EU-Verordnung

FREIER VERKEHR NICHT-PERSONENBEZOGENER DATEN

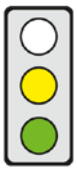
cep**Analyse** Nr. 33/2017

Centrum für Europäische Politik

KERNPUNKTE

Ziel der Verordnung: Die Kommission will den freien Verkehr nicht-personenbezogener Daten erleichtern und den Wettbewerb zwischen Cloud-Anbietern und anderen Datenverarbeitungsdiensten in der EU fördern.

Betroffene: Anbieter von Datenspeicherungs- und Datenverarbeitungsdiensten; Unternehmen, Behörden sowie private und berufliche Nutzer solcher Dienste.



Pro: (1) Das grundsätzliche Verbot nationaler „Datenlokalisierungsauflagen" fördert den grenzüberschreitenden Wettbewerb, wodurch die Preise für Cloud-Dienstleistungen sinken dürften.

(2) Die Nichteinführung eines gesetzlichen Anspruchs auf „Datenportabilität" für berufliche Nutzer ist sachgerecht.

Contra: (1) Es ist unverhältnismäßig, den Mitgliedstaaten per se eine Berufung auf alle anderen Rechtfertigungsgründe als die „öffentliche Sicherheit" zu versagen.

(2) Unverhältnismäßig ist auch, dass die Kommission die Rechtsform einer Verordnung statt einer Richtlinie als dem milderen Mittel gewählt hat.

Die wichtigsten Passagen im Text sind durch einen Seitenstrich gekennzeichnet.

INHALT

Titel

Vorschlag COM (2017) 495 vom 13. September 2017 für eine **Verordnung über** einen Rahmen für **den freien Verkehr nicht personenbezogener Daten** in der Europäischen Union

Kurzdarstellung

- **Hintergrund und Ziele**
  - Die Kommission will im Rahmen ihrer digitalen Binnenmarktstrategie [COM (2015) 192, s. cep**Analyse**] den freien Verkehr nicht-personenbezogener Daten in der EU verwirklichen und so insgesamt eine wettbewerbsorientierte europäische Datenwirtschaft schaffen (S. 4).
  - Die Verordnung ergänzt die Vorschriften für personenbezogene Daten (s. dazu cep**Studie**), u.a.
    - die Datenschutzgrundverordnung (EU) 2016/679 („DSGVO"; s. cep**Analyse**) und
    - die E-Datenschutz-Richtlinie 2002/58/EG, ggf. ersetzt durch die Verordnung [COM (2017) 10, s. cep**Analyse**].
  - Die Kommission will (S. 2 und 6, Erwägungsgrund 21)
    - den freien Verkehr nicht-personenbezogener Daten in der EU durch den Abbau von „Lokalisierungsbeschränkungen" verbessern und Rechtsunsicherheit beseitigen,
    - sicherstellen, dass Regulierungs- und Aufsichtsbehörden zu „ordnungspolitischen Kontrollzwecken" Zugang zu Daten behalten, auch wenn diese in anderen Mitgliedstaaten gespeichert werden, und
    - durch Förderung der Selbstregulierung „beruflichen Nutzern" von Datenspeicherungs- und Datenverarbeitungsdiensten den Anbieterwechsel und die Rückübertragung von Daten auf ihre eigenen IT-Systeme erleichtern und dadurch den Wettbewerb zwischen solchen Diensten verbessern.
- **Anwendungsbereich und Begriffsbestimmungen**
  - Die Verordnung gilt für Anbieter, die Datenspeicherungs- und Datenverarbeitungsdienste für in der EU wohnhafte oder niedergelassene Nutzer erbringen („Cloud-Anbieter"), soweit sie nicht-personenbezogene Daten verarbeiten. Ob der Anbieter einen Sitz in der EU hat, ist unerheblich. (Art. 2 Abs. 1 lit. a)
  - Die Verordnung gilt auch, wenn in der EU wohnhafte oder niedergelassene natürliche oder juristische Personen solche Daten für ihren „Eigenbedarf" speichern oder verarbeiten (Art. 2 Abs. 1 lit. b).
  - Nicht-personenbezogene „Daten" sind „andere" als „personenbezogene Daten" nach der DSGVO (Art. 3 Nr. 1 i.V.m Art. 4 Abs. 1 der DSGVO), d.h. alle Informationen, die sich nicht auf eine identifizierte oder auch nur indirekt identifizierbare natürliche Person.
  - Beispiele für nicht-personenbezogene Daten sind Daten aus Steuerunterlagen und Buchhaltung von Unternehmen, oder von Industrierobotern oder durch Sensoren ermittelte Werte ohne Personenbezug.
  - Die Verordnung gilt für jede vom Nutzer selbst vorgenommene oder an Cloud-Anbieter ausgelagerte Datenspeicherung oder -verarbeitung (Erwägungsgrund 11).
- **Abbau von „Datenlokalisierungsauflagen" (DLA)**
  - Die Verordnung verbietet alle „Datenlokalisierungsauflagen" (DLA), es sei denn, sie sind „aus Gründen der öffentlichen Sicherheit gerechtfertigt" und verhältnismäßig (Art. 4 Abs. 1, Art. 5 EUV, Erwägungsgrund 12).

Autoren: Dr. Anja Hoffmann, LL.M. Eur. und Philipp Eckhardt hoffmann@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-107 | www.cep.eu

– DLA sind nationale Rechts- oder Verwaltungsvorschriften, die (Art. 3 Nr. 5)
  - vorschreiben, dass Daten im eigenen Mitgliedstaat gespeichert oder verarbeitet werden müssen, oder
  - die Speicherung oder Verarbeitung von Daten in einem anderen Mitgliedstaat behindern, etwa durch die Pflicht, einen lokalen Anbieter zu nutzen oder eine Genehmigung einzuholen.
– Die Mitgliedstaaten müssen binnen 18 Monaten nach Veröffentlichung der Verordnung alle DLA aufheben oder gegenüber der Kommission begründen, welche DLA gerechtfertigt sind und demnach beibehalten werden sollen (Art. 4 Abs. 3, Art. 10 Abs. 2).
– Die Mitgliedstaaten dürfen sich zur Rechtfertigung nur auf die „öffentliche Sicherheit" und nicht auf andere Gründe wie die öffentliche Ordnung oder Gesundheit berufen (Art. 4 Abs. 1, Erwägungsgrund 12).
– Sie müssen der Kommission alle Entwürfe neuer oder geänderter DLA notifizieren (Art. 4 Abs. 2).
– Jeder Mitgliedstaat muss eine Website („zentrale Informationsstelle") mit den „Einzelheiten" über die geltenden DLA bereitstellen. Die Kommission verlinkt diese Seiten. (Art. 4 Abs. 4 und 5)

► **Verfügbarkeit der Daten für zuständige Behörden, Amtshilfe**
– Regulierungs- und Aufsichtsbehörden, die für amtliche Zwecke Zugang zu den Daten benötigen, behalten ihre Zugriffsrechte. Der Zugang darf ihnen nicht aus dem Grund versagt werden, dass die Daten in einem anderen Mitgliedstaat gespeichert oder verarbeitet werden. (Art. 5 Abs. 1, Erwägungsgrund 16)
– Wenn der zur Datenübermittlung verpflichtete Nutzer eines Cloud-Dienstes der Behörde keine Daten übermittelt oder ihr keinen Zugang gewährt, gilt:
  - Sieht das EU-Recht oder ein internationales Abkommen einen „besonderen Kooperationsmechanismus" für den Datenaustausch vor, muss die Behörde diesen nutzen (Art. 5 Abs. 4, Erwägungsgrund 18).
  - Greift kein „besonderer Kooperationsmechanismus" und hat die Behörde „alle anwendbaren Mittel" ausgeschöpft, muss die zuständige Behörde im Land des Speicherorts ihr auf Antrag Amtshilfe leisten, außer wenn dies der „öffentlichen Ordnung" in diesem Land zuwiderläuft (Art. 5 Abs. 2, S. 5).
– Die Mitgliedstaaten müssen „zentrale Anlaufstellen" einrichten, die die Amtshilfeanträge der ausländischen Behörden entgegennehmen und an die zuständige nationale Behörde weiterleiten (Art. 7 Abs. 1-4).

► **Erleichterte Datenübertragung für „berufliche Nutzer"**
– „Berufliche Nutzer" sind alle (Art. 3 Nr. 8)
  - natürlichen und juristischen Personen, die einen Datenspeicherungs- und Datenverarbeitungsdienst bei ihrer gewerblichen, geschäftlichen, handwerklichen oder sonstigen beruflichen Tätigkeit nutzen, sowie
  - öffentlichen Einrichtungen, die diese Dienste nutzen, um ihre Aufgaben zu erfüllen.
– Die Kommission fördert die Entwicklung EU-weit geltender Verhaltensregeln („Codes of Conduct") für Cloud-Dienste im Wege der Selbstregulierung (Art. 6 Abs. 1 lit. a, b). Berufliche Nutzer solcher Dienste sollen
  - einfacher den Anbieter wechseln können, indem „Leitlinien für bewährte Verfahren" entwickelt werden,
  - vorvertraglich über die Konditionen für den Wechsel zu einem anderen Cloud-Anbieter bzw. für die Rückübertragung gespeicherter Daten in die nutzereigenen IT-Systeme („Portabilität") informiert werden,
  - die Konditionen verschiedener Anbieter – etwa die technischen und betrieblichen Anforderungen, Prozesse, Fristen, Formate, Entgelte und Garantien bei Insolvenz – einfacher vergleichen können.
– Die Cloud-Anbieter sollen die Verhaltensregeln innerhalb von 18 Monaten nach Veröffentlichung der Verordnung im EU-Amtsblatt „wirksam umsetzen", was die Kommission überprüft (Art. 6 Abs. 2, 3).

Wesentliche Änderungen zum Status quo

► Der Grundsatz des freien Datenverkehrs wird erstmals auch für nicht-personenbezogene Daten geregelt. Bislang gab es keine expliziten EU-Vorgaben zum freien Verkehr dieser Daten und zum Abbau von DLA.

► Mitgliedstaaten können DLA nur noch aus Gründen der öffentlichen Sicherheit rechtfertigen. Auf andere Gründe wie die öffentliche Ordnung und Gesundheit dürfen sie sich nicht mehr berufen.

Subsidiaritätsbegründung der Kommission

Da das Kernproblem in der grenzüberschreitenden Datenmobilität liegt, können der freie Datenverkehr und der Binnenmarkt für die betroffenen Dienstleistungen nicht auf nationaler Ebene verwirklicht werden.

Politischer Kontext

Bereits in ihrer digitalen Binnenmarktstrategie [COM (2015) 192, S. 16f., s. cep**Analyse**] und deren Halbzeitüberprüfung [COM (2017) 228 final, S. 14] sowie in der Mitteilung „Aufbau einer europäischen Datenwirtschaft" [COM 2017(9), S. 8f.] kündigte die Kommission eine Initiative für den freien Verkehr nicht-personenbezogene Daten an.

Stand der Gesetzgebung

13.09.17 Annahme durch Kommission

Politische Einflussmöglichkeiten

Generaldirektionen:	GD Connect (Kommunikationsnetze, Inhalte und Technologien)
Ausschüsse des Europäischen Parlaments:	Binnenmarkt (federführend), Berichterstatterin: Anna Corazza Bildt, EVP
Bundesministerien:	Wirtschaft und Energie (BMWi) (federführend)
Ausschüsse des Deutschen Bundestags:	N.N.
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Unternehmen und Behörden in der EU sind heutzutage aufgrund nationaler DLA gezwungen, ihre Daten im Inland zu speichern und zu verarbeiten. Anbieter aus dem EU-Ausland werden so daran gehindert, ihre Dienste diesen Unternehmen und Behörden aus ihrem Herkunftsland heraus anzubieten. DLA führen daher dazu, dass Daten innerhalb der EU häufig nicht dort gespeichert und verarbeitet werden, wo dies am kostengünstigsten und effizientesten wäre. DLA können etwa verhindern, dass Daten in Mitgliedstaaten gespeichert und verarbeitet werden, in denen die zum Betrieb der Cloud-Server anfallenden Energiekosten gering sind, wie etwa in Schweden, Finnland oder Griechenland. In den nordeuropäischen Mitgliedstaaten ist die Speicherung und Verarbeitung auch aufgrund der klimatischen Bedingungen häufig zu geringeren Kosten möglich. Bei DLA in westeuropäischen Mitgliedstaaten fallen wiederum häufig hohe Lohnkosten an, die einen Großteil der Kosten bei diesen Dienstleistungen ausmachen und in einem osteuropäischen Mitgliedstaat deutlich geringer sind.

Das grundsätzliche Verbot nationaler DLA – außer aus Gründen der öffentlichen Sicherheit – stärkt daher den digitalen Binnenmarkt, sorgt für eine effizientere Allokation von Ressourcen und **fördert den grenzüberschreitenden Wettbewerb, wodurch auch die Preise für Cloud-Dienstleistungen sinken dürften.**

Ob der Vorstoß der Kommission Erfolg hat, hängt jedoch nicht allein von den Vorgaben dieser Verordnung ab. Denn nicht alle Barrieren für den grenzüberschreitenden Datenverkehr sind gesetzlicher Natur. Auch fehlt es an Vertrauen in die Datensicherheit und den Schutz von Geschäftsgeheimnissen im EU-Ausland. Dieses Vertrauen kann nicht allein durch legislative Maßnahmen der EU gewonnen werden, sondern erfordert auch vertrauensbildende Maßnahmen der Mitgliedstaaten und Anbieter selbst.

Die Nichteinführung eines gesetzlichen Anspruchs beruflicher Nutzer gegenüber ihren Cloud-Anbietern **auf Übertragung ihrer nicht-personenbezogenen Daten** – im Gegensatz zu personenbezogenen Daten (Art. 20 DSGVO) – **zu anderen Anbietern oder zurück in die eigenen IT-Systeme („Datenportabilität")** kommt darin zum Ausdruck, dass die Branche sich im Wege der Selbstregulierung Verhaltensregeln („Code of Conduct") auferlegen soll. Dies **ist sachgerecht.**

Zwar kann das Fehlen dieses Anspruchs es beruflichen Nutzern durchaus erschweren, den Anbieter zu wechseln oder die Daten wieder in die eigenen IT-Systeme zu übertragen (Lock-in-Effekt). Geht das fehlende Recht zur Portabilität auf vertragliche Vereinbarungen zwischen Nutzer und Anbieter zurück, besteht bei beruflichen Nutzern jedoch kein Schutzbedarf. Nicht nur kann solchen Nutzern eine rechtliche Prüfung vor Vertragsschluss zugemutet werden. Auch verhindert der Wettbewerb unter den Anbietern, dass diese ihren potentiellen Kunden Vertragsbestimmungen aufzwingen können. Soweit die fehlende Möglichkeit zur Datenportabilität technische Ursachen hat, ist ein gesetzlicher Portabilitätsanspruch ebenfalls nicht hilfreich. Denn er verringert die Anreize zur Entwicklung innovativer Dienste.

Juristische Bewertung

Kompetenz

Dass die Kommission die Verordnung auf die allgemeine Rechtsangleichungskompetenz im Binnenmarkt (Art. 114 AEUV) stützt, ist vertretbar. Die Verordnung soll durch den Abbau von Hindernissen (DLA) einen wirksam funktionierenden Binnenmarkt für Cloud-Dienstleistungen schaffen (S. 3, 4).

Subsidiarität

Unproblematisch. Grenzüberschreitende Datenmobilität kann die EU besser regeln als die Mitgliedstaaten.

Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Die Verordnung beschränkt die Möglichkeiten für Mitgliedstaaten, DLA zu rechtfertigen, indem sie nur noch die „öffentliche Sicherheit" als Rechtfertigungsgrund anerkennt. DLA bedürfen der Rechtfertigung, weil sie die Dienst- und Niederlassungsfreiheit von Cloud-Anbietern einschränken. Bislang dürfen sich die Mitgliedstaaten hierzu auch auf den Schutz der öffentlichen Ordnung und der Gesundheit oder auf andere zwingende Gründe des Allgemeinwohls berufen (vgl. etwa Art. 16 Abs. 1 lit. b der Dienstleistungsrichtlinie [2006/123/EG], Art. 3 Abs. 4 der E-Commerce-Richtlinie 2000/31/EG, Art. 49ff., 56 ff. AEUV).

Die geplante **Beschränkung der Rechtfertigungsgründe für DLA auf den Schutz der „öffentlichen Sicherheit" ist grundsätzlich zulässig, weil dadurch die Grundfreiheiten erweitert werden.** Die Mitgliedstaaten können durch ihre Beteiligung am Gesetzgebungsverfahren über den Rat ihre Handlungsspielräume selbstbestimmt einschränken (Müller-Graff in Streinz, EUV/AEUV, 2. Aufl. 2012, Art. 49 Rn. 44). Der Europäische Gerichtshof (EuGH) hat in Bezug auf die Dienstleistungsrichtlinie anerkannt, dass der EU-Gesetzgeber beim Erlass eines Sekundärrechtsakts, der eine im Primärrecht verankerte Grundfreiheit konkretisiert, die Rechtfertigungsgründe für freiheitsbeeinträchtigende Maßnahmen der Mitgliedstaaten beschränken kann: Der damit verfolgte Zweck, Beschränkungen, die das ordnungsgemäße Funktionieren des Binnenmarkts in gravierender Weise beeinträchtigen, systematisch und schnell zu beseitigen, stehe mit dem Primärrecht in Einklang (Rs. C-593/13, Rn. 39f.). Ist eine Maßnahme – etwa zum Schutz der öffentlichen Ordnung – sekundärrechtlich untersagt, kann sie nicht auf der Grundlage des Primärrechts gerechtfertigt werden, da dies die Harmonisierung untergraben würde (Rn. 37).

Es ist jedoch unverhältnismäßig, alle anderen Motive für den Erlass von DLA außer der „öffentlichen Sicherheit" **per se** für illegitim zu erklären und **den Mitgliedstaaten** so künftig von vornherein **eine Berufung auf alle anderen** anerkannten **Rechtfertigungsgründe** wie die öffentliche Ordnung, Gesundheit oder andere zwingende Gründe des Allgemeinwohls **zu versagen.** Es sollte den Mitgliedstaaten grundsätzlich vorbehalten bleiben, auch aus anderen legitimen Interessen ausnahmsweise eine Speicherung im Inland zu verlangen, sofern die damit verbundene Einschränkung der Grundfreiheiten zum Schutz dieses Interesses verhältnismäßig ist. **Das Verhältnismäßigkeitskriterium stellt insoweit eine ausreichende Schranken-Schranke dar**.

Die Pflicht der Mitgliedstaaten, der Kommission alle DLA schon im Entwurfsstadium zu notifizieren, schafft Transparenz und trägt dazu bei, langwierige und komplizierte Vertragsverletzungsverfahren zu vermeiden. Lässt man – wie oben favorisiert – weitere Rechtfertigungsmöglichkeiten für DLA zu, sollten die Mitgliedstaaten in ihrer „Begründung" für aufrechterhaltene DLA auch das legitime Ziel und die Verhältnismäßigkeit der DLA zu dessen Schutz hinreichend darlegen müssen.

Dass nationale Behörden künftig für den Datenzugriff ggf. auf Amtshilfe aus dem Land des Speicherorts angewiesen sind, kann zwar zu Verzögerungen beim behördlichen Datenzugriff führen. Dies ist aber im Hinblick auf die Vorteile einer freien Wahl des Speicherorts hinnehmbar, zumal die Amtshilferegelung nur subsidiär greift und nur begrenzten Verwaltungsaufwand erfordert. Der EuGH lässt bloße „verwaltungstechnische Nachteile" i.d.R. nicht zur Rechtfertigung ausreichen (siehe z.B. Rs. C-386/04-Stauffer, Rn. 49, 51). **Klargestellt werden muss** aber**, ob Behörden die Amtshilfe** nach dieser Verordnung **auch** dann **nutzen dürfen, wenn** vorhandene **vorrangige Kooperationsmechanismen scheitern** oder stocken, **und wie sie den Zugriff** ggf. **durchsetzen können.** Zudem sollte der Begriff der „Datenverarbeitung" definiert werden.

Unverhältnismäßig ist, dass die Kommission die Rechtsform einer Verordnung gewählt hat (Art. 5 Abs. 4 EUV). Hinreichende Rechtssicherheit kann auch durch eine Richtlinie geschaffen werden, in der der Grundsatz des freien Datenverkehrs und die geplanten Pflichten für die Mitgliedstaaten klar geregelt werden. Diesen verbliebe dann z.B. bei der Schaffung der Verwaltungsstrukturen für die Amtshilfe mehr Umsetzungsspielraum.

Sonstige Vereinbarkeit mit EU-Recht

Durch die Definition nicht-personenbezogener „Daten" als „andere" als personenbezogenen Daten werden Überlappungen mit der DSGVO sinnvollerweise vermieden. Die Abgrenzung zwischen personenbezogenen und nicht-personen-bezogenen Daten kann jedoch im Einzelfall schwierig sein, zumal aus anonymisierten Daten wieder personenbezogene Daten entstehen können, weil die Daten später doch re-identifiziert oder mit anderen Daten gekoppelt werden. Klargestellt werden muss, welche Regeln für gemischte Datensätze gelten, bei denen personenbezogene und nicht-personenbezogene Daten nicht ohne Aufwand getrennt werden können.

Auswirkungen auf das deutsche Recht

Deutschland muss alle in deutschen Rechts- oder Verwaltungsvorschriften enthaltenen DLA innerhalb von 18 Monaten nach Veröffentlichung der Verordnung aufheben oder gegenüber der Kommission rechtfertigen. Überprüft werden müssen u.a. die steuer- und handelsrechtlichen Buchführungs- und Aufbewahrungspflichten, soweit sie die Datenspeicherung im Ausland an Bewilligungen oder Bedingungen knüpfen, wie etwa § 146 Abs. 2 AO, § 14b Abs. 2 UStG und § 41 Abs. 1 EStG. Gleiches gilt für Pflichten zur Nutzung lokaler Provider wie in Art. 7 des Bayerischen Ausführungsgesetzes zum Personenstandsgesetz.

Zusammenfassung der Bewertung

Das grundsätzliche Verbot nationaler DLA fördert den grenzüberschreitenden Wettbewerb, wodurch die Preise für Cloud-Dienstleistungen sinken dürften. Die Nichteinführung eines gesetzlichen Anspruchs beruflicher Nutzer auf Übertragung ihrer nicht-personenbezogenen Daten zu anderen Anbietern oder zurück in die eigenen IT-Systeme („Datenportabilität") ist sachgerecht. Die Beschränkung der Rechtfertigungsgründe für DLA auf den Schutz der „öffentlichen Sicherheit" ist grundsätzlich zulässig, weil dadurch die Grundfreiheiten erweitert werden. Es ist unverhältnismäßig, den Mitgliedstaaten eine Berufung auf alle anderen Rechtfertigungsgründe zu versagen. Das Verhältnismäßigkeitskriterium stellt insoweit eine ausreichende Schranken-Schranke dar. Klargestellt werden muss, ob Behörden die Amtshilfe auch nutzen dürfen, wenn vorrangige Kooperationsmechanismen scheitern. Unverhältnismäßig ist, dass die Kommission die Rechtsform einer Verordnung gewählt hat.