen Bedarf durchgeführt wird.

(2) Bei einem Datensatz, der aus personenbezogenen und nicht-personenbezogenen Daten besteht, gilt diese Verordnung für die nicht-personenbezogenen Daten des Datensatzes. Sind personenbezogene und nicht-personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden, berührt diese Verordnung nicht die Anwendung der Verordnung (EU) 2016/679.

(3) Diese Verordnung gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen.

Diese Verordnung berührt nicht die Rechts- und Verwaltungsvorschriften, die sich auf die interne Organisation der Mitgliedstaten beziehen und die Behörden und Einrichtungen des öffentlichen Rechts im Sinne von Artikel 2 Absatz 1 Nummer 4 der Richtlinie 2014/24/EU die Befugnisse und Zuständigkeiten für die Datenverarbeitung ohne eine vertragliche Vergütung privater Parteien zuteilen, sowie die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die die Wahrnehmung dieser Befugnissen und Zuständigkeiten regeln.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Verordnung gelten folgende Begriffsbestimmungen:

1. „Daten“ bezeichnet Daten, die keine personenbezogenen Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 sind;
2. „Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Daten in elektronischer Form wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3. „Entwürfe von Vorschriften“ bezeichnet Texte, die entworfen worden sind, um sie als allgemeine Rechts- oder Verwaltungsvorschriften zu erlassen, und die sich im Stadium der Ausarbeitung befinden, in dem noch wesentliche Änderungen möglich sind;
4. „Diensteanbieter“ bezeichnet eine natürliche oder juristische Person, die Datenverarbeitungsdienste erbringt;
5. „Datenlokalisierungsauflage“ bezeichnet eine Verpflichtung, ein Verbot, eine Bedingung, eine Beschränkung oder eine andere Anforderung, die in Rechts- oder Verwaltungsvorschriften eines Mitgliedstaats enthalten ist oder sich aus allgemeinen und einheitlichen Verwaltungspraktiken in einem Mitgliedstaat und Einrichtungen des öffentlichen Rechts, unbeschadet der Richtlinie 2014/24/EU auch im Bereich der Vergabe öffentlicher Aufträge, ergibt und die bestimmt, dass die Datenverarbeitung im Hoheitsgebiet eines bestimmten Mitgliedstaats stattfinden muss, oder die die Verarbeitung von Daten in einem anderen Mitgliedstaat behindert;
6. „zuständige Behörde“ bezeichnet eine Behörde eines Mitgliedstaats oder eine andere nach nationalem Recht zur Wahrnehmung hoheitlicher Befugnisse oder zur Ausübung öffentlicher Gewalt ermächtigte Einrichtung, die nach Unionsrecht oder nach nationalem Recht befugt ist, zur Erfüllung ihrer amtlichen Pflichten Zugang zu Daten zu erlangen, die von einer natürlichen oder juristischen Person verarbeitet werden;
7. „Nutzer“ bezeichnet eine natürliche oder juristische Person einschließlich einer Behörde oder einer Einrichtung des öffentlichen Rechts, die einen Datenverarbeitungsdienst benutzt oder beauftragt;
8. „beruflicher Nutzer“ bezeichnet eine natürliche oder juristische Person, einschließlich einer Behörde oder einer Einrichtung des öffentlichen Rechts, die einen Datenverarbeitungsdienst im Zusammenhang mit ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit bzw. der Erfüllung ihrer Aufgaben benutzt oder beauftragt.

Artikel 4

Freier Datenverkehr in der Union

(1) Datenlokalisierungsauflagen sind unzulässig, es sei denn, sie sind aus Gründen der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit gerechtfertigt.

Absatz 3 und auf der Grundlage des bestehenden Unionsrechts festgelegte Datenlokalisierungsauflagen bleiben von Unterabsatz 1 dieses Absatzes unberührt.

(2) Die Mitgliedstaaten teilen der Kommission umgehend alle Entwürfe von Vorschriften mit, die neue Datenlokalisierungsauflagen enthalten oder bestehende Datenlokalisierungsauflagen ändern, gemäß den Verfahren, die in den Artikeln 5, 6 und 7 der Richtlinie (EU) 2015/1535 festgelegt sind.

(3) Die Mitgliedstaaten sorgen bis zum 30. Mai 2021 dafür, dass alle bestehenden Datenlokalisierungsauflagen, die durch allgemeine Rechts- und Verwaltungsvorschriften geregelt sind und die nicht mit Absatz 1 des vorliegenden Artikels vereinbar sind, aufgehoben werden.

Ist ein Mitgliedstaat der Ansicht, dass eine bestehende Maßnahme mit einer Datenlokalisierungsauflage mit Absatz 1 des vorliegenden Artikels vereinbar ist und deshalb in Kraft bleiben kann, teilt er der Kommission diese Maßnahme zusammen mit einer Begründung der Aufrechterhaltung bis zum 30. Mai 2021 mit. Unbeschadet Artikel 258 AEUV prüft die Kommission binnen sechs Monaten nach Eingang einer solchen Mitteilung, ob die betreffende Vorschrift mit Absatz 1 des vorliegenden Artikels vereinbar ist, und übermittelt dem betroffenen Mitgliedstaat gegebenenfalls Anmerkungen, gegebenenfalls einschließlich der Empfehlung, die Vorschrift zu ändern oder aufzuheben.

(4) Die Mitgliedstaaten machen die Einzelheiten sämtlicher in ihrem Hoheitsgebiet geltenden, durch allgemeine Rechts- oder Verwaltungsvorschriften geregelten Datenlokalisierungsauflagen über eine nationale einheitliche Online-Informationsstelle öffentlich verfügbar und halten diese Informationen auf dem neuesten Stand oder übermitteln aktualisierte Einzelheiten über alle derartigen Lokalisierungsauflagen an eine zentrale Informationsstelle, die gemäß einem anderen Unionsakt eingerichtet wurde.

(5) Die Mitgliedstaaten teilen der Kommission die Adresse ihrer in Absatz 4 genannten einheitlichen Informationsstelle mit. Die Kommission veröffentlicht die Verweise auf diese Stellen zusammen mit einer regelmäßig aktualisierten konsolidierten Liste aller Datenlokalisierungsauflagen gemäß Absatz 4, einschließlich zusammenfassender Informationen über diese Auflagen, auf ihrer Website.

Artikel 5

Verfügbarkeit von Daten für zuständige Behörden

(1) Diese Verordnung lässt die Befugnisse der zuständigen Behörden, zur Erfüllung ihrer amtlichen Pflichten, gemäß dem Unionsrecht oder nationalen Recht, Zugang zu Daten zu verlangen oder zu erhalten, unberührt. Der Zugang zuständiger Behörden zu Daten darf nicht mit der Begründung verweigert werden, dass die Daten in einem anderen Mitgliedstaat verarbeitet werden.

(2) Wird einer zuständigen Behörde, die um Zugang zu den Daten eines Nutzers ersucht hat, kein Zugang gewährt, so kann sie, sofern im Unionsrecht oder in internationalen Abkommen kein bestimmter Kooperationsmechanismus für den Datenaustausch zwischen den zuständigen Behörden verschiedener Mitgliedstaaten vorgesehen ist, eine zuständige Behörde in einem anderen Mitgliedstaat nach dem in Artikel 7 festgelegten Verfahren um Amtshilfe ersuchen.

(3) Beinhaltet ein Amtshilfeersuchen die Erlangung des Zugangs zu Räumlichkeiten einer natürlichen oder juristischen Person, einschließlich der Datenverarbeitungsanlagen und -mittel, durch die ersuchte Behörde, so muss ein solcher Zugang im Einklang mit dem Unionsrecht oder dem nationalen Verfahrensrecht stehen.

(4) Die Mitgliedstaaten können in Übereinstimmung mit dem Unionsrecht oder dem nationalen Recht wirksame, verhältnismäßige und abschreckende Sanktionen verhängen, wenn gegen eine Verpflichtung zur Bereitstellung von Daten verstoßen wird.

Im Falle von Rechtsmissbrauch durch einen Nutzer kann ein Mitgliedstaat, sofern dies durch die Dringlichkeit des Zugriffs auf die Daten und unter Berücksichtigung der Interessen der betroffenen Parteien gerechtfertigt ist, streng verhältnismäßige einstweilige Maßnahmen gegen diesen Nutzer ergreifen. Verfügt eine einstweilige Maßnahme die Relokalisierung von Daten, und dauert diese Relokalisierung länger als 180 Tage, ist dies der Kommission innerhalb dieser 180 Tage mitzuteilen. Die Kommission prüft die Maßnahme und beurteilt deren Vereinbarkeit mit dem Unionsrecht schnellstmöglich und trifft, soweit erforderlich, geeignete Maßnahmen. Die Kommission tauscht mit den in Artikel 7 genannten einheitlichen Anlaufstellen der Mitgliedstaaten Informationen über ihre Erfahrungen in dieser Hinsicht aus.

Artikel 6

Übertragung von Daten

(1) Die Kommission fördert und erleichtert die Entwicklung von Verhaltensregeln für die Selbstregulierung auf Unionsebene (im Folgenden „Verhaltensregeln"), um zu einer wettbewerbsfähigen Datenwirtschaft auf der Grundlage der Grundsätze der Transparenz und der Interoperabilität und unter angemessener Berücksichtigung offener Standards beizutragen, wobei unter anderem folgende Aspekte abgedeckt werden:

a) bewährte Verfahren zur Erleichterung des Wechsels des Diensteanbieters und der Übertragung von Daten in einem strukturierten, gängigen, maschinenlesbaren Format, bei Bedarf oder auf Wunsch des Diensteanbieters, der die Daten empfängt, auch in einem offenen Standardformat;

b) Vorschriften für Mindestangaben, damit sichergestellt ist, dass berufliche Nutzer vor dem Abschluss eines Datenverarbeitungsvertrags hinreichend genaue, klare und transparente Informationen in Bezug auf die Prozesse, technischen Anforderungen, Fristen und Entgelte erhalten, die für einen beruflichen Nutzer gelten, der zu einem anderen Diensteanbieter wechseln oder Daten in seine eigenen IT-Systeme zurückübertragen möchte;

c) Ansätze für Zertifizierungssysteme, mit denen der Vergleich von Datenverarbeitungsprodukten und -diensten für berufliche Nutzer erleichtert wird, unter Berücksichtigung bestehender nationaler oder internationaler Normen, zur Erleichterung der Vergleichbarkeit dieser Produkte und Dienste. Diese Ansätze können sich unter anderem auf das Qualitätsmanagement, das Informationssicherheitsmanagement, das Betriebskontinuitätsmanagement und das Umweltmanagement beziehen;

d) Kommunikationspläne mit multidisziplinärem Ansatz, um den relevanten Akteuren die Verhaltensregeln nahe zu bringen.

(2) Die Kommission stellt sicher, dass die Verhaltensregeln in enger Zusammenarbeit mit allen relevanten Interessenträgern, einschließlich KMU-Verbänden und Startups sowie Nutzern und Anbietern von Cloud-Diensten, entwickelt werden.

(3) Die Kommission hält die Diensteanbieter dazu an, die Entwicklung der Verhaltensregeln bis zum 29. November 2019 abzuschließen und sie bis zum 29. Mai 2020 wirksam umzusetzen.

Artikel 7

Verfahren für die Zusammenarbeit zwischen den Behörden

(1) Jeder Mitgliedstaat benennt eine einheitliche Anlaufstelle, die bezüglich der Anwendung dieser Verordnung mit den einheitlichen Anlaufstellen der anderen Mitgliedstaaten und mit der Kommission in Verbindung steht. Die Mitgliedstaaten teilen der Kommission die benannten einheitlichen Anlaufstellen und etwaige spätere Änderungen dieser Angaben mit.

(2) Wenn eine zuständige Behörde eines Mitgliedstaats einen anderen Mitgliedstaat gemäß Artikel 5 Absatz 2 um Amtshilfe ersucht, um Zugang zu Daten zu erlangen, so richtet sie einen ordnungsgemäß begründeten Antrag an die einheitliche Anlaufstelle des betreffenden Mitgliedstaats. Der Antrag enthält eine schriftliche Darlegung der Gründe und der Rechtsgrundlagen für das Zugangsbegehren.

(3) Die einheitliche Anlaufstelle ermittelt die jeweils zuständige Behörde ihres Mitgliedstaats und leitet den gemäß Absatz 2 erhaltenen Antrag an diese zuständige Behörde weiter.

(4) Die auf diese Weise ersuchte jeweilige zuständige Behörde muss ohne unangemessene Verzögerung und innerhalb einer der Dringlichkeit des Ersuchens entsprechenden Frist antworten und der nachsuchenden zuständigen Behörde die angeforderten Daten zur Verfügung stellen oder mitteilen, dass sie die Voraussetzungen für die Beantragung von Amtshilfe nach dieser Verordnung für nicht erfüllt hält.

(5) Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe gemäß Artikel 5 Absatz 2 ausgetauscht werden, dürfen nur im Zusammenhang mit den Zwecken des Ersuchens verwendet werden.

(6) Die einheitlichen Anlaufstellen müssen den Nutzern allgemeine Informationen über diese Verordnung bereitstellen, darunter Angaben zu den Verhaltensregeln.

Artikel 8

Bewertung und Leitlinien

(1) Die Kommission übermittelt dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss spätestens am 29. November 2022 einen Bericht über die Bewertung der Anwendung dieser Verordnung, insbesondere hinsichtlich

a) der Anwendung dieser Verordnung, insbesondere auf Datensätze, die aus personenbezogenen und nicht-personenbezogenen Daten bestehen, im Hinblick auf Entwicklungen der Märkte und technologische Entwicklungen, mit denen neue Möglichkeiten zur Entanonymisierung von Daten geschaffen werden könnten,

b) der Umsetzung von Artikel 4 Absatz 1 und insbesondere der Ausnahme aus Gründen der öffentlichen Sicherheit durch die Mitgliedstaaten und

c) der Aufstellung und wirksamen Umsetzung der Verhaltensregeln und der tatsächlichen Bereitstellung von Informationen durch Diensteanbieter.

(2) Die Mitgliedstaaten übermitteln der Kommission alle Informationen, die für die Ausarbeitung des in Absatz 1 genannten Berichts erforderlich sind.

(3) Bis zum 29. Mai 2019 veröffentlicht die Kommission informierende Leitlinien über die Wechselwirkungen der vorliegenden Verordnung und der Verordnung (EU) 2016/679, insbesondere im Hinblick auf Datensätze, die sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen.

Artikel 9

Schlussbestimmungen

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

Die Geltungsdauer dieser Verordnung beginnt sechs Monate nach ihrer Veröffentlichung.

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

Geschehen zu Straßburg am 14. November 2018.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
A. TAJANI	K. EDTSTADLER