EUROPÄISCHE
KOMMISSION

Brüssel, den 29.5.2019
COM(2019) 250 final

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

Inhaltsverzeichnis

Dieses Dokument wird von der Europäischen Kommission lediglich zu Informationszwecken bereitgestellt. Es enthält keine verbindliche Auslegung der 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 und stellt keinen Beschluss oder Standpunkt der Europäischen Kommission dar. Das Dokument lässt jeden solchen Beschluss oder Standpunkt der Europäischen Kommission sowie die Befugnisse des Gerichtshofs der Europäischen Union zur Auslegung der Verordnung in Übereinstimmung mit den EU-Verträgen unberührt.

1. Einführung

In einer zunehmend datengesteuerten Wirtschaft stehen die Datenströme im Mittelpunkt von Geschäftsprozessen in Unternehmen jeder Größe und in allen Wirtschaftszweigen. Neue digitale Technologien eröffnen der breiten Öffentlichkeit, den Unternehmen und den öffentlichen Verwaltungen in der Europäischen Union (EU) neue Möglichkeiten.

Um den grenzüberschreitenden Austausch von Daten weiter zu verbessern und die Datenwirtschaft anzukurbeln, haben das Europäische Parlament und der Rat im November 2018 auf der Grundlage eines Vorschlags der Europäischen Kommission (im Folgenden „Kommission“) die Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union[1] (im Folgenden „Verordnung über den freien Verkehr nicht-personenbezogener Daten“) angenommen. Die Verordnung gilt ab dem 28. Mai 2019. Der Grundsatz des freien Verkehrs personenbezogener Daten ist bereits in der Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG[2] (im Folgenden „Datenschutz-Grundverordnung“) festgelegt. Daher gibt es nun einen umfassenden Rahmen für einen gemeinsamen europäischen Datenraum und den freien Verkehr aller Daten innerhalb der Europäischen Union.[3]

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten schafft Rechtssicherheit für Unternehmen, die ihre Daten nun überall in der EU verarbeiten können, erhöht das Vertrauen in Datenverarbeitungsdienste und tritt der Anbieterabhängigkeit (*vendor lock-in*) entgegen. Dadurch erhalten Kunden mehr Auswahl, die Effizienz wird verbessert und es werden Anreize für die Verwendung von Cloud-Technologien geboten, was zu erheblichen Einsparungen für Unternehmen in der EU führen wird. Einer Studie zufolge können Unternehmen in der EU 20-50 % ihrer IT-Kosten durch Migration zur Cloud einsparen.[4]

Dank der beiden Verordnungen ist der freie Datenverkehr zwischen den Mitgliedstaaten sichergestellt, sodass die Nutzer von Datenverarbeitungsdiensten mit den in verschiedenen EU-Märkten gesammelten Daten ihre Produktivität und Wettbewerbsfähigkeit verbessern können. Somit lassen sich die Größenvorteile des großen EU-Marktes vollumfänglich nutzen, was die globale Wettbewerbsfähigkeit der Nutzer und die Vernetzung der europäischen Datenwirtschaft verbessert.

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten weist drei besondere Merkmale auf:

- Sie verbietet den Mitgliedstaaten grundsätzlich die Anwendung von Datenlokalisierungsauflagen. Ausnahmen hiervon sind nur aus Gründen der öffentlichen Sicherheit im Einklang mit dem Grundsatz der Verhältnismäßigkeit zulässig.

---

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

[2] 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).

[3] Die Datenschutz-Grundverordnung gilt auch für den Europäischen Wirtschaftsraum (EWR), dem Island, Liechtenstein und Norwegen angehören. Darüber hinaus ist die Verordnung über den freien Verkehr nicht-personenbezogener Daten von Bedeutung für den EWR.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe* (Messung der wirtschaftlichen Auswirkungen des Cloud-Computing in Europa), SMART 2014/0031, 2016. Online abrufbar unter: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Sie sieht einen Kooperationsmechanismus vor, der sicherstellen soll, dass die zuständigen Behörden weiterhin in der Lage sind, ihr Recht auf Zugang zu Daten, die in einem anderen Mitgliedstaat verarbeitet werden, auszuüben.
- Sie gibt den Unternehmen der Branche Anreize, mit Unterstützung der Kommission Verhaltensregeln für die Selbstregulierung im Hinblick auf den Anbieterwechsel und die Übertragung von Daten auszuarbeiten.

Zweck dieser Leitlinien

Mit diesen Leitlinien kommt die Kommission ihrer Verpflichtung aus Artikel 8 Absatz 3 der Verordnung über den freien Verkehr nicht-personenbezogener Daten nach, Leitlinien über das Zusammenwirken dieser Verordnung und der Datenschutz-Grundverordnung zu veröffentlichen, „insbesondere im Hinblick auf Datensätze, die sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen".

Die Leitlinien sollen den Nutzern – insbesondere kleinen und mittleren Unternehmen – helfen, das Verhältnis zwischen der Verordnung über den freien Verkehr nicht-personenbezogener Daten und der Datenschutz-Grundverordnung besser zu verstehen.[5] Sie gehen daher insbesondere auf folgende Aspekte ein: i) die Begriffe „nicht-personenbezogene Daten" und „personenbezogene Daten", ii) die Grundsätze des freien Datenverkehrs und das Verbot von Datenlokalisierungsauflagen nach beiden Verordnungen und iii) den Begriff der Übertragung bzw. Übertragbarkeit von Daten nach der Verordnung über den freien Verkehr nicht-personenbezogener Daten. Sie decken zudem die in den beiden Verordnungen festgelegten Anforderungen an die Selbstregulierung ab.

Der Verordnung über den freien Verkehr nicht-personenbezogener Daten unterliegen nur „Daten, die keine personenbezogenen Daten" im Sinne der Datenschutz-Grundverordnung sind. Die Datenschutz-Grundverordnung regelt die Verarbeitung personenbezogener Daten, die ein wesentlicher Bestandteil des Datenschutzrahmens der EU[6] ist. Sie trat in den Mitgliedstaaten am 25. Mai 2018 in Kraft. In der Verordnung werden harmonisierte Vorschriften zum Schutz von Personen in der EU und im EWR im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten und den freien Datenverkehr festgelegt. Die Datenschutz-Grundverordnung i) präzisiert, welche Informationen personenbezogene Daten darstellen, ii) legt die Rechtsgrundlage für ihre Verarbeitung fest und iii) definiert unter

---

[5] Erwägungsgrund 37 der 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.

[6]
- 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).
- Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).
- 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).
- 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) – wird derzeit überarbeitet.

anderem die Rechte und Pflichten, die bei der Verarbeitung dieser Daten zu beachten sind.[7] In Bezug auf den Grundsatz des freien Verkehrs personenbezogener Daten heißt es in Artikel 1 Absatz 3 der Datenschutz-Grundverordnung: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden."

In den meisten realen Situationen dürfte ein Datensatz sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten bestehen. In diesem Zusammenhang spricht man häufig von einem „gemischten Datensatz". Im nachstehenden Abschnitt 2.2 wird das Zusammenwirken der Verordnung über den freien Verkehr nicht-personenbezogener Daten und der Datenschutz-Grundverordnung in Bezug auf gemischte Datensätze näher erläutert.

Im Interesse der Klarheit sei betont, dass keine widersprüchlichen Verpflichtungen nach der Datenschutz-Grundverordnung und der Verordnung über den freien Verkehr nicht-personenbezogener Daten bestehen.

2. Zusammenwirken der Verordnung über den freien Verkehr nicht-personenbezogener Daten und der Datenschutz-Grundverordnung hinsichtlich gemischter Datensätze

2.1 Der Begriff „nicht-personenbezogene Daten" in der Verordnung über den freien Verkehr nicht-personenbezogener Daten

Mit der Verordnung über den freien Datenverkehr nicht-personenbezogener Daten[8] soll der freie Verkehr von Daten, die keine personenbezogenen Daten sind, gewährleistet werden. In der gesamten Verordnung wird der Begriff „Daten" im Sinne von „Daten, die keine personenbezogenen Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 sind"[9] verwendet. Diese Daten, hier auch als „**nicht-personenbezogene Daten**" bezeichnet, werden in Abgrenzung zu personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung definiert.

Personenbezogene Daten

Laut Datenschutz-Grundverordnung „bezeichnet der Ausdruck „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person

---

[7] Weitere Informationen zu verschiedenen Aspekten der 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) und des Europäischen Datenschutzrechts sind auf der Website des Europäischen Datenschutzausschusses, der nach Artikel 70 der Datenschutz-Grundverordnung eine Reihe von Leitlinien herausgegeben hat, abrufbar unter: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Auf der entsprechenden Website finden sich auch Hinweise auf Leitlinien, Empfehlungen und andere Dokumente, die von der Vorgängerin des Europäischen Datenschutzausschusses, der Artikel-29-Datenschutzgruppe, herausgegeben wurden. Um Bürger und Unternehmen für die 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) zu sensibilisieren, hat die Kommission außerdem eine Mitteilung mit dem Titel „Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Geltung der Datenschutz-Grundverordnung ab 25. Mai 2018" (COM(2018) 43 final/2) veröffentlicht, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1517578296944&uri=CELEX:52018DC0043R(01).

[8] Artikel 1 der 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.

[9] Siehe Artikel 3 Nummer 1 der 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.

angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann".

Die weit gefasste Definition personenbezogener Daten in der Datenschutz-Grundverordnung ist beabsichtigt und im Vergleich zu früheren Rechtsvorschriften im Wesentlichen unverändert geblieben[10]. Verschiedene Aspekte dieser Definition wie „alle Informationen", „die sich auf ... beziehen" und „identifizierte oder identifizierbare" wurden bereits von der Artikel-19-Datenschutzgruppe[11] in ihrer Stellungnahme 4/2007 vom 20. Juni 2007 zum Begriff der personenbezogenen Daten (WP 136) behandelt.

In Bereichen wie der Forschung ist es gängige Praxis, personenbezogene Daten zu pseudonymisieren, um die Identität einer Person zu verschleiern. **Pseudonymisierung** bedeutet die Verarbeitung personenbezogener Daten in einer Weise, die es unmöglich macht, diese Daten ohne zusätzliche Informationen einer bestimmten Person zuzuordnen. Diese zusätzlichen Informationen werden getrennt aufbewahrt und durch organisatorische oder technische Maßnahmen (z. B. Verschlüsselung) gesichert[12,13]. Derart pseudonymisierte Daten gelten jedoch weiterhin als Informationen über eine identifizierbare Person, wenn sie dieser Person durch Verwendung zusätzlicher Informationen zugeordnet werden können.[14] Somit **stellen sie personenbezogene Daten** im Einklang mit der Datenschutz-Grundverordnung **dar**.

Nicht-personenbezogene Daten

Handelt es sich bei Daten um keine „personenbezogenen Daten" im Sinne der Datenschutz-Grundverordnung, so sind sie als **nicht-personenbezogen** anzusehen. Nicht-personenbezogene Daten lassen sich je nach Herkunft klassifizieren als

- Daten, die sich ursprünglich nicht auf eine identifizierte oder identifizierbare natürliche Person bezogen, z. B. Daten über Wetterbedingungen, die von Sensoren generiert werden,

---

[10] Siehe Artikel 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (gültig bis 24. Mai 2018, aufgehoben durch die Datenschutz-Grundverordnung). Siehe auch die Rechtsprechung des Gerichtshofs zur Definition personenbezogener Daten, in der die weite Auslegung dieses Begriffs anerkannt wird, z. B.: Urteil des Gerichtshofs vom 29. Januar 2009, Productores de Música de España (Promusicae) gegen Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54; Urteil des Gerichtshofs vom 24. November 2011, Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, ECLI:EU:C:2011:771; Urteil des Gerichtshofs vom 19. Oktober 2016, Patrick Breyer gegen Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779.

[11] Die Artikel-29-Datenschutzgruppe war ein beratendes Gremium, das der Kommission beratend zur Seite stand und die Kommission bei der Entwicklung einer harmonisierten Datenschutzpolitik in der EU unterstützte. Nach dem Inkrafttreten der Datenschutz-Grundverordnung am 25. Mai 2018 wurde die Artikel-29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss abgelöst.

[12] Siehe Artikel 4 Nummer 5 der 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), in dem der Begriff „Pseudonymisierung" definiert wird.

[13] So gälte beispielsweise eine Forschungsstudie über die Wirkungen eines neuen Arzneimittels als Pseudonymisierung, wenn die personenbezogenen Daten der Studienteilnehmer durch einzigartige Merkmale (z. B. Nummer oder Code) in der Forschungsdokumentation ersetzt und ihre personenbezogenen Daten separat mit den zugewiesenen einzigartigen Merkmalen in einem gesicherten Dokument (z. B. in einer passwortgeschützten Datenbank) aufbewahrt würden.

[14] Siehe Erwägungsgrund 26 der 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).

die auf Windturbinen installiert sind, oder Daten über den Wartungsbedarf industrieller Maschinen;

- Daten, die ursprünglich personenbezogene Daten waren, später jedoch **anonymisiert**[15] wurden. Die „Anonymisierung" personenbezogener Daten unterscheidet sich von der Pseudonymisierung (siehe oben), denn ordnungsgemäß anonymisierte Daten können nicht einmal durch die Verwendung zusätzlicher Daten[16] einer bestimmten Person zugeordnet werden und sind daher nicht-personenbezogene Daten.

Die Bewertung, ob Daten ordnungsgemäß anonymisiert werden, hängt von den besonderen einzigartigen Umständen jedes Einzelfalls ab.[17] Mehrere Beispiele für die erneute Identifizierung vermeintlich anonymisierter Datensätze haben gezeigt, dass eine entsprechende Bewertung anspruchsvoll sein kann[18]. Um festzustellen, ob eine natürliche Person identifizierbar ist, muss man alle Mittel prüfen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden können, um die natürliche Person direkt oder indirekt zu identifizieren[19].

Beispiele für nicht-personenbezogene Daten:

- Daten, die in dem Maße aggregiert werden, dass einzelne Ereignisse (beispielsweise individuelle Auslandsreisen oder Reisemuster natürlicher Personen, die personenbezogene Daten darstellen könnten) nicht mehr identifizierbar sind, können als anonyme Daten eingestuft werden[20]. Anonyme Daten werden beispielsweise in Statistiken oder in

[15] Siehe Erwägungsgrund 26 der 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), in dem es heißt: „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann".

[16] Siehe Urteil des Gerichtshofs vom 19. Oktober 2016, Patrick Breyer gegen Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779. Der Gerichtshof befand, dass dynamische IP-Adressen personenbezogene Daten darstellen können, selbst wenn ein Dritter (z. B. Internetdienstanbieter) über zusätzliche Daten verfügt, die eine Identifizierung der Person ermöglichen würden. Die Möglichkeit der Identifizierung der Person muss ein Mittel darstellen, das nach allgemeinem Ermessen wahrscheinlich dazu benutzt werden könnte, die Person direkt oder indirekt zu identifizieren.

[17] Die Anonymisierung der Daten sollte stets unter Verwendung der neuesten Anonymisierungstechniken erfolgen.

[18] Beispiele für eine erneute Identifizierung vermeintlich anonymisierter Daten sind folgender für den ITRE-Ausschuss des Europäischen Parlaments durchgeführten Studie über künftige Datenströme zu entnehmen: Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee*, 2017, S. 22, Kasten 2. Online abrufbar unter: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

[19] Siehe Erwägungsgrund 26 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), in dem es heißt: „Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."

[20] Siehe dazu die Stellungnahme 05/2014 der Artikel-29-Datenschutzgruppe zu Anonymisierungstechniken, angenommen am 10. April 2014, WP 216, S. 9: „Nur wenn der Verantwortliche die Daten in einem Maße aggregiert, in dem die einzelnen Ereignisse nicht mehr identifizierbar sind, kann der entsprechende Datensatz als anonym eingestuft werden. Wenn zum Beispiel eine Organisation Daten über individuelle Reisebewegungen erfasst, würden die individuellen Reisemuster auf der Ebene der Veranstaltung für jede Partei weiterhin als personenbezogene Daten gelten, solange der Verantwortliche (oder jede andere Partei) noch Zugang zu den ursprünglichen Rohdaten hat, selbst wenn direkte Kennungen aus dem Datensatz, der Dritten bereitgestellt wird, entfernt wurden. Würde jedoch der Verantwortliche die Rohdaten löschen und lediglich hochgradig aggregierte Statistiken an Dritte weitergeben, etwa in einer Aussage wie „Montags verkehren auf der Strecke X 160 % mehr Fluggäste als dienstags", so würde dies als anonyme Daten gelten."

Verkaufsberichten verwendet (z. B. zur Beurteilung der Popularität eines Produkts und seiner Merkmale).

- Hochfrequenzhandelsdaten im Finanzsektor oder Daten zur Präzisionslandwirtschaft, die dazu beitragen, den Einsatz von Pestiziden, Nährstoffen und Wasser zu überwachen und zu optimieren.

Können jedoch nicht-personenbezogene Daten in irgendeiner Weise mit einer bestimmten natürlichen Person in Verbindung gebracht werden, sodass letztere direkt oder indirekt identifizierbar ist, so sind die Daten als personenbezogene Daten anzusehen.

Wenn beispielsweise ein Qualitätskontrollbericht über eine Produktionslinie es ermöglicht, die Daten mit bestimmten Fabrikarbeitern (z. B. denjenigen, die die Produktionsparameter festlegen) in Verbindung zu bringen, so würden die Daten als personenbezogene Daten gelten und die Datenschutz-Grundverordnung ist anzuwenden. Gleiches gilt, wenn Entwicklungen in den Bereichen Technologie und Datenanalyse es ermöglichen, anonymisierte Daten in personenbezogene Daten zu konvertieren[21].

Da sich die Begriffsbestimmung von personenbezogenen Daten auf „natürliche Personen" bezieht, sind Datensätze mit den Namen und Kontaktdaten juristischer Personen im Prinzip als nicht-personenbezogene Daten zu betrachten.[22] In bestimmten Situationen können sie jedoch personenbezogene Daten darstellen[23]. Dies ist beispielsweise der Fall, wenn der Name der juristischen Person mit dem einer natürlichen Person übereinstimmt, die Eigentümerin der juristischen Person ist, oder wenn die Information eine bestimmte oder bestimmbare natürliche Person betrifft[24].

2.2 Gemischte Datensätze

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten und die Datenschutz-Grundverordnung betrachten den freien Datenverkehr in der EU aus zwei verschiedenen Blickwinkeln.

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten enthält ein allgemeines Verbot von Datenlokalisierungsauflagen für nicht-personenbezogene Daten. Nach Artikel 4 Absatz 1 der Verordnung sind Datenlokalisierungsauflagen unzulässig, es sei denn, sie sind aus Gründen der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit gerechtfertigt.

Die Datenschutz-Grundverordnung gewährleistet nicht nur ein hohes Schutzniveau für personenbezogene Daten, sondern auch den freien Verkehr personenbezogener Daten. Nach Artikel 1 Absatz 3 der Verordnung darf der freie Verkehr personenbezogener Daten „aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten

[21] Werden personenbezogene Daten unrechtmäßig verarbeitet oder verstößt die Verarbeitung anderweitig gegen die Datenschutz-Grundverordnung, können die betroffenen Personen (natürliche Personen) nach der Datenschutz-Grundverordnung eine Beschwerde bei einer nationalen Aufsichtsbehörde (Datenschutzbehörde) in der EU einreichen oder vor einem nationalen Gericht einen wirksamen Rechtsbehelf einlegen. Die Aufgaben, Zuständigkeiten und Befugnisse der nationalen Aufsichtsbehörden sind in Kapitel VI Abschnitt 2 der Datenschutz-Grundverordnung geregelt.

[22] Erwägungsgrund 14 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) besagt Folgendes: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person." Dies ist jedoch vor dem Hintergrund der Definition des Begriffs „personenbezogene Daten" in Artikel 4 Nummer 1 der Datenschutz-Grundverordnung auszulegen.

[23] Siehe Urteil des Gerichtshofs vom 9. November 2010 in den verbundenen Rechtssachen Volker und Markus Schecke GbR (C-92/09) und Hartmut Eifert (C-93/09) / Land Hessen, ECLI:EU:C:2010:662, Rn. 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

weder eingeschränkt noch verboten werden.“ Zusammen sehen die beiden Verordnungen den freien Verkehr „aller“ Daten innerhalb der EU vor. Auf die besonderen Bestimmungen wird in den Abschnitten 3.1 und 3.2 näher eingegangen.

Ein gemischter Datensatz besteht sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten. Gemischte Datensätze, die den größten Teil der in der Datenwirtschaft verwendeten Datensätze ausmachen, kommen aufgrund technologischer Entwicklungen, z. B. Internet der Dinge (digitale Vernetzung von Objekten), künstliche Intelligenz und Technologien für die Analyse großer Datenmengen, häufig vor.

Beispiele für gemischte Datensätze:

- Steuerregistereinträge von Unternehmen, in denen Name und Telefonnummer des Geschäftsführers des Unternehmens angegeben sind
- Datensätze bei Banken, insbesondere Datensätze mit Angaben zu Kunden und Transaktionen, z. B. für Zahlungsdienste (Kredit- und Debitkarten), Anträge auf Partnerbeziehungsmanagement (*Partner Relationship Management* – PRM) und Darlehensverträge, Unterlagen, in denen Daten natürlicher und juristischer Personen gemischt sind
- Anonymisierte statistische Daten von Forschungseinrichtungen und die ursprünglich erhobenen Rohdaten, z. B. die Antworten der einzelnen Teilnehmer auf die Fragen im Rahmen statistischer Erhebungen
- Wissensdatenbanken von Unternehmen zu IT-Problemen und deren Lösungen, die sich auf die IT-Störmeldungen einzelner Personen stützen
- Daten im Zusammenhang mit dem Internet der Dinge, wenn einige der Daten Annahmen über bestimmbare Personen ermöglichen (z. B. Anwesenheit an einer bestimmten Adresse und Nutzungsmuster)
- Analysen der Betriebslog-Daten von Produktionsanlagen in der verarbeitenden Industrie

Beispiel: Dienste für Kundenbeziehungsmanagement

Einige Banken nutzen Dienste Dritter für Kundenbeziehungsmanagement (*Customer Relationship Management* – CRM), für die in der CRM-Umgebung Kundendaten bereitgestellt werden müssen. Zu den Daten, die für den CRM-Dienst benötigt werden, gehören alle Informationen, die für ein wirksames Management der Interaktion mit den Kunden erforderlich sind, z. B. ihre Postanschrift und E-Mail-Adresse, ihre Telefonnummer, die Waren und Dienstleistungen, die sie kaufen, und die Verkaufsberichte, einschließlich aggregierter Daten. Diese Daten können daher sowohl personenbezogene als auch nicht-personenbezogene Kundendaten umfassen.

Für gemischte Datensätze sieht die Verordnung über den freien Verkehr nicht-personenbezogener Daten[25] Folgendes vor:

„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.“

Dies bedeutet im Falle eines Datensatzes, der sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten besteht,

[25] Artikel 2 Absatz 2.

- dass für die nicht-personenbezogenen Daten des Datensatzes die Verordnung über den freien Verkehr nicht-personenbezogener Daten gilt,
- dass für die personenbezogenen Daten des Datensatzes die den freien Verkehr betreffende Bestimmung der Datenschutz-Grundverordnung[26] gilt und
- dass, falls die nicht-personenbezogenen Daten und die personenbezogenen Daten „untrennbar miteinander verbunden" sind, die Datenschutzrechte und -pflichten aus der Datenschutz-Grundverordnung in vollem Umfang für den gesamten gemischten Datensatz gelten, und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen[27].

Diese Auslegung steht mit dem durch die Charta der Grundrechte der Europäischen Union[28] garantierten Recht auf Schutz personenbezogener Daten und mit Erwägungsgrund 8 der Verordnung über den freien Verkehr nicht-personenbezogener Daten[29] im Einklang. In Erwägungsgrund 8 der Verordnung heißt es: „Die vorliegende Verordnung lässt den Rechtsrahmen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten … und insbesondere die [Datenschutz-Grundverordnung] und die Richtlinien (EU) 2016/680 … und 2002/58/EG … unberührt."

Praktisches Beispiel:

Ein innerhalb der EU tätiges Unternehmen bietet seine Dienste über eine Plattform an. Unternehmen laden (als Kunden) ihre Dokumente, die gemischte Datensätze enthalten, auf die Plattform hoch. Als „Verantwortlicher" muss das Unternehmen, das die Dokumente hochlädt, dafür sorgen, dass die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt. Zum Zwecke der Verarbeitung des Datensatzes im Auftrag des Verantwortlichen muss das Unternehmen, das die Dienste anbietet (der „Auftragsverarbeiter"), die Daten im Einklang mit der Datenschutz-Grundverordnung speichern und verarbeiten, u. a. um sicherzustellen, dass ein angemessenes Sicherheitsniveau für die Daten gewährleistet ist, etwa durch Verschlüsselung.

Der Begriff „untrennbar miteinander verbunden" ist in keiner der beiden Verordnungen[30] definiert. In der Praxis kann davon ausgegangen werden, dass er sich auf einen Datensatz bezieht, der personenbezogene Daten sowie nicht-personenbezogene Daten enthält, deren Trennung unmöglich ist oder vom Verantwortlichen als wirtschaftlich ineffizient oder technisch nicht machbar angesehen wird. Dies wäre zum Beispiel der Fall, wenn sich beim Erwerb von CRM- und Verkaufsberichtssystemen die Softwarekosten für das Unternehmen verdoppeln würden, weil es für das CRM (personenbezogene Daten) und für die auf die CRM-Daten gestützten Verkaufsberichtssysteme (aggregierte/nicht-personenbezogene Daten) jeweils eine eigene Software erwerben müsste.

---

[26] Artikel 1 Absatz 3 der 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). Siehe auch Abschnitt 3.2 dieser Mitteilung.

[27] Hierauf wird in der nur in englischer Sprache vorliegenden Arbeitsunterlage der Kommissionsdienststellen zur Folgenabschätzung als Begleitunterlage zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (SWD(2017) 304 final), Teil 1/2, S. 3, hingewiesen: „*regardless of how much of personal data are included in mixed datasets, GDPR needs to be fully complied with in respect to the personal data part of the set.*" (unabhängig davon, wie hoch der Anteil personenbezogener Daten an einem gemischten Datensatz ist, muss in Bezug auf die zu dem Satz gehörenden personenbezogenen Daten die DSGVO (Datenschutz-Grundverordnung) in vollem Umfang eingehalten werden).

[28] Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391).

[29] Erwägungsgrund 8 der Verordnung.

[30] Verordnung über den freien Verkehr nicht-personenbezogener Daten und Datenschutz-Grundverordnung.

Durch eine Trennung dürfte der Datensatz auch erheblich an Wert verlieren. Zudem erschwert der sich ändernde Charakter der Daten (siehe Abschnitt 2.1) eine klare Unterscheidung und somit Trennung der verschiedenen Datenkategorien.

Wichtig ist, dass keine der beiden Verordnungen die Unternehmen dazu verpflichtet, die Datensätze, für die sie verantwortlich sind oder die sie verarbeiten, zu trennen.

Bei einem gemischten Datensatz sind daher im Allgemeinen die Pflichten des Verantwortlichen und des Auftragsverarbeiters zu erfüllen und die Rechte der betroffenen Personen zu achten, die in der Datenschutz-Grundverordnung festgelegt sind.

Verarbeitung von Gesundheitsdaten

Zu einem gemischten Datensatz können auch Gesundheitsdaten gehören. Beispiele sind unter anderem elektronische Patientenakten, klinische Prüfungen oder Datensätze, die von verschiedenen mobilen Anwendungen für Gesundheit und Wohlbefinden erhoben werden (z. B. von Anwendungen, die den Gesundheitszustand messen, an die Einnahme von Arzneimitteln erinnern oder die Entwicklung der Fitness verfolgen)[31]. Die Grenzen zwischen den personenbezogenen und den nicht-personenbezogenen Daten in diesen Datensätzen verschwimmen aufgrund technologischer Entwicklungen immer mehr. Ihre Verarbeitung muss daher im Einklang mit der Datenschutz-Grundverordnung erfolgen, insbesondere (da Gesundheitsdaten nach der Verordnung eine besondere Kategorie von Daten darstellen) mit Artikel 9, der ein allgemeines Verbot der Verarbeitung besonderer Kategorien von Daten und Ausnahmen von diesem Verbot enthält.

Die Daten in gemischten Datensätzen, die Gesundheitsdaten enthalten, können eine wertvolle Informationsquelle sein, z. B. für die medizinische Forschung, für die Messung der Nebenwirkungen eines verschriebenen Arzneimittels, für krankheitsstatistische Zwecke oder für die Entwicklung neuer Gesundheitsdienstleistungen oder Behandlungen. Bei der Durchführung der ersten Verarbeitungsvorgänge und bei der Durchführung weiterer Datenverarbeitungsvorgänge ist jedoch die Datenschutz-Grundverordnung einzuhalten. Jede Verarbeitung von Gesundheitsdaten muss daher auf einer gültigen Rechtsgrundlage[32] und mit einer angemessenen Begründung erfolgen, sicher sein und ausreichende Garantien bieten.

Schließlich sind Rechtssicherheit und Vertrauen in die Datenverarbeitung für Einzelpersonen und Unternehmen unerlässlich. Sie sind auch für die Datenwirtschaft von entscheidender Bedeutung. Beide Verordnungen gewährleisten dies und beide dienen dem Ziel, den freien Datenverkehr nicht zu verändern.

3. Freier Datenverkehr und Aufhebung von Datenlokalisierungsauflagen

In diesem Abschnitt werden der Begriff „Datenlokalisierungsauflagen“ nach der Verordnung über den freien Verkehr nicht-personenbezogener Daten und der Grundsatz des freien Verkehrs nach der Datenschutz-Grundverordnung ausführlicher erläutert. Obwohl sich diese Bestimmungen an die Mitgliedstaaten richten, kann es für Unternehmen aufschlussreich sein, ein genaueres Bild davon zu erhalten, wie diese beiden Verordnungen zum freien Verkehr aller Daten innerhalb der EU beitragen.

---

[31] Entwicklung und Betrieb mobiler Gesundheitsanwendungen erfordern die strikte Einhaltung der Vorschriften der Datenschutz-Grundverordnung. Dies wird im Verhaltenskodex für den Schutz der Privatsphäre bei mobilen Gesundheitsanwendungen weiter konkretisiert, der zurzeit ausgearbeitet wird. Weitere Informationen zum Stand der Entwicklung: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

[32] Siehe Artikel 6 Absatz 1 der 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).

3.1 Freier Verkehr nicht-personenbezogener Daten

Nach der Verordnung über den freien Verkehr nicht-personenbezogener Daten[33] sind „Datenlokalisierungsauflagen … unzulässig, es sei denn, sie sind aus Gründen der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit gerechtfertigt."

Datenlokalisierungsauflagen sind definiert[34] 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 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"[35].

Die Definition veranschaulicht, dass die Maßnahmen, die den freien Datenverkehr innerhalb der EU beschränken, verschiedene Formen annehmen können. Sie können in Rechts- und Verwaltungsvorschriften festgelegt sein oder sich sogar aus einer allgemeinen, einheitlichen Verwaltungspraxis ergeben. Zudem umfasst das Verbot von Datenlokalisierungsauflagen sowohl direkte als auch indirekte Maßnahmen, die den freien Verkehr nicht-personenbezogener Daten beschränken würden.

Direkte Datenlokalisierungsauflagen können etwa in der Verpflichtung bestehen, die Daten an einem bestimmten geografischen Ort zu speichern (z. B.: die Server müssen sich in einem bestimmten Mitgliedstaat befinden), oder in der Verpflichtung, besonderen nationalen technischen Anforderungen zu genügen (z. B.: die Daten müssen in einem bestimmten nationalen Format vorliegen).

Indirekte Datenlokalisierungsauflagen, die die Verarbeitung der nicht-personenbezogenen Daten in anderen Mitgliedstaaten behindern würden, können in unterschiedlicher Form erteilt werden. Dazu können Auflagen gehören, technische Anlagen zu nutzen, die in einem bestimmten Mitgliedstaat zertifiziert oder genehmigt worden sind, oder andere Auflagen, die bewirken, dass die Verarbeitung von Daten außerhalb eines bestimmten geografischen Gebiets oder Hoheitsgebiets innerhalb der Europäischen Union erschwert wird[36,37].

Bei der Prüfung, ob eine bestimmte Maßnahme eine indirekte Datenlokalisierungsauflage darstellt, müssen die besonderen Umstände des Einzelfalls berücksichtigt werden.

---

[33] Artikel 4 Absatz 1 der Verordnung.

[34] Artikel 3 Nummer 5 der 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.

[35] Es sei darauf hingewiesen, dass die Wahlmöglichkeiten der Marktteilnehmer und des öffentlichen Sektors bezüglich des Standorts der Datenverarbeitung durch rechtliche Unsicherheiten bezüglich der Reichweite rechtmäßiger oder unrechtmäßiger Datenlokalisierungsauflagen weiter eingeschränkt werden (siehe Erwägungsgrund 4 der 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).

[36] Erwägungsgrund 4 der 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.

[37] Siehe zwei Studien über Datenlokalisierungsauflagen, die vor Erlass der Verordnung über den freien Verkehr nicht-personenbezogener Daten durchgeführt wurden: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, SMART-Nummer 2015/2016, online abrufbar unter: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185, und 2) Time.lex, Spark Legal Network and Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, SMART-Nummer 2015/0054, online abrufbar unter: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

In der Verordnung über den freien Verkehr nicht-personenbezogener Daten[38] wird auf den Begriff der **öffentlichen Sicherheit** gemäß der Auslegung durch den Gerichtshof der Europäischen Union verwiesen. Dieser Begriff „bezieht sich sowohl auf die innere als auch die äußere Sicherheit eines Mitgliedstaats[39] 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[40] 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."

Datenlokalisierungsauflagen, die aus Gründen der öffentlichen Sicherheit gerechtfertigt sind, müssen auch verhältnismäßig sein. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union verlangt der Grundsatz der Verhältnismäßigkeit, dass die erlassenen Maßnahmen geeignet sind, die Erreichung des angestrebten Ziels zu gewährleisten, dass sie aber nicht über das für diesen Zweck erforderliche Maß hinausgehen[41].

Aus Gründen der Klarheit lässt das Verbot von Datenlokalisierungsauflagen bereits bestehende unionsrechtliche Beschränkungen unberührt.[42]

Ferner beinhaltet die Verordnung über den freien Verkehr nicht-personenbezogener Daten keine Verpflichtungen für Unternehmen und beschränkt auch nicht ihre Vertragsfreiheit zu entscheiden, wo ihre Daten verarbeitet werden sollen.

Die Mitgliedstaaten müssen die Einzelheiten sämtlicher in ihrem Hoheitsgebiet geltenden Datenlokalisierungsauflagen über eine **nationale einheitliche Online-Informationsstelle** (nationale Website) öffentlich verfügbar machen. Sie müssen diese Informationen auf dem neuesten Stand halten oder aktualisierte Einzelheiten an eine zentrale Informationsstelle übermitteln, die nach einem anderen Unionsakt eingerichtet wurde.[43] Der Einfachheit halber und um EU-weit Unternehmen den Zugang zu relevanten Informationen zu erleichtern, wird die Kommission Links zu diesen Informationsstellen auf dem Portal „Ihr Europa"[44] veröffentlichen.

---

[38] Erwägungsgrund 19 der Verordnung.

[39] Siehe zum Beispiel Urteil des Gerichtshofs vom 23. November 2010, Land Baden-Württemberg/Tsakouridis, C-145/09, ECLI:EU:C:2010:708, Rn. 43, und Urteil vom 4. April 2017, Sahar Fahimian/Bundesrepublik Deutschland, C-544/15, ECLI:EU:C:2017:225, Rn. 39.

[40] Siehe zum Beispiel das Urteil des Gerichtshofs vom 22. Dezember 2008, Kommission der Europäischen Gemeinschaften/Republik Österreich, C-161/07, ECLI:EU:C:2008:759, Rn. 35 und die dort angeführte Rechtsprechung, und Urteil vom 26. März 2009, Kommission der Europäischen Gemeinschaften/Italienische Republik, C-326/07, ECLI:EC:C:2009:193, Rn. 70 und die dort angeführte Rechtsprechung.

[41] Siehe zum Beispiel das Urteil des Gerichtshofs vom 8. Juli 2010, Afton Chemical Limited/Secretary of State for Transport, C-343/09, ECLI:EU:C:2010:419, Rn. 45 und die dort angeführte Rechtsprechung.

[42] Siehe zum Beispiel Artikel 245 Absatz 2 der Richtlinie 2006/112/EG vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem: „Die Mitgliedstaaten können von den in ihrem Gebiet ansässigen Steuerpflichtigen verlangen, ihnen den Aufbewahrungsort mitzuteilen, wenn sich dieser außerhalb ihres Gebiets befindet." Diese Bestimmung muss jedoch in Verbindung mit Artikel 249 gelesen werden, in dem es heißt: „Bewahrt ein Steuerpflichtiger von ihm ausgestellte oder empfangene Rechnungen elektronisch in einer Weise auf, die einen Online-Zugriff auf die Daten gewährleistet, und liegt der Aufbewahrungsort in einem Mitgliedstaat, in dem er nicht ansässig ist, haben die zuständigen Behörden des Mitgliedstaats, in dem er ansässig ist, für die Zwecke dieser Richtlinie im Rahmen der Rechtsvorschriften des Mitgliedstaats, in dem der Steuerpflichtige ansässig ist, und soweit dies für diese Behörden zur Kontrolle erforderlich ist, das Recht auf elektronischen Zugriff auf diese Rechnungen sowie auf deren Herunterladen und Verwendung."

[43] Artikel 4 Absatz 4 der 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.

[44] https://europa.eu/youreurope/index.htm

3.2 Freier Verkehr personenbezogener Daten

In der Datenschutz-Grundverordnung[45] heißt es: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden."

Legt ein Mitgliedstaat Datenlokalisierungsauflagen für personenbezogene Daten aus anderen Gründen als dem Schutz personenbezogener Daten fest, so ist dies im Lichte der Grundfreiheiten und der zulässigen Ausnahmegründe für Eingriffe in die Grundfreiheiten zu prüfen, wie sie im Vertrag über die Arbeitsweise der Europäischen Union[46,47] verankert und im einschlägigen EU-Recht vorgesehen sind, z. B. in der Dienstleistungsrichtlinie[48] und in der Richtlinie über den elektronischen Geschäftsverkehr[49].

Beispiel:

Ein nationales Gesetz schreibt vor, dass Gehaltskonten aus Gründen der Regulierungsaufsicht, z. B. durch nationale Steuerbehörden, in einem bestimmten Mitgliedstaat geführt werden müssen. Eine solche nationale Bestimmung würde nicht unter Artikel 1 Absatz 3 der Datenschutz-Grundverordnung fallen, da sie nicht mit dem Schutz personenbezogener Daten begründet wird. Stattdessen wäre diese Vorschrift im Lichte der im Vertrag über die Arbeitsweise der Europäischen Union verankerten Grundfreiheiten und der zulässigen Ausnahmegründe für Eingriffe in diese Freiheiten zu prüfen.

In der Datenschutz-Grundverordnung[50] wird anerkannt, dass die Mitgliedstaaten bestimmte Bedingungen, auch Beschränkungen, für die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten festlegen können. Laut ihrem Erwägungsgrund 53 sollte dies jedoch den freien Verkehr personenbezogener Daten innerhalb der EU nicht beeinträchtigen, falls solche Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten. Dies steht im Einklang mit Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union, der die Rechtsgrundlage für den Erlass der Vorschriften über das Recht auf den Schutz personenbezogener Daten und der Vorschriften über den freien Verkehr solcher Daten bildet.

---

[45] Artikel 1 Absatz 3 der 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).

[46] Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 47).

[47] Siehe auch das Urteil des Gerichtshofs vom 19. Juni 2008, Kommission/Großherzogtum Luxemburg, C-319/06, ECLI:EU:C:2008:350, Rn. 90–91: Der Gerichtshof war der Auffassung, dass die Verpflichtung, bestimmte Dokumente in einem bestimmten Mitgliedstaat bereitzuhalten und aufzubewahren, eine Beschränkung des freien Dienstleistungsverkehrs darstellt; eine Begründung, „dass das Vorhandensein ... geeignet ist, die Erfüllung der Überwachungsaufgaben der Behörden dieses Staates im Allgemeinen zu erleichtern", ist nicht ausreichend.

[48] Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36).

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

[50] Artikel 9 Absatz 4 der 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).

3.3 Anwendungsbereich der Verordnung über den freien Verkehr nicht-personenbezogener Daten

Wie bereits erwähnt, soll die Verordnung über den freien Verkehr nicht-personenbezogener Daten den freien Verkehr nicht-personenbezogener Daten innerhalb der Union[51] gewährleisten. Sie gilt daher nicht für eine Datenverarbeitung, die außerhalb der Union stattfindet, und auch nicht für Datenlokalisierungsauflagen in Bezug auf eine solche Verarbeitung[52,53].

Der Anwendungsbereich der Verordnung ist daher gemäß Artikel 2 Absatz 1 beschränkt auf die Verarbeitung nicht-personenbezogener elektronischer Daten in der EU, die

a) als eine Dienstleistung für Nutzer erfolgt, die in der EU wohnhaft oder niedergelassen sind, ungeachtet dessen, ob der Diensteanbieter in der EU niedergelassen ist oder nicht, oder
b) von einer natürlichen oder juristischen Person, die in der EU wohnhaft oder niedergelassen ist, für ihren eigenen Bedarf durchgeführt wird.

Beispiele:

Artikel 2 Absatz 1 Buchstabe a der Verordnung über den freien Verkehr nicht-personenbezogener Daten:

- Ein in den USA niedergelassener Anbieter von Cloud-Diensten erbringt Dienstleistungen für Kunden, die in der EU wohnhaft oder niedergelassen sind. Der Cloud-Diensteanbieter verwaltet seine Tätigkeiten über Server, die sich im Gebiet der EU befinden, und auf denen die Daten seiner europäischen Kunden gespeichert oder anderweitig verarbeitet werden. Dazu muss der Cloud-Diensteanbieter keine eigene Infrastruktur in der EU haben, sondern kann z. B. auch Serverkapazitäten in der EU anmieten. Die Verordnung über den freien Verkehr nicht-personenbezogener Daten gilt für diese Art der Datenverarbeitung.
- Ein in Japan niedergelassener Cloud-Diensteanbieter bietet seine Dienste für europäische Kunden an. Die Verarbeitungskapazitäten des Anbieters befinden sich in Japan, und alle Verarbeitungstätigkeiten finden dort statt. Die Verordnung über den freien Verkehr nicht-personenbezogener Daten findet in diesem Fall keine Anwendung, da alle Verarbeitungstätigkeiten außerhalb der EU stattfinden[54].

Artikel 2 Absatz 1 Buchstabe b der Verordnung über den freien Verkehr nicht-personenbezogener Daten:

---

[51] Siehe Artikel 1 der 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.

[52] Siehe Erwägungsgrund 15 der 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.

[53] Der Begriff „Verarbeitung“ ist in einem weiten Sinn definiert worden (Artikel 3 Nummer 2 der 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), sodass – wie in Erwägungsgrund 17 betont wird – die Verordnung für eine Verarbeitung im weitesten Sinne gelten und die Verwendung aller Arten von IT-Systemen erfassen sollte.

[54] Die 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 gilt nicht für Datenlokalisierungsauflagen der Mitgliedstaaten in Bezug auf die Speicherung nicht-personenbezogener Daten in Drittländern, die in den nationalen Rechtsordnungen enthalten sein können. Zur Klarstellung sei betont: Die Datenschutz-Grundverordnung gilt für die Verarbeitung personenbezogener Daten betroffener Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter, soweit die Datenverarbeitung im Zusammenhang damit steht, a) diesen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist, oder b) das Verhalten dieser Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt (siehe Artikel 3 Absatz 2 der Datenschutz-Grundverordnung).

- Ein kleines europäisches Start-up-Unternehmen aus dem Mitgliedstaat A will sein Geschäft ausweiten und eine Niederlassung im Mitgliedstaat B eröffnen. Um Kosten zu sparen, soll die Speicherung und Verarbeitung der Daten der neuen Niederlassung zentral auf seinen Servern erfolgen, die sich im Mitgliedstaat A befinden. Die Mitgliedstaaten dürfen eine solche IT-Zentralisierung nicht verbieten, es sei denn, dies ist aus Gründen der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit gerechtfertigt.

Obwohl die Verordnung über den freien Verkehr nicht-personenbezogener Daten nicht anwendbar ist, wenn die gesamte Verarbeitung nicht-personenbezogener Daten außerhalb der EU stattfindet, ist dennoch die Datenschutz-Grundverordnung einzuhalten, wenn personenbezogene Daten Teil des Datensatzes sind. So müssen insbesondere die Vorschriften der Datenschutz-Grundverordnung für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen auf jeden Fall eingehalten werden[55].

3.4 Tätigkeiten in Bezug auf die interne Organisation der Mitgliedstaaten

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten verpflichtet die Mitgliedstaaten nicht dazu, die Erbringung von Leistungen im Zusammenhang mit nicht-personenbezogenen Daten auszulagern, die sie selbst erbringen oder auf anderem Wege als durch die Vergabe öffentlicher Aufträge organisieren möchten[56].

Artikel 2 Absatz 3 Unterabsatz 2 der Verordnung über den freien Verkehr nicht-personenbezogener Daten lautet:

„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[57] 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.“[58]

---

[55] Bezüglich der Übermittlung personenbezogener Daten an Drittländer ist die Website der Kommission zu beachten: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en. Siehe hierzu auch die *Mitteilung der Kommission an das Europäische Parlament und den Rat – Austausch und Schutz personenbezogener Daten in einer globalisierten Welt*, COM(2017) 7 final, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2017:7:FIN. In Bezug auf Japan hat die Kommission am 23. Januar 2019 ihren Angemessenheitsbeschluss angenommen, nach dem personenbezogene Daten auf der Grundlage starker Schutzgarantien ungehindert zwischen den beiden Volkswirtschaften übermittelt werden können.

[56] Erwägungsgrund 14 der 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.

[57] In Artikel 2 Absatz 1 Nummer 4 der 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) heißt es: *„Einrichtungen des öffentlichen Rechts“ sind Einrichtungen mit sämtlichen der folgenden Merkmale: a) Sie wurden zu dem besonderen Zweck gegründet, im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen, b) sie besitzen Rechtspersönlichkeit und c) sie werden überwiegend vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts finanziert oder unterstehen hinsichtlich ihrer Leitung der Aufsicht dieser Gebietskörperschaften oder Einrichtungen, oder sie haben ein Verwaltungs-, Leitungs- beziehungsweise Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts ernannt worden sind;“*

[58] In Erwägungsgrund 13 der 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 wird betont, dass die Verordnung unbeschadet der Richtlinie 2014/24/EU gilt.

Es kann berechtigte Interessen geben, die eine solche „Selbsterbringung“ von Datenverarbeitungsdiensten rechtfertigen, beispielsweise eine „Internalisierung“ oder gegenseitige Vereinbarungen zwischen öffentlichen Verwaltungen. Typische Beispiele sind die Nutzung einer „Behörden-Cloud“ oder eine Behörde, die eine zentrale IT-Stelle mit der Erbringung von Datenverarbeitungsdiensten für öffentliche Einrichtungen und Stellen beauftragt.

Dennoch werden die Mitgliedstaaten durch die Verordnung über den freien Verkehr nicht-personenbezogener Daten dazu angehalten, die wirtschaftliche Effizienz und andere Vorteile einer Nutzung externer Dienstleister zu beachten[59,60]. Haben die nationalen Behörden aber begonnen, die Datenverarbeitung mit vertraglicher Vergütung privater Parteien „nach außen“ zu vergeben und erfolgt die Verarbeitung innerhalb der EU, so fällt diese Verarbeitung unter die Verordnung über den freien Verkehr nicht-personenbezogener Daten, was bedeutet, dass der Grundsatz des freien Verkehrs nicht-personenbezogener Daten auf die allgemeine und Verwaltungspraxis der nationalen Behörden Anwendung findet. Insbesondere müssen sie dann auf Datenlokalisierungsauflagen verzichten, z. B. in Ausschreibungen für die Vergabe öffentlicher Aufträge[61].

4. Selbstregulierungskonzepte zur Unterstützung des freien Datenverkehrs

Selbstregulierung trägt zu Innovation und Vertrauen unter den Marktteilnehmern bei und hat das Potenzial, besser auf Marktveränderungen zu reagieren. Dieser Abschnitt enthält einen Überblick über Selbstregulierungsinitiativen für die Verarbeitung sowohl personenbezogener als auch nicht-personenbezogener Daten.

4.1 Übertragung von Daten und Wechsel des Cloud-Diensteanbieters

Eines der Ziele der Verordnung über den freien Verkehr nicht-personenbezogener Daten besteht darin, eine Abhängigkeit von einem bestimmten Anbieter zu vermeiden. Dazu kommt es, wenn die Nutzer nicht zwischen Dienstleistern wechseln können, weil ihre Daten im System des Anbieters „eingesperrt“ sind, z. B. aufgrund eines spezifischen Datenformats oder aufgrund vertraglicher Vereinbarungen, und nicht nach außerhalb des IT-Systems dieses Anbieters übertragen werden können. Die ungehinderte Übertragbarkeit von Daten ist wichtig, damit die Nutzer frei zwischen Anbietern von Datenverarbeitungsdiensten wählen können und somit ein wirksamer Wettbewerb auf dem Markt gewährleistet ist.

In einem breiten Spektrum digitaler Wirtschaftszweige, einschließlich der Cloud-Dienste, gewinnt die Übertragbarkeit von Daten zwischen verschiedenen Unternehmen immer mehr an Bedeutung.

Nach Artikel 6 der Verordnung über den freien Verkehr nicht-personenbezogener Daten fördert und erleichtert die Kommission die Entwicklung von Verhaltensregeln für die Selbstregulierung auf Unionsebene („Verhaltensregeln“), um zu einer wettbewerbsfähigen Datenwirtschaft beizutragen. Auf dieser Grundlage sollen die Unternehmen im Rahmen der

---

[59] Erwägungsgrund 14 der 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.

[60] Ein externer Dienstleister wäre ein Unternehmen, bei dem es sich um keine „Einrichtung des öffentlichen Rechts“ handelt, wie in Artikel 2 Absatz 1 Nummer 4 der 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) definiert.

[61] Erwägungsgrund 13 der 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.

Selbstregulierung Verhaltensregeln im Hinblick auf den Anbieterwechsel und die Übertragung von Daten ausarbeiten.

Bei der Ausarbeitung solcher Verhaltensregeln für die Übertragung von Daten sollte eine Reihe von Aspekten berücksichtigt werden, insbesondere:

- **bewährte Verfahren** zur Erleichterung des Wechsels des Diensteanbieters und der Übertragung von Daten in einem strukturierten, gängigen, maschinenlesbaren Format,
- **Vorschriften für Mindestangaben**, damit sichergestellt ist, dass berufliche Nutzer vor dem Abschluss eines Datenverarbeitungsvertrags hinreichend genaue und klare 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,
- **Ansätze für Zertifizierungssysteme**, damit Cloud-Dienste besser vergleichbar sind, und
- **Kommunikationspläne** zur Bekanntmachung der Verhaltensregeln.

Auf dem Markt der Cloud-Dienste hat die Kommission damit begonnen, im Rahmen des digitalen Binnenmarkts die Tätigkeiten der von Cloud-Beteiligten gebildeten Arbeitsgruppen unterstützen, in denen Cloud-Fachleute und berufliche Nutzer, darunter auch kleine und mittlere Unternehmen, zusammenkommen. Eine der Untergruppen arbeitet derzeit im Zuge der Selbstregulierung an Verhaltensregeln für die Übertragung von Daten und den Wechsel zwischen Cloud-Diensteanbietern (SWITO-Arbeitsgruppe)[62], eine andere Untergruppe befasst sich mit der Entwicklung einer Cloud-Sicherheitszertifizierung (CSPCERT-Arbeitsgruppe)[63].

Die SWIPO-Arbeitsgruppe arbeitet an Verhaltensregeln für das gesamte Spektrum von Cloud-Diensten, *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) und *Software-as-a-Service* (SaaS).

Die Kommission geht davon aus, dass die verschiedenen Verhaltensregeln durch **Mustervertragsklauseln** ergänzt werden[64]. Diese sollen eine ausreichende technische und rechtliche Spezifität bei der praktischen Einführung und Anwendung der Verhaltensregeln ermöglichen, was gerade für kleine und mittlere Unternehmen von besonderer Bedeutung ist. Die Ausarbeitung der Mustervertragsklauseln ist nach der Aufstellung der Verhaltensregeln geplant (die bis zum 29. November 2019 abgeschlossen sein sollte).

Gemäß Artikel 8 der Verordnung über den freien Verkehr nicht-personenbezogener Daten wird die Kommission bis zum 29. November 2022 eine Bewertung der Durchführung der Verordnung vornehmen. Dadurch soll es möglich werden, Folgendes zu beurteilen: i) die Auswirkungen des freien Datenverkehrs in Europa, ii) die Anwendung der Verordnung, insbesondere auf gemischte Datensätze, iii) das Ausmaß, in dem die Mitgliedstaaten bestehende ungerechtfertigte Datenlokalisierungsauflagen tatsächlich aufgehoben haben, und iv) die Wirksamkeit der Verhaltensregeln auf dem Markt in Bezug auf die Übertragung von Daten und den Wechsel zwischen Cloud-Diensteanbietern.

---

[62] *Cloud Switching and Porting Data Working Group* (Arbeitsgruppe für Cloud-Wechsel und Datenübertragung).

[63] *European Cloud Service Provider Certification Working Group* (Arbeitsgruppe für die Zertifizierung europäischer Cloud-Diensteanbieter). Siehe hierzu auch Abschnitt 4.3.

[64] Siehe Erwägungsgrund 30 der 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.

Der Begriff der Übertragbarkeit und das Zusammenwirken mit der Datenschutz-Grundverordnung

Beide Verordnungen[65] beziehen sich auf die Übertragbarkeit von Daten und zielen darauf ab, das Übertragen von Daten von einem IT-Umfeld in ein anderes zu erleichtern, d. h. entweder in die Systeme anderer Anbieter oder in örtlich betriebene Systeme. Dies verhindert eine Anbieterabhängigkeit und fördert den Wettbewerb zwischen den Diensteanbietern. In ihrem Herangehen an die Übertragbarkeit unterscheiden sich die beiden Verordnungen jedoch bezüglich der Beziehungen zwischen den betroffenen Interessengruppen und der Rechtsnatur der Vorschriften.

Das Recht auf Übertragung personenbezogener Daten gemäß Artikel 20 der Datenschutz-Grundverordnung stellt auf die Beziehung zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ab. Es handelt sich hier um das Recht der betroffenen Person, ihre personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, an einen anderen Verantwortlichen oder an ihre eigenen Speichereinrichtungen zu übermitteln[66]. Die betroffenen Personen in dieser Beziehung sind in der Regel Verbraucher, die verschiedene Online-Dienste nutzen und die zwischen solchen Dienstleistern wechseln möchten.

Dagegen sieht Artikel 6 der Verordnung über den freien Verkehr nicht-personenbezogener Daten kein Recht beruflicher Nutzer auf Übertragung von Daten vor, sondern stattdessen einen Selbstregulierungsansatz mit freiwilligen Verhaltensregeln für die Branche. Gleichzeitig stellt er auf eine Situation ab, in der ein beruflicher Nutzer die Verarbeitung seiner Daten an einen Dritten, der einen Datenverarbeitungsdienst anbietet, ausgelagert hat[67]. Als „beruflicher Nutzer“ gilt gemäß Artikel 3 Nummer 8 der Verordnung über den freien Verkehr nicht-personenbezogener Daten „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.“

In der Praxis betrifft die Übertragbarkeit nach Artikel 6 der Verordnung über den freien Verkehr nicht-personenbezogener Daten die gewerbliche Beziehung zwischen einem beruflichen Nutzer (der auch ein „für die Verarbeitung Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung sein kann, falls personenbezogene Daten verarbeitet werden) und einem Diensteanbieter (der in ähnlicher Weise in bestimmten Fällen als „Auftragsverarbeiter“ einzustufen ist).

Trotz der Unterschiede können sich Situationen ergeben, in denen die Übertragbarkeit von Daten sowohl von der Verordnung über den freien Verkehr nicht-personenbezogener Daten als

---

[65] Artikel 6 der 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 und Artikel 20 der 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).

[66] Siehe dazu: Artikel-29-Datenschutzgruppe: Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 Rev.01, angenommen am 13. Dezember 2016, zuletzt geändert und angenommen am 5. April 2017.

[67] In Erwägungsgrund 29 der 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 heißt es: „Während das geltende Unionsrecht [d. h. die Datenschutz-Grundverordnung] 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.“

auch von der Datenschutz-Grundverordnung im Hinblick auf gemischte Datensätze erfasst wird.

Beispiel:

Ein Unternehmen, das einen Cloud-Dienst nutzt, will seinen Cloud-Diensteanbieter wechseln und alle Daten zu einem neuen Anbieter übertragen. Der Wechsel des Dienstleisters und die Übertragung der Daten sind in dem Vertrag zwischen dem Kunden und dem Cloud-Diensteanbieter geregelt. Wenn sich der alte Cloud-Diensteanbieter an die nach der Verordnung über den freien Verkehr nicht-personenbezogener Daten aufgestellten Verhaltensregeln hält, so muss die Übertragung der Daten im Einklang mit den darin festgelegten Vorgaben erfolgen.

Enthalten die zu den übertragenen Datensätze auch personenbezogene Daten, so sind bei der Übertragung alle einschlägigen Bestimmungen der Datenschutz-Grundverordnung einzuhalten, wobei insbesondere sichergestellt sein muss, dass der neue Cloud-Diensteanbieter die geltenden Anforderungen, z. B. in Bezug auf die Sicherheit, ebenfalls erfüllt[68].

Beispiel:

Wenn eine Bank beschließt, ihren Dienstleister für das Kundenbeziehungsmanagement (CRM) zu wechseln, kann es sein, dass einige (personenbezogene und nicht-personenbezogene) Daten vom alten Anbieter zum neuen übertragen werden müssen. Für diese Daten gelten dann verschiedene rechtliche Anforderungen, von denen einige aus der Datenschutz-Grundverordnung und andere aus der Verordnung über den freien Verkehr nicht-personenbezogener Daten stammen.

4.2 Verhaltensregeln und Zertifizierungssysteme zum Schutz personenbezogener Daten

Mithilfe von Verhaltensregeln und Zertifizierungsverfahren kann der Nachweis erbracht werden, dass die Verpflichtungen aus der Datenschutz-Grundverordnung eingehalten werden (siehe Artikel 24 Absatz 3 und Artikel 28 Absatz 5).

Nach Artikel 40 Absatz 1 und Artikel 42 Absatz 1 der Datenschutz-Grundverordnung sollen die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss und die Kommission die Branche dazu anhalten, Verhaltensregeln aufzustellen und Datenschutz-Zertifizierungsverfahren einzuführen.

Verbände oder andere Vereinigungen, die bestimmte Kategorien von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern vertreten, können Verhaltensregeln für einen bestimmten Sektor ausarbeiten. Der Entwurf der Verhaltensregeln muss der jeweiligen zuständigen Aufsichtsbehörde zur Genehmigung vorgelegt werden[69]. Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so muss die Aufsichtsbehörde diesen dem Europäischen Datenschutzausschuss vorlegen, bevor sie ihn genehmigt. Der Ausschuss gibt daraufhin seine Stellungnahme dazu ab, ob der Entwurf mit der Datenschutz-Grundverordnung vereinbar ist.

[68] Siehe dazu: Artikel-29-Datenschutzgruppe: Stellungnahme 5/2012 zum Cloud-Computing, angenommen am 1. Juli 2012, WP 196, in der die Stellung und die Verpflichtungen der Cloud-Nutzer und Cloud-Diensteanbieter in Bezug auf die Verarbeitung personenbezogener Daten weiter präzisiert werden.

[69] Siehe Artikel 40 Absatz 5 und Artikel 55 der 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).

Der Europäische Datenschutzausschuss hat seine Leitlinien 1/2019 für Verhaltensregeln und Überwachungsstellen gemäß der Datenschutz-Grundverordnung[70] veröffentlicht. Die Leitlinien enthalten auch Informationen über die Ausarbeitung von Verhaltensregeln, Kriterien für ihre Genehmigung und andere nützliche Informationen. Ebenso enthalten die Leitlinien 1/2018 des Europäischen Datenschutzausschusses für die Zertifizierung und die Festlegung von Zertifizierungskriterien gemäß den Artikeln 42 und 43 der Datenschutz-Grundverordnung[71] Informationen über die Zertifizierung nach dieser Verordnung und die Ausarbeitung und Genehmigung von Zertifizierungskriterien.

Beispiele für Verhaltensregeln, die von der Cloud-Branche aufgestellt wurden:

EU Cloud Code of Conduct: Diese EU-Verhaltensregeln für Cloud-Dienste wurden mit Unterstützung der Kommission in Zusammenarbeit mit der *Cloud Select Industry Group* (C-SIG) auf der Grundlage der Datenschutzrichtlinie[72] und anschließend der Datenschutz-Grundverordnung ausgearbeitet. Die EU-Verhaltensregeln für Cloud-Dienste beziehen sich auf das gesamte Spektrum der Cloud-Dienste – *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS) und *Infrastructure-as-a-Service* (IaaS)[73].

Code of Conduct for Cloud Infrastructure Service Providers in Europe (CISPE)[74]: Im Mittelpunkt dieser Verhaltensregeln für Anbieter von Cloud-Infrastruktur-Diensten in Europa stehen die Erbringer von IaaS-Diensten. Die CISPE-Verhaltensregeln bestehen aus Anforderungen an IaaS-Anbieter, die sich als Auftragsdatenverarbeiter gemäß der Datenschutz-Grundverordnung betätigen. Sie enthalten auch Bestimmungen über die Leitungsstruktur für ihre Umsetzung und Anwendung.

Cloud Security Alliance's Code of Conduct for GDPR Compliance: Die Verhaltensregeln der Cloud-Sicherheitsallianz (CSA) zur Einhaltung der DSGVO richten sich an alle Interessenträger im Bereich des Cloud-Computing und des europäischen Datenschutzrechts wie Cloud-Diensteanbieter, Cloud-Kunden und potenzielle Kunden, Cloud-Prüfer und Cloud-Mittler. Sie decken das gesamte Spektrum der Cloud-Diensteanbieter ab[75].

4.3 Stärkung des Vertrauens in eine grenzüberschreitende Datenverarbeitung – Zertifizierung der Sicherheit

Wie in Erwägungsgrund 33 der Verordnung über den freien Verkehr nicht-personenbezogener Daten dargelegt, soll durch die Stärkung des Vertrauens in eine grenzüberschreitende Datenverarbeitung die Neigung von Marktteilnehmern und öffentlichen Stellen verringert werden, Datenlokalisierung stellvertretend für Datensicherheit zu verwenden. Im Anschluss an das von der Kommission im Jahr 2017 vorgeschlagene Paket zur Cybersicherheit[76] arbeitet die

---

[70] Europäischer Datenschutzausschuss: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (Leitlinien 1/2019 für Verhaltensregeln und Überwachungsstellen gemäß der Verordnung 2016/679), angenommen am 12. Februar 2019, Fassung zur öffentlichen Konsultation, online abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

[71] Europäischer Datenschutzausschuss: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (Leitlinien 1/2018 für die Zertifizierung und die Festlegung von Zertifizierungskriterien gemäß den Artikeln 42 und 43 der Verordnung 2016/679), angenommen am 23. Januar 2019, online abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en.

[72] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Geltungsende: 24. Mai 2018).

[73] Weitere Informationen über die EU-Verhaltensregeln für Cloud-Dienste: https://eucoc.cloud/en/home.html.

[74] Weitere Informationen über die CISPE-Verhaltensregeln: https://cispe.cloud/code-of-conduct/.

[75] Weitere Informationen über die CSA-Verhaltensregeln: https://gdpr.cloudsecurityalliance.org/.

[76] Weitere Informationen: https://ec.europa.eu/digital-single-market/en/cyber-security.

CSPCERT-Arbeitsgruppe derzeit an Empfehlungen für die Schaffung eines europäischen Cloud-Zertifizierungssystems, das der Kommission vorgelegt werden soll. Ein solches System könnte den freien Datenverkehr erleichtern, Cloud-Dienste besser vergleichbar machen und die Nutzung von Cloud-Diensten fördern. Die Kommission kann die ENISA (die Agentur der Europäischen Union für Cybersicherheit) damit beauftragen, ein mögliches System gemäß den einschlägigen Bestimmungen des Rechtsakts zur Cybersicherheit[77] auszuarbeiten. Ein solches System könnte sowohl personenbezogene als auch nicht-personenbezogene Daten erfassen. Zusätzlich zu den Vorgaben im Rechtsakt zur Cybersicherheit kann – wie in Abschnitt 4.2 hervorgehoben – auch die Datenschutz-Grundverordnung herangezogen werden, um nachzuweisen, dass geeignete Garantien für die Datensicherheit bestehen[78].

Abschließende Bemerkungen

Rechtssicherheit und Vertrauen in die Datenverarbeitung sind eine wichtige Voraussetzung, damit die EU das Potenzial ihrer Daten im Zuge der Entwicklung von Wertschöpfungsketten über Sektoren und Grenzen hinweg umfassend erschließen kann. Beide Verordnungen gewährleisten dies, und beide dienen dem Ziel des freien Datenverkehrs. Die Verordnung über den freien Verkehr nicht-personenbezogener Daten und die Datenschutz-Grundverordnung bilden zusammen das Fundament für den freien Verkehr aller Daten innerhalb der Europäischen Union und für eine in hohem Maße wettbewerbsfähige europäische Datenwirtschaft.

[77] Verordnung des Europäischen Parlaments und des Rates vom 17. April 2019 über die Agentur der Europäischen Union für Cybersicherheit (ENISA) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[78] Siehe Erwägungsgrund 74 des Rechtsakts zur Cybersicherheit.