Europäischer Wirtschafts- und Sozialausschuss

TEN/699
Leitlinien für den freien Verkehr nicht personenbezogener Daten

STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

Mitteilung der Kommission an das Europäische Parlament und den Rat – Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union
[COM(2019) 250 final]

Berichterstatterin: **Laure BATUT**

Befassung	Europäische Kommission, 22/07/2019
Rechtsgrundlage	Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	11/09/2019
Verabschiedung auf der Plenartagung	25/09/2019
Plenartagung Nr.	546
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	161/2/6

1. Empfehlungen

1.1 Der Europäische Wirtschafts- und Sozialausschuss (EWSA) empfiehlt der Kommission,

- in Bezug auf die Definitionskriterien für nicht-personenbezogene Daten und den Anwendungsbereich der Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten (im Folgenden: VO (EU) 2018/1807) eine einfache und klare Form der Kommunikation zu wählen, um Unsicherheiten zu beseitigen und das Vertrauen zu stärken;
- die einschlägigen Akteure auf Überschneidungen zwischen den EU-Datenrechtsvorschriften hinzuweisen;
- den freien Datenverkehr zu begünstigen und gleichzeitig dafür Sorge zu tragen, dass personenbezogene Daten nicht zunehmend als nicht personenbezogene Daten betrachtet werden, und sicherzustellen, dass der gesamte Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) erhalten bleibt, auch wenn dies mittelfristig eventuell darauf hinausläuft, die beiden Verordnungen im Sinne eines besseren Schutzes zusammenzufassen, um eine zunehmende Kommerzialisierung von Daten zu verhindern;
- die Errichtung und Entwicklung von Zusammenschlüssen europaweiter Cloud-Dienste zu fördern;
- die Europäerinnen und Europäer kurzfristig dabei zu unterstützen, die notwendigen Algorithmen für die Verarbeitung nicht-personenbezogener Massendaten im einheitlichen Datenmarkt zu nutzen; die Mitgliedstaaten dazu zu ermutigen, die Bildung im Bereich der Informationstechnologien (IT) und der künstlichen Intelligenz (KI) auf allen Ebenen (Schule, Hochschule, Arbeitswelt) lebensbegleitend auszubauen;
- die Akteure dazu anzuhalten, einen Geist der Verantwortung, des ethischen Bewusstseins und der Solidarität zu entwickeln und nicht zuzulassen, dass die Selbstregulierung und die gütliche Beilegung von Streitigkeiten zu unterschiedlichen Auslegungen der Texte führt;
- nicht zu zögern, auf Regulierungsinstrumente zurückzugreifen;
- Sanktionen für Verstöße gegen Verhaltensregeln zu unterstützen;
- einen Fahrplan auszuarbeiten, um zu prüfen, ob die Unternehmen im Zusammenhang mit der freien Nutzung ihrer Daten im Sinne der VO (EU) 2018/1807 tatsächlich über Rechtssicherheit verfügen;
- Bilanz der derzeitigen Lage in den 27 Mitgliedstaaten zu ziehen und die Arbeit der nationalen Anlaufstellen zu bewerten, sobald sie 12 Monate tätig waren;
- die ihr obliegenden Informations-, Kommunikations- und Frühwarnfunktionen umfassend wahrzunehmen;
- die Mitgliedstaaten aufzufordern, sich mit den Akteuren über ihre Kriterien für „öffentliche Sicherheit“ zu verständigen;
- die Mitgliedstaaten aufzufordern, ihre Speicherorte für nicht übertragbare Daten bekanntzugeben;
- die Wettbewerbspolitik rechtzeitig zu überprüfen, um sicherzustellen, dass sie in ihrer derzeitigen Form an den freien Datenverkehr angepasst ist.

2. **Einleitung**

2.1 Der EWSA nimmt die Absicht der Kommission zur Kenntnis, den Unternehmen, für die die Übertragung nicht-personenbezogener Daten relevant ist, Leitlinien an die Hand zu geben, bevor die Interessenträger dann im Lauf des Jahres 2020 Verhaltensregeln aushandeln. Da Datensätze häufig gemischt sind, d. h., sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen, ist es für Unternehmen nicht ohne weiteres klar, welche Datenschutzmaßnahmen zu ergreifen sind. Bevor der EWSA auf einzelne Aspekte der Mitteilung eingeht, möchte er zunächst die wesentlichen Grundsätze der geltenden Rechtsvorschriften Revue passieren lassen.

2.2 Die Kommission hat festgestellt, dass sich der mangelnde Wettbewerb zwischen den Cloud-Diensten in der EU und damit die mangelnde Datenmobilität in einem oligopolistischen Umfeld negativ auf den Datenmarkt ausgewirkt haben. Nach der VO (EU) 2018/1807 sind die Mitgliedstaaten gehalten, ihre Datenlokalisierungsauflagen so weit wie möglich einzuschränken und für möglichst einheitliche Rechtsvorschriften in diesem Bereich zu sorgen, um das Wachstum anzuregen und die Innovationskapazitäten der Unternehmen freizusetzen.

2.3 Mit der Annahme der Verordnung über den freien Verkehr nicht-personenbezogener Daten als Ergänzung zur DSGVO wird in den EU-Texten des 21. Jahrhunderts eine „fünfte Grundfreiheit“ geschaffen, die sich auf alle Daten erstreckt (Zitat: Anna-Maria Corazza Bildt, Mitglied des Europäischen Parlaments und Berichterstatterin). Dieses immaterielle Gut – wenn man es so bezeichnen kann – muss nach den Wünschen seiner Inhaber an Service-Provider/Hosting-Anbieter in anderen Ländern als dem EU-Land, in dem sie generiert und/oder genutzt wurden, zur Verwaltung übertragen werden können (Artikel 1 der VO (EU) 2018/1807). Auf diese Weise wird eine günstigere Situation für die Dateninhaber geschaffen und ihre Wettbewerbsposition gestärkt.

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten (VO (EU) 2018/1807)

2.4 Durch die Verordnung (EU) 2018/1807 wird der freie Verkehr nicht-personenbezogener Daten in der EU begünstigt, um die Weiterentwicklung der künstlichen Intelligenz, des Cloud-Computing und der Massendatenanalyse zu ermöglichen. Die Verordnung sieht vor (Artikel 6), dass die Kommission die Entwicklung von Verhaltensregeln für die Selbstregulierung auf Unionsebene durch die Akteure, die mit diesen nicht-personenbezogenen Daten arbeiten, steuert, fördert und erleichtert.

2.5 Die hier erörterte Mitteilung richtet sich an Fachleute aus Kleinstunternehmen und KMU und soll ihnen mithilfe von Leitlinien das Verständnis des Zusammenwirkens dieser Verordnung und der DSGVO erleichtern. Zur Veranschaulichung nennt die Kommission zahlreiche Fallbeispiele.

2.6 Die in Erarbeitung befindlichen Verhaltensregeln dürften zwischen November 2019 und Mai 2020 fertiggestellt werden (Erwägungsgründe 30 und 31, Artikel 6 Absatz 1). Bei ihrer Erarbeitung werden die Standpunkte aller Parteien berücksichtigt. Zwei öffentliche Anhörungen finden statt, und die Kommission wird durch zwei Arbeitsgruppen, die sich aus Fachleuten

zusammensetzen, unterstützt: Eine befasst sich mit der Cloud-Cybersicherheitszertifizierung (CSPCERT-Arbeitsgruppe) und eine weitere mit der Übertragung von Daten und dem Wechsel zwischen Cloud-Diensteanbietern (SWIPO-Arbeitsgruppe). Ihre Beiträge betreffen die Bereiche Infrastruktur als Dienstleistung (Infrastructure-as-a-Service – IaaS) und Software als Dienstleistung (Software-as-a-Service – SaaS). Im Mai 2020 wird die Kommission vorschlagen, die Industrie bei der Ausarbeitung von Standardvertragsklauseln zu unterstützen, und 2022 wird sie dem Europäischen Parlament, dem Rat und dem EWSA über die Anwendung der Verordnung Bericht erstatten, insbesondere in Bezug auf die Nutzung gemischter Daten.

3. Allgemeine Bemerkungen

3.1 Anliegen der Kommission: die Verordnung über den freien Verkehr nicht-personenbezogener Daten mit der Datenschutz-Grundverordnung in Einklang bringen

3.1.1 Um die beiden sich ergänzenden Verordnungen miteinander in Einklang zu bringen, erklärt die Kommission, dass 1) **Datenlokalisierungsauflagen von nun an verboten** sind; 2) die Daten für die **zuständigen Behörden** zugänglich bleiben; 3) die Daten mobil und mithin „übertragbar" werden. In der Datenschutz-Grundverordnung wird der Begriff „Übertragbarkeit" verwendet. In der VO (EU) 2018/1807 ist von „Übertragung" die Rede. Die Nutzer können ihre Daten aus dem Land der Generierung exportieren und sie nach Wechsel des Diensteanbieters ohne (größeren) Aufwand zwecks Speicherung, Verarbeitung oder Analyse zurückholen. Im Gegensatz zur „Übertragbarkeit", die ein Recht der Beteiligten ist, findet die „Übertragung" nach Verhaltensregeln und somit im Rahmen von Selbstregulierungsbemühungen statt.

3.1.2 Darin besteht ein wichtiger Unterschied zwischen den beiden Verordnungen: die eine stützt sich auf das **zwingende Recht**, die andere auf nicht rechtsverbindliche Instrumente (***soft law***), die bekanntlich wesentlich weniger Sicherheiten bieten. Wie die Kommission selbst feststellt, bestehen die meisten Datensätze sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten, die **untrennbar miteinander verbunden** sind, so dass sie als „gemischte" Datensätze zu betrachten sind.

3.1.3 Der EWSA begrüßt diesen unterstützenden Ansatz und stellt die gewählten Beispiele nicht infrage. Es ist nicht seine Aufgabe, weitere zu nennen. Er stellt jedoch fest, dass sich die Leitlinien der Kommission für die Akteure darauf beschränken, den Kontext anhand von Fallbeispielen zu veranschaulichen. Der EWSA möchte die Kommission jedoch warnend auf die kritischen Bereiche hinweisen, die den Nutzern seiner Ansicht nach trotz der Leitlinien und künftig vorliegenden Verhaltensregeln Schwierigkeiten bereiten könnten.

3.2 Grundsätze

3.2.1 Der Grundsatz des freien Datenverkehrs

Die Hindernisse für den freien Verkehr nicht-personenbezogener Daten sind weniger geografisch bedingt, sondern eher funktioneller Natur und/oder stehen im Zusammenhang mit den Mitteln, die den Unternehmen zur Nutzung der Informationstechnologien zur Verfügung stehen.

Nach der VO (EU) 2018/1807 sind Datenlokalisierungsauflagen für nicht-personenbezogene Daten in einem bestimmten Hoheitsgebiet unzulässig (Artikel 4). Die Mitgliedstaaten werden aufgefordert, alle anderslautenden Bestimmungen binnen 24 Monaten ab Inkrafttreten der Verordnung (Mai 2021) aufzuheben.

Ausnahmen aus Gründen der öffentlichen Sicherheit sind nach der Verordnung gestattet. Die Mitgliedstaaten müssen ausführliche Informationen über ihre Lokalisierungsauflagen auf nationaler Ebene online veröffentlichen. Die Europäische Kommission kann Anmerkungen formulieren und sie verlinkt die einschlägigen Websites der Mitgliedstaaten.

3.2.2 Ausnahmen vom Grundsatz des freien Datenverkehrs

- Die Behörden der Mitgliedstaaten können **auf die übermittelten Daten zugreifen**: Nach der VO (EU) 2018/1807 ist ein Verfahren vorgesehen, das es einer Aufsichtsbehörde eines Staates X erlaubt, die in einem Staat Y verarbeiteten Daten einzusehen. Ein Verfahren für eine zwischenstaatliche Zusammenarbeit ist vorgesehen (Artikel 5 und 7). Der EWSA hegt jedoch ernste Bedenken, dass bestimmte Daten (Buchführungs-, Finanz-, Vertragsdaten usw.) ohne Lokalisierung der Kontrolle durch die Aufsichtsbehörden der Mitgliedstaaten entgehen könnten. Er fordert die Kommission auf, nicht zu zögern, ggf. auf Regulierungsinstrumente zurückzugreifen.

- Die **einheitliche Anlaufstelle** des jeweiligen Mitgliedstaats bearbeitet den Antrag im Benehmen mit der einzelstaatlichen Aufsichtsbehörde, die über die Zulässigkeit des Antrags befindet und die Daten zur Verfügung stellen oder aber den Zugang verwehren kann. Im Geiste der VO (EU) 2018/1807 sollten die einheitlichen Anlaufstellen die Akteure dabei unterstützen, in der gesamten Union in voller Kenntnis der Sachlage und unter Wettbewerbsbedingungen über die Übertragung ihrer Daten zu entscheiden und ihre Diensteanbieter auszuwählen.

  Nach Auffassung des EWSA können die zahlreichen Unsicherheiten, die mit der Anwendung dieses Grundsatzes verbunden sind, nicht allein durch die Leitlinien beseitigt werden. Die Rechtfertigungsgründe der Mitgliedstaaten, der gute Glaube der Beteiligten und das reibungslose Funktionieren der Anlaufstellen sind schwierig zu beurteilen. Bewertungen in diesem Bereich dürften sich als problematisch erweisen.

- Verbot direkter oder indirekter Datenlokalisierungsauflagen, es sei denn sie sind aus Gründen der „öffentlichen Sicherheit“ gerechtfertigt. Der EWSA ist der Auffassung, dass der in der Verordnung verwendete Begriff der „öffentlichen Sicherheit“ nicht präzise genug ist, und fragt sich, was genau er, auf Datenverkehr und -kommerzialisierung bezogen, beinhaltet. In der VO (EU) 2018/1807 ist eine Datenlokalisierungsauflage definiert als „eine Verpflichtung, ein Verbot, eine Bedingung, eine Beschränkung oder eine andere Anforderung, die in Rechts- oder Verwaltungsvorschriften eines Mitgliedstaats enthalten ist oder sich aus [...] Verwaltungspraktiken [...] ergibt und die bestimmt, dass die Datenverarbeitung im Hoheitsgebiet eines bestimmten Mitgliedstaats stattfinden muss [...]“[1].

[1] Verordnung (EU) Nr. 1807/2018, Artikel 3 Absatz 5.

Im Sinne des Gerichtshofs der Europäischen Union (EuGH)2 (und laut Erwägungsgrund 19 der VO (EU) 2018/1807) bezieht sich der Begriff der öffentlichen Sicherheit „sowohl auf die innere als auch die äußere Sicherheit eines Mitgliedstaats“ und setzt das Bestehen „einer tatsächlichen erheblichen Gefahr voraus, die ein Grundinteresse der Gesellschaft berührt“. Diese Definition umfasst genetische Daten, biometrische Daten und Gesundheitsdaten. Die Reaktion des Mitgliedstaats muss verhältnismäßig sein.

3.2.3 Sowohl in Bezug auf den freien Datenverkehr als auch die Datenlokalisierung ist der EWSA der Ansicht, dass

- die verschiedenen Kriterien sehr unterschiedlich ausgelegt werden können;
- im Einzelfall eine gerichtliche Klärung notwendig ist, wodurch das nötige Vertrauen in den Handel beeinträchtigt werden kann, insbesondere bei sensiblen Daten; Streitigkeiten, die sich aus den Verhaltensregeln ergeben, könnten zu einer noch stärkeren Fragmentierung führen;
- die Uhren der Justiz ticken langsamer und können nicht mit dem Tempo von Digitalisierung und Datenverkehr mithalten.

Der EWSA ist der Meinung, dass die Unsicherheiten und die komplexe Sachlage für Kleinstunternehmen und KMU abschreckend sind.

3.2.4 Der EWSA stellt mit Bedauern fest, dass in den Leitlinien nicht darauf eingegangen wird, wie bei Rechtsstreitigkeiten vorzugehen ist und wie überprüft werden kann, ob die Mitgliedstaaten die Kriterien der öffentlichen Sicherheit einhalten und welche Sanktionen ggf. gegen sie verhängt werden könnten. Der EWSA fürchtet, dass der erläuternde Text der Mitteilung nicht ausreicht, um es den Akteuren der Kleinstunternehmen und der KMU zu ermöglichen, sämtliche rechtliche Hürden der Texte zu nehmen, und dass aufgrund der Unwägbarkeiten kein Gefühl des Vertrauens und der Rechtssicherheit entstehen kann, was für die Entwicklung des Sektors erforderlich ist.

3.2.5 Der EWSA erkennt an, dass es der Kommission mit der Mitteilung gelungen ist, umfassend und einem „Top-down“-Ansatz folgend über die durch die beiden Verordnungen bedingte Sachlage zu informieren. Die Mitteilung wird von Kleinstunternehmen und KMU dringend benötigt. Der EWSA spricht sich dafür aus, die Arbeit der nationalen Anlaufstellen und die Nutzung der entsprechenden Internetseiten der Kommission durch diese Akteure zu bewerten, sobald sie sechs Monate tätig waren, damit ggf. rasch Korrekturen vorgenommen werden können, wenn ein Mangel an Information und Kommunikation festzustellen ist.

---

2 Siehe Mitteilung COM(2019) 250 final, Fußnoten S. 11/12, sowie das Urteil in den Rechtssachen C-331/16 und C-366/16 K. gegen Staatssecretaris van Veiligheid en Justitie (C-331/16) und H. F. gegen Belgische Staat: „42. *Zum **Begriff der öffentlichen Sicherheit** geht aus der Rechtsprechung des Gerichtshofs hervor, dass er **sowohl die innere als auch die äußere Sicherheit eines Mitgliedstaats umfasst** (Urteil vom 23. November 2010, Tsakouridis, C-145/09, EU:C:2010:708, Rn. 43). Die innere Sicherheit kann insbesondere durch eine **unmittelbare Bedrohung der Ruhe und der physischen Sicherheit** der Bevölkerung des betreffenden Mitgliedstaats beeinträchtigt sein (vgl. in diesem Sinne Urteil vom 22. Mai 2012, I, C-348/09, EU:C:2012:300, Rn. 28).* Die äußere Sicherheit kann insbesondere durch die **Gefahr einer erheblichen Störung der auswärtigen Beziehungen dieses Mitgliedstaats** oder des friedlichen Zusammenlebens der Völker beeinträchtigt sein (vgl. in diesem Sinne Urteil vom 23. November 2010, Tsakouridis, C-145/09, EU:C:2010:708, Rn. 44).“

4. Besondere Bemerkungen

4.1 Zu den Daten

4.1.1 Nicht-personenbezogene Daten sind definitionsgemäß alle elektronischen Daten, die keine personenbezogenen Daten im Sinne der DSGVO sind. Dabei kann es sich um Handelsdaten handeln, um Präzisionslandwirtschafts-Daten, um Daten für die Wartung von Maschinen, um meteorologische Daten usw.

4.1.2 Die von öffentlichen Stellen wie Krankenhäusern, Sozialämtern oder Finanzämtern erhobenen Daten können in engem Zusammenhang mit personenbezogenen Daten von Patienten oder Steuerzahlern stehen. Unternehmen, die diese Daten nutzen, müssen sicherstellen, dass sie nicht bestimmten Personen zugeordnet oder nach ihrer Anonymisierung wieder deanonymisiert werden können. Unter Umständen sind die hierfür erforderlichen Verfahren für Kleinstunternehmen oder KMU zu zeit- und kostenintensiv. Der gesamte freie Datenverkehr in der EU wird durch die DSGVO und die Verordnung (EU) 2018/1807 geregelt. Wenn gemischte Daten „**untrennbar miteinander verbunden**“ sind, gelten für die betroffenen Datensätze die rechtlichen Schutzvorkehrungen der DSGVO (Erwägungsgrund 8 und Art. 2 Abs. 2 der Verordnung (EU) 2018/1807). Zur ersten Beschränkung des freien Verkehrs nicht-personenbezogener Daten im Zusammenhang mit der öffentlichen Sicherheit kommt somit eine weitere Beschränkung hinzu, die mit der Art der Daten an sich zusammenhängt. Das ist ein zentraler Aspekt der Mitteilung, in der mehrfach darauf hingewiesen wird, wie eng personenbezogene und nicht-personenbezogene Daten miteinander verknüpft sind: „Gemischte Datensätze [...] kommen [...] häufig vor“ (Mitteilung, Punkt 2.2); sie können „untrennbar miteinander verbunden“ sein (Punkt 2.2), wobei „[...] keine der beiden Verordnungen die Unternehmen dazu verpflichtet, die Datensätze [...] zu trennen“ (Punkt 2.2).

4.1.3 Es ist Sache des Unternehmens, zu beurteilen, ob die von ihm verarbeiteten nicht-personenbezogenen Daten mit personenbezogenen Daten „untrennbar verbunden“ sind, und wenn ja, sie zu schützen. Es ist keine leichte Aufgabe für ein Unternehmen, Daten für eine Weitergabe vorzubereiten. Eine allgemeine Definition gemischter Daten zu finden, scheint unmöglich, und die Überschneidungen zwischen den beiden Verordnungen dürften zu weiteren Interferenzen mit anderen Texten zum Datenrecht führen, wie beispielsweise zum geistigen Eigentum: nicht-personenbezogene Daten können frei fließen, wenn sie jedoch in einem Werk weiterverwendet werden, gelten andere Regeln. Nach Auffassung des EWSA wird es ein komplexes Spannungsfeld zwischen den verschiedenen Texten geben. In der Rechtsprechung wurde bereits gefordert, dass die untrennbare Verbindung anhand des Vernunftkriteriums beurteilt werden sollte. Der EWSA stellt fest, dass in der erörterten Mitteilung natürlich nicht alle Fälle zur Unterstützung der Akteure durchexerziert werden können und dass die Sachlage eher große Unternehmen begünstigt. Der EWSA empfiehlt der Kommission, dafür Sorge zu tragen, dass die personenbezogenen Daten in der Praxis nicht zunehmend als nicht-personenbezogene Daten betrachtet werden, und sicherzustellen, dass der gesamte Anwendungsbereich der DSGVO erhalten bleibt, auch wenn dies mittelfristig eventuell darauf hinausläuft, die beiden Verordnungen im Sinne eines besseren Schutzes zusammenzufassen, um eine zunehmende Kommerzialisierung von Daten zu verhindern.

4.2 **Zur Übertragbarkeit, Übertragung, Verarbeitung und Speicherung von Daten**

Nach der DSGVO ist die Übertragbarkeit durch die Verordnung geregelt (Artikel 20), nach der VO (EU) 2018/1807 unterliegt sie der Selbstregulierung. Der EWSA bedauert, dass Rechtsstreitigkeiten Tür und Tor geöffnet wird und beträchtliche Rechtsunsicherheit entstehen kann, die vor allem zu Lasten der Kleinstunternehmen und der KMU gehen dürfte. Er ist der Ansicht, dass nicht-personenbezogene Daten zwar immaterielle Güter sind, sie aber aufgrund ihres freien Verkehrs ein- und ausgeführt werden können. Vor diesem Hintergrund wäre eine Debatte über das Eigentum an solchen Daten von Interesse. Mehr als die Einzeldaten birgt jedoch die Datenmasse ein echtes Wertpotenzial. Der EWSA glaubt daher, dass die Wettbewerbspolitik unter Umständen nicht an diese Art von Markt angepasst ist. Er fragt sich, inwiefern die geschaffene Sachlage zur Steigerung der Produktivität von Kleinstunternehmen und KMU beitragen wird. Die Kommissionsmitteilung gibt ihnen diesbezüglich keinen Aufschluss.

4.3 **Zu den Diensteanbietern**

4.3.1 In der EU gibt es weder große Betreiber noch eine europäische Cloud, was der EWSA seit jeher bedauert. Die ständig anvisierten Skaleneffekte bleiben den US-amerikanischen IT-Giganten und einigen chinesischen Unternehmen vorbehalten. Selbst Ministerien der Mitgliedstaaten sind versucht, ihnen die Verwaltung ihrer Daten anzuvertrauen (Fall Frankreich).

4.3.2 Nach Auffassung des EWSA sollten in Europa Partner-Ökosysteme geschaffen und die Übertragung von Daten zwischen verschiedenen Plattformen vorgesehen werden. Über die Mitteilung hinaus könnte die Kommission die Kleinstunternehmen und KMU dabei unterstützen, entsprechende Ressourcen zu entwickeln, etwa nach dem Vorbild ihres 2018 aufgelegten Projekts eines Zusammenschlusses europaweiter Cloud-Dienste im Bereich der Erbringung wirtschaftlicher und nicht-wirtschaftlicher Dienstleistungen von allgemeinem Interesse (On-Demand-Dienst, Function as a Service (*FaaS*)). Auch das Netz digitaler Innovationszentren („*A network of Digital Innovation Hubs*“, web/Commission/DIHs/Januar 2019) geht in diese Richtung.

4.4 **Zur Datensicherheit**[3]

4.4.1 Auf interner Ebene überprüfen die nationalen Betreiber[4] die Art der Daten, die sie übertragen möchten, und sichern diese. Die Datenlokalisierungsauflagen entsprachen Sicherheitsvorschriften, die über das einzelstaatliche Recht überprüft werden konnten. Trotz der DSGVO und der VO (EU) 2018/1807 gibt es keine einheitlichen IT-Sicherheitsstandards in den verschiedenen EU-Mitgliedstaaten. Nach Ansicht des EWSA sollten den Kleinstunternehmen und den KMU sowie den privaten und öffentlichen Diensten in verschiedenen Sprachen fundierte diesbezügliche Informationen durch die nationalen Anlaufstellen zur Verfügung gestellt werden.

---

3 ABl. C 227 vom 28.6.2018, S. 86.

4 ABl. C 218 vom 23.7.2011, S. 130.

Auf externer Ebene könnte es dem EWSA zufolge Drittlands-Unternehmen schwer fallen, im Einklang mit den Verhaltensregeln Daten nach einer von ihren Inhabern erwünschten erneuten Weitergabe zurückzugeben. Er befürchtet, dass es langfristig schwierig werden könnte, die Zuständigkeiten auseinanderzuhalten.
Der EWSA empfiehlt der Kommission, die europäischen Akteure dahingehend zu unterstützen, dass sie kurzfristig in der Lage sein werden, die notwendigen Algorithmen für die Verarbeitung nicht-personenbezogener Massendaten im einheitlichen Datenmarkt zu nutzen.

4.4.2 Die Frage des Standorts und der Sicherheit der Server muss in den wirtschaftlichen und diplomatischen Verhandlungen zwischen den Staaten geklärt werden. Es handelt sich um eine entscheidende Frage. Zwar teilen sich die Mitgliedstaaten und die EU die Zuständigkeit für die Verwaltung der Daten, doch wäre es mit Blick auf die IT-Giganten und ihre jeweiligen Heimatstaaten durchaus riskant für die Mitgliedstaaten, jeder für sich verhandeln zu wollen.

4.4.3 Der EWSA empfiehlt der Kommission, ausführlichere Erklärungen zu den Verpflichtungen der Diensteanbieter hinsichtlich der Vorhaltung nicht-personenbezogener Daten, zu den angewandten Methoden, zu den Standorten und zur geplanten oder zulässigen Speicherdauer und zur Weiterverwendung nach der Verarbeitung zu liefern, denn diese Aspekte stehen in Verbindung mit der Datensicherheit und können für Unternehmen im internationalen Wettbewerb relevant sein.

4.5 Zu den Verhaltensregeln

4.5.1 Ab Mai 2019 sind die von der VO (EU) 2018/1807 betroffenen Akteure (vornehmlich Nutzer und Anbieter von Cloud-Computing-Diensten) dazu aufgerufen, binnen 12 Monaten ihre Verhaltensregeln auszuarbeiten. Laut Kommission sollten dabei bewährte Verfahren, Ansätze für Zertifizierungssysteme und Kommunikationspläne berücksichtigt werden. Die SWIPO-Arbeitsgruppe und die CSPCERT-Arbeitsgruppe bringen dabei ihren Sachverstand ein.

4.5.2 Die Kommission verweist auf das Vorgehen im Zusammenhang mit der DSGVO (Mitteilung, S. 20/21). Da diese der Stellungnahme des EDSA[5] unterliegt, kann sie als Bezugspunkt für die VO (EU) 2018/1807 dienen. Die Vertretungsverbände einer Branche können ihre Verhaltensregeln ausarbeiten. Die Verfasser müssen den zuständigen Behörden nachweisen, dass ihr Entwurf von Verhaltensregeln – unabhängig davon, ob er sich auf die nationale Ebene bezieht oder länderübergreifend ist – einem bestimmten Bedarf der Branche entspricht, die Anwendung der Verordnung erleichtert und wirksame Mechanismen zur Überprüfung der Einhaltung dieser Regeln vorsieht.

4.5.3 Bereits vor Inkrafttreten der DSGVO hatten die wichtigsten Anbieter von Infrastruktur als Dienstleistung (Infrastructure as a Service – *IaaS*) und Software als Dienstleistung (Software as a Service – *SaaS*) ihre eigenen Verhaltensregeln aufgestellt, um die Umsetzungsmodalitäten festzulegen und damit die von den Fachleuten[6] angemahnten Unsicherheiten zu beseitigen;

---

5 Europäischer Datenschutzausschuss (EDSA); Leitlinien 1/2019 über Verhaltensregeln, 12.2.2019: https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12019-codes-conduct-and-monitoring-bodies-under_de.

6 Anbieter von Cloud-Infrastruktur-Diensten in Europa (Cloud Infrastructure Services Providers in Europe – CISPE).

KMU wurden eingebunden, da davon ausgegangen wurde, dass die Selbstzertifizierung für viele KMU den hohen Kosten einer Zertifizierung vorzuziehen waren.

4.5.4 Der EWSA befürwortet einen sektorspezifischen Ansatz im Zusammenhang mit der VO (EU) 2018/1807, wenn ein Pauschalkonzept für alle nicht angemessen erscheint. Im Rahmen der DSGVO wurde eine nicht erschöpfende Liste von Punkten erstellt, die in den Verhaltensregeln behandelt werden könnten (Artikel 40 Absatz 2), insbesondere in Bezug auf faire und transparente Verfahren, Sicherheit bei der Datenübertragung und die Regelung von Streitigkeiten. In ihrem eigenen Interesse und zur Stärkung des Vertrauens der Verbraucher in den europäischen Ansatz müssen die Akteure angehalten werden, diese Punkte zu beherzigen und einen Geist der Verantwortung, des ethischen Bewusstseins und der Solidarität zu entwickeln, insbesondere durch Verhaltensregeln, in denen das Thema künstliche Intelligenz berücksichtigt wird. Auf diesen Punkt möchte der EWSA besonders hinweisen: Er empfiehlt der Kommission, nicht zuzulassen, dass die Selbstregulierung und die gütliche Beilegung von Streitigkeiten zu unterschiedlichen Auslegungen der Texte führt. Vielmehr sollte alles dafür getan werden, um sie zu vereinheitlichen, damit letztlich Regeln geschaffen werden, die auf alle anwendbar sind. Dies sollte auch in den Informations- und Kommunikationsbemühungen der Kommission zum Ausdruck kommen.

5. **Zur Bewertung**

Die Kommission wird eine regelmäßige Bewertung mit Blick auf die Auswirkungen auf den freien Datenverkehr, die Anwendung der Verordnung, die Aufhebung beschränkender Maßnahmen durch die Mitgliedstaaten und die Wirksamkeit der Verhaltensregeln vornehmen. Nach Meinung des EWSA sollten die Vertreter der Zivilgesellschaft aufgefordert werden, sich in diesem Zusammenhang zu äußern[7]. Damit gesellschaftsweit ein Gefühl der Sicherheit und somit Vertrauen in die neuen digitalen Praktiken entsteht, müssen sich die Union und die Mitgliedstaaten darum bemühen, die Unsicherheiten in Bezug auf das anwendbare Recht, die Vertraulichkeit, die verlustfreie Datenspeicherung und -wiederherstellung, die Garantien der Akteure betreffend Durchführbarkeit und guten Glauben sowie finanzielle Garantien auszuräumen. Die untrennbare Verbindung personenbezogener und nicht-personenbezogener Daten gibt Anlass zu Sorge, und angesichts ihres Anteils an der Gesamtheit der Datensätze fragt sich der EWSA, ob die Selbstregulierung wirklich der einzig gangbare Weg ist. Er empfiehlt, dass die Bestimmungen der DSGVO mittelfristig auf alle Daten und Datenbewegungen anwendbar sein sollten, mit einigen Ausnahmen betreffend „echte“ nicht-personenbezogene Daten.

Brüssel, den 25. September 2019

Luca JAHIER
Präsident des Europäischen Wirtschafts- und Sozialausschusses

*

* *

NB: Anhang auf den folgenden Seiten.

7 ABl. C 487 vom 28.12.2016, S. 92; ABl. C 62 vom 15.2.2019, S. 292.

ANHANG
zur Stellungnahme

Folgende abgelehnte Änderungsanträge erhielten mindestens ein Viertel der abgegebenen Stimmen (Art. 59 Abs. 3 der Geschäftsordnung):

Ziffer 4.1.3

Ändern:

Es ist Sache des Unternehmens, zu beurteilen, ob die von ihm verarbeiteten nicht-personenbezogenen Daten mit personenbezogenen Daten „untrennbar verbunden" sind, und wenn ja, sie zu schützen. Es ist keine leichte Aufgabe für ein Unternehmen, Daten für eine Weitergabe vorzubereiten. Eine allgemeine Definition gemischter Daten zu finden, scheint unmöglich, und die Überschneidungen zwischen den beiden Verordnungen dürften zu weiteren Interferenzen mit anderen Texten zum Datenrecht führen, wie beispielsweise zum geistigen Eigentum: nicht-personenbezogene Daten können frei fließen, wenn sie jedoch in einem Werk weiterverwendet werden, gelten andere Regeln. Nach Auffassung des EWSA wird es ein komplexes Spannungsfeld zwischen den verschiedenen Texten geben. In der Rechtsprechung wurde bereits gefordert, dass die untrennbare Verbindung anhand des Vernunftkriteriums beurteilt werden sollte. Der EWSA stellt fest, dass in der erörterten Mitteilung natürlich nicht alle Fälle zur Unterstützung der Akteure durchexerziert werden können und dass die Sachlage eher große Unternehmen begünstigt. Der EWSA empfiehlt der Kommission, dafür Sorge zu tragen, dass die personenbezogenen Daten in der Praxis nicht zunehmend als nicht-personenbezogene Daten betrachtet werden, und sicherzustellen, dass der gesamte Anwendungsbereich der DSGVO erhalten bleibt, ~~auch wenn dies mittelfristig eventuell darauf hinausläuft, die beiden Verordnungen im Sinne eines besseren Schutzes zusammenzufassen,~~ um einen besseren Schutz zu gewährleisten und eine zunehmende Kommerzialisierung von Daten zu verhindern.

Ziffer 5

Ändern:

Die Kommission wird eine regelmäßige Bewertung mit Blick auf die Auswirkungen auf den freien Datenverkehr, die Anwendung der Verordnung, die Aufhebung beschränkender Maßnahmen durch die Mitgliedstaaten und die Wirksamkeit der Verhaltensregeln vornehmen. Nach Meinung des EWSA sollten die Vertreter der Zivilgesellschaft aufgefordert werden, sich in diesem Zusammenhang zu äußern. Damit gesellschaftsweit ein Gefühl der Sicherheit und somit Vertrauen in die neuen digitalen Praktiken entsteht, müssen sich die Union und die Mitgliedstaaten darum bemühen, die Unsicherheiten in Bezug auf das anwendbare Recht, die Vertraulichkeit, die verlustfreie Datenspeicherung und -wiederherstellung, die Garantien der Akteure betreffend Durchführbarkeit und guten Glauben sowie finanzielle Garantien auszuräumen. Die untrennbare Verbindung personenbezogener und nicht-personenbezogener Daten gibt Anlass zu Sorge, und angesichts ihres Anteils an der Gesamtheit der Datensätze

fragt sich der EWSA, ob die Selbstregulierung wirklich der einzig gangbare Weg ist. ~~Er empfiehlt, dass die Bestimmungen der DSGVO mittelfristig auf alle Daten und Datenbewegungen anwendbar sein sollten, mit einigen Ausnahmen betreffend „echte" nicht-personenbezogene Daten.~~

Ziffer 1.1, dritter Spiegelstrich

Ändern:

Der Europäische Wirtschafts- und Sozialausschuss (EWSA) empfiehlt der Kommission,

……

- *den freien Datenverkehr zu begünstigen und gleichzeitig dafür Sorge zu tragen, dass personenbezogene Daten nicht zunehmend als nicht personenbezogene Daten betrachtet werden, und sicherzustellen, dass der gesamte Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) erhalten bleibt, ~~auch wenn dies mittelfristig eventuell darauf hinausläuft, die beiden Verordnungen im Sinne eines besseren Schutzes zusammenzufassen,~~ um <u>einen besseren Schutz zu gewährleisten und</u> eine zunehmende Kommerzialisierung von Daten zu verhindern;*

…….

Begründung

Die DSGVO und die VO (EU) 2018/1807 beruhen auf unterschiedlichen Rechtsgrundlagen, auf Artikel 16 AEUV über das Grundrecht jeder Person auf den Schutz ihrer personenbezogenen Daten bzw. Artikel 114 AEUV über die Angleichung der Rechts- und Verwaltungsvorschriften. Diese Artikel räumen der EU einen unterschiedlichen Handlungsspielraum im privatwirtschaftlichen Bereich ein (weshalb die EU mit der DSGVO sehr strenge und komplexe Vorschriften eingeführt hat und bei der VO (EU) 2018/1807 auf Selbstregulierung als am besten geeignetes und verhältnismäßiges Instrument setzt). Die beiden Instrumente lassen sich daher nicht in ein Rechtsinstrument zusammenfassen.

Ergebnis der Abstimmung über die Änderungsanträge:

Ja-Stimmen:	54
Nein-Stimmen:	84
Enthaltungen:	18