EUROPÄISCHE
KOMMISSION

Brüssel, den 10.1.2017
COM(2017) 9 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

„AUFBAU EINER EUROPÄISCHEN DATENWIRTSCHAFT“

{SWD(2017) 2 final}

„AUFBAU EINER EUROPÄISCHEN DATENWIRTSCHAFT“

1. EINLEITUNG

Daten sind zu einer unerlässlichen Quelle für das Wirtschaftswachstum, die Schaffung von Arbeitsplätzen und den gesellschaftlichen Fortschritt geworden. Datenanalysen tragen zur Optimierung von Verfahren und Entscheidungen bei, ermöglichen Innovationen und erleichtern Zukunftsprognosen. Dieser globale Trend birgt gewaltige Möglichkeiten für unterschiedlichste Bereiche – von Gesundheit, Umwelt und Ernährungssicherheit über Klimapolitik und Ressourceneffizienz bis hin zu Energie, intelligenten Verkehrssystemen und intelligenten Städten.

Kennzeichnend für die „Datenwirtschaft“[1] ist ein Ökosystem unterschiedlicher Marktteilnehmer, wie Hersteller, Forscher und Infrastrukturanbieter, deren Zusammenarbeit dafür sorgt, dass Daten zugänglich und nutzbar sind. So können die Marktteilnehmer Wert aus diesen Daten schöpfen, indem sie vielfältige Anwendungen hervorbringen, die ein enormes Potenzial zur Verbesserung unseres Lebensalltags bieten (Verkehrsmanagement, Optimierung von Ernten oder Telegesundheitsdienste).

Der Wert der EU-Datenwirtschaft lag 2014 bei schätzungsweise 257 Mrd. EUR (1,85 % des EU-BIP)[2]. 2015 erreichte er bereits 272 Mrd. EUR (1,87 % des EU-BIP) und erzielte damit innerhalb eines Jahres ein Wachstum von 5,6 %. Nach derselben Schätzung dürfte mit einem weiteren Anstieg dieses Werts bis 2020 auf 643 Mrd. EUR bzw. auf 3,17 % des EU-BIP insgesamt zu rechnen sein, sofern die politischen und rechtlichen Rahmenbedingungen für die Datenwirtschaft rechtzeitig geschaffen werden.

Mit der Datenschutz-Grundverordnung (DS-GVO)[3] werden ab Mai 2018 statt der bislang noch bestehenden 28 nationalen Rechtsvorschriften für ganz Europa einheitliche Vorschriften gelten. Der neu geschaffene Mechanismus der federführenden Aufsichtsbehörde[4] stellt sicher, dass in der EU für die Aufsicht über ein Unternehmen, das Daten grenzüberschreitend verarbeitet, nur noch eine Datenschutzbehörde zuständig ist. Dadurch wird die einheitliche Auslegung der neuen Vorschriften gewährleistet. So wird in grenzüberschreitenden Fällen, in die mehrere nationale Datenschutzbehörden einbezogen sind, ein einziger Beschluss gefasst, damit sichergestellt ist, dass gemeinsame Probleme auch gemeinsam gelöst werden. Darüber hinaus schafft die DS-GVO gleiche

---

1 Die Datenwirtschaft misst, wie sich der Datenmarkt, d. h. der Markt, auf dem aus Rohdaten gewonnene digitale Daten als Produkte oder Dienste gehandelt werden, auf die Gesamtwirtschaft insgesamt auswirkt. Sie umfasst die Erzeugung, Erhebung, Speicherung, Verarbeitung, Verteilung, Analyse, Aufbereitung, Lieferung und Nutzung von Daten mit Hilfe der Digitaltechnik (*European Data Market Studie*, SMART 2013/0063, IDC, 2016).

2 *European Data Market Studie*, SMART 2013/0063, IDC, 2016.

3 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 95/56/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

4 Artikel 56 der Datenschutz-Grundverordnung.

Bedingungen für EU-Unternehmen und in Drittländern ansässige Unternehmen, denn Letztere werden dieselben Vorschriften anwenden müssen wie EU-Unternehmen, wenn sie in der EU Waren und Dienstleistungen anbieten oder Verhaltensmuster von Personen erfassen wollen. Ein größeres Vertrauen der Verbraucher kommt sowohl den in der EU als auch den in Drittländern ansässigen Wirtschaftsteilnehmern zugute.

Die e-Datenschutz-Richtlinie bezieht sich auf die Vertraulichkeit elektronischer Kommunikationsdienste in der EU. Die in Form einer Verordnung[5] parallel zu dieser Mitteilung vorgeschlagene Überarbeitung der e-Datenschutz-Richtlinie zielt auf ein hohes Schutzniveau in vollständiger Übereinstimmung mit der DS-GVO ab. Strenge Datenschutzvorschriften schaffen das Vertrauen, das die digitale Wirtschaft benötigt, um im Binnenmarkt weiter wachsen zu können.

Präsident Juncker betonte in seiner Rede zur Lage der Europäischen Union am 14. September 2016: „*Europäer sein heißt, ein Anrecht darauf zu haben, dass die eigenen personenbezogenen Daten durch strenge europäische Gesetze geschützt werden. Denn Europäer möchten keine Drohnen, die über ihre Köpfe kreisen und jede ihrer Bewegungen aufzeichnen. Europäer möchten auch keine Unternehmen, die alle ihre Mausklicks speichern. Deshalb haben Parlament, Rat und Kommission im Mai dieses Jahres eine gemeinsame europäische Datenschutz-Grundverordnung verabschiedet: ein strenges europäisches Gesetz, das für alle Unternehmen gilt – wo immer sie ihren Sitz haben und wann immer Daten verarbeitet werden. Denn in Europa spielt der Schutz der Privatsphäre eine Rolle. Das ist eine Frage der Menschenwürde.*“

In ihrer Mitteilung von 2012 über den „Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“[6] und ihrer Mitteilung „Für eine florierende datengesteuerte Wirtschaft“[7] aus dem Jahr 2014 verwies die Kommission darauf, dass für den freien Datenfluss zwischen den Mitgliedstaaten unionsweit moderne und kohärente Regeln benötigt werden, sowie dass im Vergleich zu den USA die Datenrevolution von der digitalen Wirtschaft in Europa nur schleppend aufgenommen wurde und es zudem an vergleichbaren industriellen Kapazitäten fehlte. Zusammenfassend stellte sie fest, dass ein nicht an den Handel mit Daten innerhalb der EU angepasstes rechtliches Umfeld zu einem unzureichenden Zugang zu großen Datensätzen, zu Zutrittsbeschränkungen für Marktneulinge und zu Hemmnissen für Investitionen führen kann.

Ungerechtfertigte **Beschränkungen des freien Datenverkehrs** sind geeignet, die Entwicklung der EU-Datenwirtschaft zu hemmen. Diese Beschränkungen bestehen in behördlichen Auflagen für den Ort der Speicherung und Verarbeitung von Daten. Die Frage des freien Datenverkehrs bezieht sich auf alle Arten von Daten: Unternehmen und Akteure der Datenwirtschaft arbeiten mit industriellen und von Maschinen generierten Daten (personenbezogenen und nicht personenbezogenen) sowie mit Daten, die durch menschliches Handeln erzeugt werden. In der Strategie für den digitalen Binnenmarkt hat die Kommission angekündigt, eine europäische Initiative vorzuschlagen, in der sie sich mit Beschränkungen des freien Datenverkehrs aus anderen Gründen als dem Schutz personenbezogener Daten in der EU sowie mit ungerechtfertigten Beschränkungen in

[5] COM(2017) 10.

[6] COM(2012) 9.

[7] COM(2014) 442.

Bezug auf den Speicher- und Verarbeitungsort der Daten befassen wird. Solche Beschränkungen umfassen Rechtsvorschriften der Mitgliedstaaten sowie Verwaltungsvorschriften und Verwaltungspraktiken mit derselben Wirkung. Mit dem Wachstum der Datenwirtschaft nimmt auch die Zahl der Vorschriften zu und damit die Unsicherheit in der Frage, wo Daten gespeichert oder verarbeitet werden können. Dies kann sich auf alle Wirtschaftszweige sowie auf private und öffentliche Organisationen auswirken, für die es schwierig werden könnte, innovativere bzw. kostengünstigere Datendienste in Anspruch zu nehmen. Ungerechtfertigte Lokalisierungsbeschränkungen beeinträchtigen die im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) festgelegte Dienstleistungs- und Niederlassungsfreiheit und laufen auch dem einschlägigen Sekundärrecht zuwider. Damit besteht die Gefahr einer Fragmentierung des Marktes, einer geringeren Dienstequalität für die Nutzer und einer geringeren Wettbewerbsfähigkeit vor allem kleinerer Datendiensteanbieter.

Angesichts der wachsenden Bedeutung von Daten und Datendiensten in der Weltwirtschaft und des möglichen Verhaltens von Drittländern in dieser Frage, sind ungerechtfertigte Lokalisierungsbeschränkungen auch Thema bei den Gesprächen, die die EU mit ihren Handelspartnern führt. Die EU-Datenschutzvorschriften dürfen nicht Gegenstand von Verhandlungen über Freihandelsabkommen sein. Wie bereits in der Mitteilung über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt[8] erläutert, sind Gespräche über den Datenschutz und Handelsverhandlungen mit Drittländern getrennt voneinander zu führen. Darüber hinaus wird die Kommission, wie in der Mitteilung „Handel für alle“[9] dargelegt, unter strikter Einhaltung und unbeschadet der EU-Datenschutzvorschriften die Handelsabkommen der EU nach Möglichkeit nutzen, um Vorschriften für den elektronischen Geschäftsverkehr und den grenzüberschreitenden Datenverkehr festzulegen und gegen neue Formen des digitalen Protektionismus vorzugehen.

Zudem wird in dem Maße, wie der datengesteuerte Wandel die Wirtschaft und Gesellschaft erfasst, eine ständig wachsende Menge an Daten von Maschinen oder Prozessen generiert, die sich auf neu entstehende Technik wie das Internet der Dinge, Fabriken der Zukunft und autonome vernetzte Systeme stützen. Die Konnektivität selbst verändert die Art und Weise, wie auf Daten zugegriffen werden kann: Der bislang in der Regel physische Datenzugriff erfolgt zunehmend per Fernzugang. Erst jetzt beginnt sich langsam abzuzeichnen, welche enorme Vielfalt bei den Quellen und Arten von Daten besteht und welche Fülle von Möglichkeiten sich in unterschiedlichsten Bereichen bietet, um Erkenntnisse aus diesen Daten beispielsweise für die Politikgestaltung zu gewinnen. Um diese Möglichkeiten nutzen zu können, müssen auf dem Datenmarkt tätige öffentliche und private Akteure Zugang zu großen und unterschiedlichen Datensätzen haben. Die Frage des Zugangs zu und der Übermittlung von Daten, die von diesen Maschinen oder Prozessen erzeugt werden, ist daher für das Entstehen einer Datenwirtschaft von zentraler Bedeutung und bedarf einer sorgfältigen Prüfung.

Weitere neue Fragen stellen sich in Bezug darauf, inwieweit die Haftungsregelungen für Schäden gelten, die durch den Fehler eines vernetzten Geräts oder eines Roboters verursacht werden, sowie in Bezug auf die Übertragbarkeit und Interoperabilität der Daten. Im Zusammenhang mit neuer Technik wie dem Internet der Dinge oder der

[8] COM(2017) 7.

[9] COM(2015) 497.

Robotik entstehen komplexe und hochkomplizierte gegenseitige Abhängigkeiten sowohl innerhalb eines Produkts (zwischen Hardware und Software) als auch zwischen vernetzten Geräten. Zudem können autonome Maschinen, durch deren unerwartetes und unbeabsichtigtes Verhalten möglicherweise Personen verletzt und Gegenstände beschädigt werden, neue Fragen aufwerfen. Diese Unklarheiten in Bezug auf die Anwendbarkeit bestehender Haftungs- und Sicherheitsvorschriften können zu Rechtsunsicherheit führen.

Wie im Zusammenhang mit dem digitalen Binnenmarkt bereits angekündigt, verfolgt die Kommission das Ziel, für die Datenwirtschaft einen klaren und angepassten Strategie- und Rechtsrahmen zu schaffen, indem noch bestehende Hindernisse für den Datenverkehr abgebaut und die von den neuen Datentechniken aufgeworfenen rechtlichen Fragen geklärt werden. Weitere Ziele, die auch mit dieser Mitteilung verfolgt werden, sind eine größere Verfügbarkeit und Nutzung von Daten, die Förderung neuer datengestützter Geschäftsmodelle sowie bessere Bedingungen für den Zugang zu Daten und die Entwicklung der Datenanalytik in der EU. Im Hinblick auf den „Aufbau einer europäischen Datenwirtschaft“ stellt die Kommission mit dieser Mitteilung konkrete Schwerpunktthemen zur Diskussion.

Diese Themen sind: freier Datenverkehr, Zugang zu und Übertragung von Daten, die von Maschinen erzeugt werden, Haftung und Sicherheit im Zusammenhang mit neu entstehender Technik sowie Übertragbarkeit nicht personenbezogener Daten, Interoperabilität und Normung. Zudem enthält diese Mitteilung Vorschläge für die Erprobung gemeinsamer regulatorischer Lösungen in einem realen Umfeld.

Zu den in dieser Mitteilung behandelten Fragen wird die Kommission einen umfassenden Dialog mit den Interessenträgern führen. Als ersten Schritt im Rahmen dieses Dialogs wird eine öffentliche Konsultation durchgeführt, die gleichzeitig mit dem Paket zur Datenwirtschaft veröffentlicht wird[10].

2. FREIER DATENVERKEHR

Eine Datenwirtschaft kann im Binnenmarkt nur dann gut funktionieren und Dynamik entfalten, wenn der Datenfluss ermöglicht und geschützt wird. In einem sich rasch verändernden technologischen Umfeld ist ein sicherer und zuverlässiger freier Datenverkehr eine wesentliche Voraussetzung für den in den Verträgen verankerten Schutz der vier Grundfreiheiten des EU-Binnenmarkts (freier Waren-, Personen-, Dienstleistungs- und Kapitalverkehr). Datendienste nehmen in der EU und weltweit rasant zu. Ein effizienter Binnenmarkt, der diesen Sektor nicht einschränkt, würde in erheblichem Umfang Möglichkeiten für mehr Wachstum und Arbeitsplätze schaffen.

Beschränkungen des freien Datenverkehrs in der EU, etwa durch ungerechtfertigte behördliche Datenlokalisierungsauflagen, können jedoch das Wachstum und die Innovation in der Datenwirtschaft sowie die Umsetzung grenzüberschreitender öffentlicher Dienste gefährden. In der Tat werden mit den Maßnahmen zur Datenlokalisierung digitale „Grenzkontrollen“ wiedereingeführt[11]. Sie reichen von

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

[11] OECD, „Emerging Policy Issues: Localisation Barriers to Trade“ (Neue politische Fragen: Lokalisierung als Handelshemmnis), 2015, sowie laufende Arbeiten.

Auflagen, mit denen Aufsichtsbehörden Finanzdienstleistern die lokale Datenspeicherung vorschreiben, über die Vorgabe, Daten mit Berufsgeheimnissen lokal zu speichern oder zu verarbeiten, bis zu pauschalen Archivierungsvorschriften für den öffentlichen Sektor, seine Daten, unabhängig von deren Sensibilität, lokal zu speichern.

Der Schutz der Privatsphäre ist ein berechtigtes Anliegen, sollte jedoch den Behörden nicht als Begründung dafür dienen, den freien Datenverkehr in ungerechtfertigter Weise einzuschränken. Wie bereits erläutert, enthält die DS-GVO einheitliche Vorschriften, die in der gesamten EU ein hohes Schutzniveau für personenbezogene Daten gewährleisten. Sie erhöht das Vertrauen der Verbraucher in Online-Dienste und stärkt die nationalen Datenschutzbehörden, die so für eine einheitliche Anwendung der Vorschriften in allen Mitgliedstaaten sorgen können. Die DS-GVO fördert das notwendige Vertrauen in die Datenverarbeitung und bildet die Grundlage für den freien Verkehr personenbezogener Daten in der EU. Sie verbietet Beschränkungen des freien Verkehrs personenbezogener Daten in der Union, sofern diese Beschränkungen mit dem Schutz der personenbezogenen Daten begründet werden[12]. Beschränkungen aus anderen Gründen als dem Schutz personenbezogener Daten (beispielsweise das Steuerrecht oder Rechnungslegungsvorschriften) fallen dagegen nicht unter diese Verordnung. Nicht gedeckt vom Anwendungsbereich der Verordnung sind nicht personenbezogene Daten, d. h. Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person[13] beziehen. Dabei kann es sich beispielsweise um von Maschinen erzeugte, nicht personenbezogene Daten handeln.

Beschränkungen der Datenlokalisierung können auf Rechtsvorschriften, Verwaltungsleitlinien oder auf eine Verwaltungspraxis zurückzuführen sein, denen zufolge Daten[14] in einem elektronischen Format[15] in einem bestimmten geografischen Gebiet oder Zuständigkeitsbereich gespeichert oder verarbeitet werden müssen. Mitunter erlassen Mitgliedstaaten derartige Auflagen in dem Glauben, dass die Aufsichtsbehörden lokal gespeicherte Daten leichter überprüfen können. Auch von Versicherungen wird eine örtliche Speicherung mit dem Schutz der Privatsphäre, Rechnungslegungszwecken, der Durchsetzung von Gesetzen sowie mit der Sicherheit der Daten begründet. In der Praxis tragen diese Maßnahmen aber nur selten dazu bei, dass die damit beabsichtigten Ziele erreicht werden.

Die Datensicherheit hängt von vielen Faktoren ab, die nicht nur den physischen Speicherort der Daten betreffen, sondern auch die Wahrung der Vertraulichkeit und der Integrität der Daten, wenn diese außerhalb ihres Speicherorts verfügbar gemacht werden. So lassen sich eine wirklich sichere Datenspeicherung und -verarbeitung weniger durch Beschränkungen der Datenlokalisierung realisieren, als vielmehr durch modernste und bewährte Verfahren des IKT-Managements – und das in einer Größenordnung, die über einzelne Systeme weit hinausgeht. Um Daten sicher vor örtlich begrenzten Naturkatastrophen oder vor Cyberangriffen zu schützen, können beispielsweise

---

12 Artikel 1 Absatz 3. So gilt eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Webseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter als personenbezogene Daten, wenn dieser über die rechtlichen Mittel verfügt, die es ihm erlauben, anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, die betreffende Person bestimmen zu lassen. Siehe Urteil in der Rechtssache C-582/14, Breyer, ECLI:EU:C:2016:779, Rdnr. 49.

13 Gemäß Artikel 4 Absatz 1 der Datenschutz-Grundverordnung.

14 Sowohl in Bezug auf Daten in privater wie auch in öffentlicher Hand.

15 Einschließlich Datensatzkopien.

Datenspeichereinrichtungen in verschiedenen Mitgliedstaaten zur gegenseitigen Absicherung genutzt und die in der Richtlinie über die Sicherheit von Netz- und Informationssystemen[16] (NIS-Richtlinie) vorgesehenen technischen und organisatorischen Vorkehrungen getroffen werden. Zudem ließe sich die Verfügbarkeit von Daten für die Zwecke der Rechtsetzung oder Aufsicht, die in keiner Weise in Frage gestellt wird, eher durch eine bessere Zusammenarbeit zwischen nationalen Behörden oder zwischen diesen Behörden und dem Privatsektor gewährleisten, als durch Lokalisierungsauflagen. So könnten sich in einem Bereich wie den Finanzdienstleistungen, in dem Aufsichtsbehörden eng zusammenarbeiten, Datenlokalisierungsauflagen sogar als kontraproduktiv erweisen[17].

In bestimmten Zusammenhängen oder in Bezug auf bestimmte Daten können Datenlokalisierungsauflagen allerdings insbesondere dann gerechtfertigt und verhältnismäßig sein, wenn beispielsweise die sichere Behandlung bestimmter Daten über kritische Energieinfrastrukturen oder die Verfügbarkeit elektronischer Beweismittel (z. B. als lokal vorgehaltene Datenbankkopien) für Strafverfolgungsbehörden oder die lokale Speicherung von Daten in bestimmten öffentlichen Registern gewährleistet werden müssen und Modalitäten für eine funktionierende grenzüberschreitende Zusammenarbeit noch nicht bestehen.

Leider geht der Trend sowohl international als auch in Europa in Richtung verstärkter Datenlokalisierung, was häufig auf der falschen Vorstellung beruht, dass lokal angesiedelte Dienste automatisch sicherer sind als grenzüberschreitende Dienste. Zudem üben der Mangel an transparenten Vorschriften und das starke Gefühl, dass Daten besser lokal gespeichert werden sollten, großen Einfluss auf den Markt für Datendienste aus. Das kann dazu führen, dass Unternehmen und Organisationen des öffentlichen Sektors kaum Zugang zu kostengünstigeren oder innovativeren Datendiensten haben oder dass grenzüberschreitend tätige Unternehmen gezwungen sind, zusätzliche Kapazitäten für die Speicherung und Verarbeitung von Daten zu schaffen. Auch könnten datenintensive Unternehmen, vor allem Startups und KMU, in der Ausweitung ihrer Tätigkeiten und bei der Erschließung neuer Märkte (weil sie beispielsweise in Datenzentren in 28 Mitgliedstaaten investieren müssten) oder bei der Zentralisierung ihrer Daten- und Analysekapazitäten behindert werden.

Derzeit wird in Europa die Endnachfrage nach IKT-bezogenen Diensten (Beratung, Hosting, Entwicklung) zu 84 % innerhalb der EU gedeckt. Würde es diesen Diensten durch eine Aufhebung von Lokalisierungsbeschränkungen erleichtert, innerhalb der EU auch grenzüberschreitend tätig zu werden, ließe sich infolge von Kosteneinsparungen und Effizienzgewinnen das BIP der EU um bis zu 8 Mrd. EUR pro Jahr steigern[18].

---

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

17 Zahlreiche EU-Bestimmungen in Bezug auf Finanzdienstleistungen und das europäische System für die Finanzaufsicht machen es notwendig, dass die Aufsichtsbehörden an jedem Ort in der EU Zugang zu Daten der Finanzinstitutionen und zu Finanztransaktionen haben. Die Anforderung, dass Daten in einem bestimmten nationalen Gebiet gespeichert werden müssen, oder Bestimmungen, die den Zugang der Aufsichtsbehörden an Verwaltungsverfahren knüpfen, könnten dazu führen, dass diese Aufsichtsbehörden nur bedingt Zugang zu den Daten erhalten, die für die Erfüllung ihres Auftrags unerlässlich sind.

18 „Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States“ (Freisetzung interner Datenflüsse in der EU: Eine wirtschaftliche Bewertung der

Die Datenlokalisierungsvorschriften mindern auch die Bereitschaft, die Speicherung und Rechenkapazitäten in größerem Umfang in eine Cloud zu verlagern. Zudem hat dies auch weitergehende gesellschaftliche Folgen. So könnte eine effizientere Nutzung von IT-Ressourcen dazu beitragen, den Energieverbrauch und die CO_2-Emissionen um netto 30 % oder mehr zu senken. Ein kleines Unternehmen, das eine Cloud nutzt, könnte seinen Energieverbrauch und seine CO_2-Emissionen um über 90 % verringern, wenn es seine Anwendungen in die Cloud verlagert, statt dieselben Anwendungen auf der eigenen Infrastruktur zu belassen. Der Weltmarkt für energieeffiziente Datenzentren dürfte Prognosen zufolge bis Ende 2020 auf 90 Mrd. EUR anwachsen. Ein fragmentierter Markt für Datendienste würde die volle Entfaltung dieser energieeffizienteren Dienste in der EU behindern und auch die Investitionsbereitschaft gefährden.

Als logische Konsequenz aus den Verpflichtungen, die ihnen aus den Bestimmungen des AEUV über die Dienstleistungs- und Niederlassungsfreiheit sowie aus dem einschlägigen Sekundärrecht erwachsen, sollten sich die Mitgliedstaaten bei allen Maßnahmen, die sich auf die Speicherung oder Verarbeitung von Daten auswirken, vom **„Grundsatz des freien Datenverkehrs in der EU“** leiten lassen, denn nur so können die vorstehend skizzierten Fragen und Beschränkungen bewältigt werden und kann die europäische Datenwirtschaft ihr Potenzial voll ausschöpfen. Jede bestehende oder neue Beschränkung in Bezug auf die Datenlokalisierung müsste auf der Grundlage des AEUV und des einschlägigen Sekundärrechts sorgfältig begründet werden, damit überprüft werden kann, ob sie im Hinblick auf ein übergeordnetes Ziel von allgemeinem Interesse, wie etwa der öffentlichen Sicherheit, notwendig und verhältnismäßig ist[19].

Der Grundsatz des freien Verkehrs personenbezogener Daten[20] ist im Primär- und Sekundärrecht verankert und sollte auch für die Fälle gelten, in denen die DS-GVO den Mitgliedstaaten das Recht einräumt, bestimmte Aspekte selbst zu regulieren. Die Mitgliedstaaten sollten dazu angehalten werden, die Öffnungsklauseln der DS-GVO nicht für weitere Einschränkungen des freien Datenverkehrs in Anspruch zu nehmen.

In seinen Schlussfolgerungen vom 15. Dezember 2016 forderte der Europäische Rat, dass noch verbleibende Hindernisse innerhalb des Binnenmarkts, auch solche, die den freien Datenverkehr beeinträchtigen, beseitigt werden[21].

Die Kommission wird zur Verwirklichung des Grundsatzes des freien Datenverkehrs wie folgt zweistufig vorgehen:

- Nach der Veröffentlichung dieser Mitteilung wird die Kommission mit den Mitgliedstaaten und anderen Interessenträgern – ausgehend von den bislang von

---

Datenlokalisierungsmaßnahmen in den EU-Mitgliedstaaten), ECIPE, 2016; die Berechnung geht von einem höheren Wettbewerbsdruck bei einem vollständig preistransparenten „industriellen“ digitalen Binnenmarkt aus.

19 Hierbei ist zu berücksichtigen, dass die Ausnahmeregelungen des AEUV restriktiv auszulegen sind. Zum einschlägigen Sekundärrecht zählen u. a. die Datenschutz-Grundverordnung, die Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr), die Richtlinie 2006/123/EG (Dienstleistungsrichtlinie) und im Hinblick auf die Entwürfe technischer Vorschriften und von Vorschriften für die Dienste der Informationsgesellschaft die Richtlinie (EU) 2015/1535 (Transparenzrichtlinie).

20 Der freie Verkehr personenbezogener Daten ist in Artikel 16 AEUV sowie im geltenden und künftigen EU-Datenschutzrecht verankert. Artikel 1 Absatz 3 der Datenschutz-Grundverordnung lautet: „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.“

21 http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/

der Kommission festgestellten Beschränkungen – einen strukturierten Dialog über Fragen der Rechtfertigung und der Verhältnismäßigkeit von Datenlokalisierungsmaßnahmen führen.

- Abhängig vom Ergebnis dieses Dialogs und sobald weitere Erkenntnisse aus der begleitenden öffentlichen Konsultation über das Ausmaß und die Art der Datenlokalisierungsbeschränkungen und deren Auswirkungen vor allem auf KMU und Startups vorliegen, wird die Kommission, falls notwendig, Vertragsverletzungsverfahren zur Beseitigung ungerechtfertigter oder unverhältnismäßiger Datenlokalisierungsmaßnahmen einleiten und möglicherweise auch weitere Initiativen zum freien Datenverkehr ergreifen. Alle in diesem Zusammenhang ergriffenen Folgemaßnahmen werden sich auf den Grundsatz der besseren Rechtsetzung stützen.

3. DATENZUGANG UND -ÜBERTRAGUNG

Maschinen und Prozesse, die auf neu aufkommender Technik wie dem Internet der Dinge beruhen, erzeugen immer größere Mengen an Daten. Solche Daten werden zunehmend als Kernkomponente für neue, innovative Dienste genutzt, um Produkte oder Produktionsprozesse zu verbessern und die Entscheidungsfindung zu unterstützen.

Die Vielfalt der von diesen Maschinen oder Prozessen erzeugten Daten bietet Akteuren des Datenmarkts eine Fülle von Möglichkeiten für Innovationen und für die Auswertung dieser Daten. So könnten Daten, die von in modernen landwirtschaftlichen Betrieben verwendeten Sensoren erfasst werden, für eine Anwendung zur Optimierung der Ernte genutzt werden, und Daten, die von Sensoren in Ampeln erfasst werden, ließen sich für das Verkehrsmanagement oder für die Streckenoptimierung nutzen.

Um den Wert derartiger Daten optimal ausschöpfen zu können, müssen die Marktteilnehmer Zugang zu großen und vielfältigen Datensätzen haben. Dies wird jedoch zum Problem, wenn die Erzeuger der Daten, diese für sich behalten und die Daten folglich nur isoliert analysiert werden. Die Frage des Zugangs zu und der Übertragung von mit solchen Maschinen oder Prozessen erzeugten Rohdaten (d. h. von Daten, die seit ihrer Erfassung weder verarbeitet noch verändert wurden) ist daher für das Entstehen einer Datenwirtschaft von zentraler Bedeutung und bedarf einer sorgfältigen Prüfung.

Die Frage des Zugangs zu von Maschinen erzeugten Daten wird derzeit in verschiedenen Sektoren (Verkehr, Energiemärkte, intelligentes Wohnumfeld, Gesundheit und Pflege) geprüft.

Bevor näher auf die aktuelle Situation beim Datenzugang in der EU eingegangen wird, sollte zunächst geklärt werden, um welche Art von Daten es geht.

3.1. Art der in Frage kommenden Daten

Allgemein können Daten personenbezogen oder nicht personenbezogen sein. So können Daten, die von Sensoren zur Messung der Temperatur in einer Wohnung erfasst werden, ihrem Wesen nach personenbezogen sein, wenn sie mit einer lebenden Person in Bezug gesetzt werden können, während Daten zur Bodenfeuchtigkeit nicht personenbezogen sind. Mit Hilfe der Anonymisierung können personenbezogene Daten in nicht

personenbezogene Daten umgewandelt werden. Gelten Daten als personenbezogen[22], finden die Datenschutzvorschriften, insbesondere die Datenschutz-Grundverordnung, Anwendung.

Daten werden von Maschinen ohne den unmittelbaren Eingriff eines Menschen im Rahmen von Computerprozessen, Anwendungen oder Diensten oder auch durch Sensoren erzeugt, die Informationen von virtuellen oder realen Geräten oder Maschinen oder von einer Software erhalten.

Ihrem Wesen nach sind von Maschinen erzeugte Daten entweder personenbezogen oder nicht personenbezogen. Wenn von Maschinen erzeugte Daten die Identifizierung einer natürlichen Person ermöglichen, gelten sie als personenbezogene Daten, so dass alle Vorschriften über personenbezogene Daten solange anwendbar sind, bis die fraglichen Daten vollständig anonymisiert wurden (beispielsweise im Falle von Standortdaten aus mobilen Anwendungen).

Der Umgang mit personenbezogenen und nicht personenbezogenen Daten durch Unternehmen und Akteure der Datenwirtschaft ist ein Thema, das sowohl den freien Datenverkehr als auch die neu auftretenden Fragen im Zusammenhang mit dem Zugang zu Daten und deren Übertragung betrifft, zumal Datenflüsse und Datensätze in der Regel beide Arten von Daten enthalten. Jede politische Maßnahme muss dieser wirtschaftlichen Realität und dem Rechtsrahmen zum Schutz personenbezogener Daten unter Achtung der individuellen Grundrechte Rechnung tragen.

3.2. Einschränkung des Datenzugangs

Zur Prüfung dieser neu auftretenden Fragen ist zunächst zu klären, wie Unternehmen und andere Marktteilnehmer Zugang zu den in der Datenwirtschaft benötigten großen und vielfältigen Datensätzen erhalten können.

Es zeigt sich[23], dass Unternehmen, die über große Datenmengen verfügen, in der Regel eher ihre hauseigenen Datenanalysekapazitäten nutzen. In den meisten Fällen werden Daten von ein und demselben Unternehmen erzeugt und analysiert, und selbst wenn die Datenanalyse an Unterauftragnehmer vergeben wird, findet eine nochmalige Verwendung der Daten nicht unbedingt statt. Zudem behalten Hersteller, Diensteanbieter oder sonstige Marktteilnehmer die mit ihren Maschinen oder mit Hilfe ihrer Produkte oder Dienste erzeugten Daten für sich und schränken damit die etwaige Wiederverwendung dieser Daten auf nachgelagerten Märkten ein. Viele Unternehmen nutzen die Möglichkeit einer nutzerfreundlichen Anwendungsprogrammierschnittstelle (API)[24] nicht oder lassen sie nicht zu. Solche Schnittstellen legen fest, wie verschiedene Anwendungen miteinander interagieren sollen und können als sichere Zugangspunkte für eine neue und innovative Nutzung der Daten im Besitz des Unternehmens dienen.

---

22 Gemäß Artikel 4 Absatz 1 der Datenschutz-Grundverordnung.

23 IDC, „European Data Market Study“ (Untersuchung des europäischen Datenmarkts), erster Zwischenbericht, 2016; „Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability“ (Hintergrunduntersuchung zur Folgenabschätzung über neu aufkommende Fragen in Bezug auf Dateneigentum, Interoperabilität, (Wieder)verwendbarkeit, Zugang zu Daten und Haftung), erster Zwischenbericht, 2016; GD Connect – hochrangige Konferenz vom 17. Oktober 2016.

24 Beispiele: https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

Daher bleibt der Austausch von Daten insgesamt begrenzt. Es bilden sich zwar langsam immer mehr Datenmärkte heraus, doch werden sie bisher noch kaum genutzt. Dies mag daran liegen, dass Unternehmen nicht mit den richtigen Instrumenten und Fähigkeiten ausgestattet sind, den wirtschaftlichen Wert ihrer Daten zu bemessen, oder befürchten, ihren Wettbewerbsvorteil einzubüßen oder zu gefährden, wenn Wettbewerber Zugang zu ihren Daten erhalten.

3.3. Von Maschinen erzeugte Rohdaten: Rechtslage in der EU und auf nationaler Ebene

Von Maschinen erzeugte Rohdaten werden vom geltenden Recht am geistigen Eigentum nicht geschützt, da sie nicht als Ergebnis einer intellektuellen Anstrengung gelten bzw. ihnen keinerlei Originalität zugesprochen wird. Das in der Richtlinie 96/9/EG über den Schutz von Datenbanken festgelegte eigenständige Schutzrecht, das dem Hersteller einer Datenbank das Recht gibt, die Entnahme und/oder die Wiederverwendung der Gesamtheit oder eines wesentlichen Teils des Inhalts einer Datenbank zu unterbinden, bietet nur unter der Voraussetzung Schutz, dass der Aufbau dieser Datenbank erhebliche Investitionen für die Beschaffung, Überprüfung oder Darstellung ihres Inhalts erforderlich machte. Mit der jüngst verabschiedeten Richtlinie (EU) 2016/943, die bis Juni 2018 in nationales Recht umzusetzen ist, werden Geschäftsgeheimnisse vor einer rechtswidrigen Aneignung sowie vor rechtswidriger Nutzung und Offenlegung geschützt. Damit Daten als „Geschäftsgeheimnis“ gelten können, müssen Maßnahmen zur Wahrung der Geheimhaltung der Informationen ergriffen werden, die das „intellektuelle Kapital“ des Unternehmens darstellen.

Nach der in verschiedenen Mitgliedstaaten geltenden Rechtslage können Rechtsansprüche in Bezug auf Daten nur dann abgeleitet werden, wenn diese Daten bestimmte Bedingungen erfüllen, um beispielsweise als geistiges Eigentum, als Datenbank oder als Geschäftsgeheimnis zu gelten. In der Regel erfüllen auf EU-Ebene die von Maschinen erzeugten Rohdaten für sich genommen die einschlägigen Bedingungen nicht.

Daher besteht derzeit weder auf nationaler noch auf Unionsebene eine umfassende Regelung – weder für den Umgang mit von Maschinen erzeugten Rohdaten, bei denen es sich nicht um personenbezogene Daten handelt, noch für deren wirtschaftliche Nutzung oder Handelbarkeit. Die Frage wird weitestgehend durch vertragliche Vereinbarungen geregelt. Möglicherweise reicht es aus, auf die in der Union verfügbaren Rechtsinstrumente des allgemeinen Vertrags- und Wettbewerbsrechts zurückzugreifen. Auch wäre es denkbar, dass in einigen Sektoren freiwillige Vereinbarungen oder Rahmenabkommen zur Anwendung kommen. Verfügen die verschiedenen Marktteilnehmer jedoch nicht über die gleiche Verhandlungsposition, könnten marktgestützte Lösungen allein sich als nicht ausreichend erweisen, um für Fairness und Innovationsfreundlichkeit zu sorgen, den Zugang für Marktneulinge zu erleichtern und Lock-in-Effekte zu vermeiden.

3.4. Die Situation in der Praxis

In einigen Fällen kann es vorkommen, dass die Hersteller oder Diensteanbieter faktisch zu „Eigentümern“ der von ihren Maschinen oder Prozessen erzeugten Daten werden, auch wenn das Eigentum dieser Maschinen bei den Nutzern liegt. Für die Hersteller kann

die faktische Kontrolle über diese Daten ein Differenzierungsmerkmal sein und ihnen einen Wettbewerbsvorteil verschaffen. Dies kann jedoch dann zum Problem werden, wenn der Nutzer, wie so häufig, vom Hersteller daran gehindert wird, die Nutzung der Daten durch Dritte zuzulassen.

Die verschiedenen Marktteilnehmer, die die Kontrolle über die Daten haben, können abhängig von den jeweiligen Besonderheiten der Märkte Lücken in der Rechtslage oder die vorstehend erläuterten rechtlichen Unklarheiten ausnutzen, und den Nutzern unfaire Standardvertragsbedingungen aufzwingen oder zu technischen Mitteln wie proprietären Formaten oder Verschlüsselung greifen. Zwar haben einige Mitgliedstaaten den Anwendungsbereich der Verbraucherschutzrichtlinie über missbräuchliche Vertragsklausen auch auf Verträge zwischen Unternehmen (B2B) ausgeweitet, das trifft jedoch nicht auf alle Mitgliedstaaten zu, weshalb es beispielsweise vorkommen kann, dass Nutzer und Unternehmen in Vereinbarungen über ausschließliche Verwertungsrechte feststecken. Möglicherweise kommt es dazu, dass Daten freiwillig geteilt werden, doch die Aushandlung entsprechender Verträge könnte bei ungleichen Verhandlungspositionen erhebliche Transaktionskosten für die schwächeren Parteien nach sich ziehen, die Rechtsberatung in Anspruch nehmen müssen.

3.5. Ein künftiger EU-Rahmen für den Datenzugang

Einige Mitgliedstaaten prüfen derzeit, wie der Zugang zu von Maschinen erzeugten Daten gewährleistet werden kann, und könnten beschließen, diese Frage selbst zu regeln. Ein unkoordiniertes Vorgehen birgt jedoch die Gefahr einer Fragmentierung und würde dem Aufbau einer EU-Datenwirtschaft sowie von grenzüberschreitenden Datendiensten und Datentechniken im Binnenmarkt schaden.

Deshalb beabsichtigt die Kommission, mit den Mitgliedstaaten und anderen Interessenträgern einen Dialog darüber aufzunehmen, wie ein etwaiger EU-Rechtsrahmen für den Datenzugang aussehen könnte. Nach Auffassung der Kommission sollte sich dieser Dialog darum drehen, wie die folgenden Ziele möglichst wirksam erreicht werden können:

- **Verbesserung des Zugangs zu anonymen, von Maschinen erzeugten Daten:** Indem die von Maschinen generierten Daten geteilt, wiederverwendet und aggregiert werden, bewirken sie eine Wertschöpfung, werden zu Innovationsquellen und ermöglichen unterschiedlichste Geschäftsmodelle[25].

- **Erleichterungen und Anreize für das Teilen solcher Daten:** Jede künftige Lösung sollte den wirksamen Datenzugang fördern und hierbei beispielsweise etwaige Unterschiede in der Verhandlungsposition der Marktteilnehmer berücksichtigen.

- **Schutz von Investitionen und Vermögen:** Jede künftige Lösung sollte – als Beitrag zur Innovation – die berechtigten Interessen der Marktteilnehmer, die in die Produktentwicklung investieren, berücksichtigen und eine angemessene Rendite gewährleisten. Gleichzeitig sollte jede künftige Lösung einen fairen

[25] Auf personenbezogene Daten findet dabei die Datenschutz-Grundverordnung Anwendung.

Vorteilsausgleich für alle an der Wertschöpfungskette Beteiligten (Dateninhaber[26], Auftragsverarbeiter und Anbieter von Anwendungen) sicherstellen.

- **Vermeidung der Offenlegung vertraulicher Daten:** Jede künftige Lösung sollte so ausgelegt sein, dass das Risiko der Offenlegung vertraulicher Daten vor allem gegenüber bereits bestehenden oder potenziellen Wettbewerbern so gering wie möglich gehalten wird. Hierzu sollte eine geeignete Klassifizierung der Daten durchgeführt werden können, bevor darüber entschieden wird, ob bestimmte Daten weitergegeben werden können oder nicht.

- **Minimierung von Lock-in-Effekten:** Die ungleiche Verhandlungsposition von Unternehmen und Privatpersonen sollte berücksichtigt werden. Vor allem für KMU, Startups und Privatpersonen sollten Lock-in-Effekte vermieden werden.

Im Verlauf des Dialogs mit den Interessenträgern beabsichtigt die Kommission, zur Frage des Zugangs zu von Maschinen erzeugten Daten die folgenden Möglichkeiten zu erörtern, die auf unterschiedlichen Ebenen ansetzen:

- **Leitfäden zur Schaffung von Anreizen für Unternehmen, Daten zu teilen:** Um den Folgen abweichender nationaler Bestimmungen entgegenzuwirken und den Unternehmen mehr Rechtssicherheit zu geben, könnte die Kommission einen Leitfaden herausgeben, wie Kontrollrechte über nicht personenbezogene Daten vertraglich geregelt werden sollten. Dieser Leitfaden würde sich auf das geltende Recht, insbesondere die Transparenz- und Fairness-Anforderungen des EU-Marketing- und -Verbraucherrechts sowie auf die Richtlinie über Geschäftsgeheimnisse und das Urheberrecht, vor allem auf die Datenbankrichtlinie, stützen. Für 2017 plant die Kommission eine Bewertung der Datenbankrichtlinie.

- **Förderung der Entwicklung technischer Lösungen für die zuverlässige Identifizierung und den Austausch von Daten:** Eine echte Kontrolle über die auf dem Markt befindlichen Daten lässt sich nur mit einer Rückverfolgbarkeit und klaren Identifizierung der Datenquellen bewerkstelligen. Um Vertrauen in das System zu schaffen, kann es sich als notwendig erweisen, zuverlässige und möglichst genormte Protokolle für die durchgehende Identifizierung von Datenquellen festzulegen. Auch API können den Aufbau eines Ökosystems von Anwendungs- und Algorithmen-Entwicklern fördern, die ein Interesse an den Daten haben, die sich im Besitz von Unternehmen befinden. API können Unternehmen und Behörden helfen, die unterschiedlichen Möglichkeiten zu ermitteln, wie sie die in ihrem Besitz befindlichen Daten wiederverwenden und nutzen können. Vor diesem Hintergrund könnte, unterstützt durch technische Leitfäden, eine breitere Nutzung offener, genormter und gut dokumentierter API einschließlich Feststellung bewährter Verfahren und deren Weitergabe an Unternehmen und Behörden in Erwägung gezogen werden. Hierunter fällt auch die Bereitstellung von Daten in maschinenlesbaren Formaten mit den zugehörigen Metadaten.

[26] Die Stelle, die die von Maschinen erzeugten Daten in der Praxis verwaltet und speichert.

- **Standardvertragsklauseln:** Mit Standardklauseln könnten ausgewogene Vorgaben für datenbezogene Verträge gemacht werden, wobei die laufende Gesamtbeurteilung der Richtlinie über missbräuchliche Vertragsklausen gebührend zu berücksichtigen wäre. Sie könnten mit der Einführung einer Kontrolle über unlautere Verträge in Vertragsbeziehungen zwischen Unternehmen gekoppelt werden[27], sodass Vertragsklauseln, die erheblich von den Standardvorgaben abweichen, als nichtig gelten würden. Zudem könnten sie durch von Interessenträgern ausgearbeitete Empfehlungen für Standardvertragsbedingungen ergänzt werden. Damit ließen sich unter Beibehaltung eines hohen Maßes an Vertragsfreiheit die rechtlichen Hindernisse für kleine Unternehmen und die Unausgewogenheit in den Verhandlungspositionen verringern.

- **Zugang im öffentlichen Interesse oder für wissenschaftliche Zwecke:** Behörden könnte der Zugang zu Daten gewährt werden, wenn dies im „allgemeinem Interesse" liegt und die Funktionsfähigkeit des öffentlichen Sektors erheblich verbessern würde, indem beispielsweise Statistikämter Zugang zu Geschäftsdaten bekämen oder die Verkehrsleitsysteme Daten von Privatfahrzeugen in Echtzeit erhielten. So würde der Zugang von Statistikämtern zu Geschäftsdaten dazu beitragen, den Aufwand für Wirtschaftsteilnehmer zu verringern, ihren Berichtspflichten nachzukommen. Genauso ist es für die wissenschaftliche Forschung auf Gebieten wie der Medizin, der Sozial- und Umweltwissenschaften unerlässlich, Zugang zu Daten aus unterschiedlichen Quellen zu erhalten und die Daten kombinieren zu können.

- **Rechte des Datenerzeugers:** Dem „Erzeuger der Daten", d. h. dem Eigentümer oder langfristigen Nutzer (d. h. dem Besitzer) des Gerätes könnte das Recht gewährt werden, nicht personenbezogene Daten zu nutzen oder anderen deren Nutzung zu gestatten. Dieser Ansatz zielt darauf ab, für eine klare Rechtslage zu sorgen und den Datenerzeugern mehr Entscheidungsfreiheit zu geben, indem sie Nutzern die Möglichkeit eröffnen können, mit ihren Daten zu arbeiten, wodurch ein Beitrag dazu geleistet würde, den ausschließlichen Zugang zu von Maschinen erzeugten Daten aufzuheben. Allerdings müsste genau festgelegt werden, welche Ausnahmen insbesondere für den nicht ausschließlichen Zugang zu den Daten durch den Hersteller oder durch Behörden gelten, etwa für das Verkehrsmanagement oder aus Umweltgründen. Im Fall personenbezogener Daten wird die betreffende Person ihr Recht beibehalten, ihre zuvor gegebene Einwilligung in die Nutzung der Daten später jederzeit zu widerrufen. Personenbezogene Daten müssen, bevor ihre weitere Nutzung durch die andere Partei gestattet werden darf, so anonymisiert werden, dass Einzelpersonen nicht mehr identifiziert werden können. Schließlich gilt die Datenschutz-Grundverordnung solange für personenbezogene Daten (unabhängig davon, ob sie von Maschinen oder anderweitig erzeugt wurden), bis die Daten anonymisiert wurden.

[27]. Natürlich müssten die Vorgaben für unlautere Vertragsbestimmungen zwischen Unternehmen (B2B) anders festgelegt werden als für Verträge zwischen Unternehmen und Verbrauchern (B2C), um dem höheren Maß an Vertragsfreiheit in den Geschäftsbeziehungen zwischen Unternehmen Rechnung zu tragen.

- **Zugang gegen Entgelt:** Für die Inhaber von Daten, wie Hersteller, Diensteanbieter und andere, könnte ein möglicherweise auf bestimmte Grundsätze (wie Fairness, Angemessenheit und Nichtdiskriminierung) gestützter Rahmen entwickelt werden, auf dessen Grundlage sie ihre Daten nach Anonymisierung gegen Entgelt zugänglich machen können. Dabei müssten berechtigte Interessen, wie der Schutz von Geschäftsgeheimnissen, berücksichtigt werden. Um den Besonderheiten jeder Branche Rechnung zu tragen, sind auch unterschiedliche Zugangsregelungen für die einzelnen Branchen und/oder Geschäftsmodelle denkbar. So könnte in einigen Fällen der vollständig oder teilweise offene Zugang zu Daten sowohl für Unternehmen als auch für die Gesellschaft der bessere Weg sein.

Die Kommission wird zu der vorstehenden Frage die Interessenträger konsultieren, um mehr Erkenntnisse über die Funktionsweise der Datenmärkte je nach Sektor zu gewinnen und mögliche Lösungen zu sondieren. In diesem Zusammenhang kommt es darauf an, eine breit angelegte Diskussion über mögliche Lösungen zu führen und unbeabsichtigte Nebeneffekte zu vermeiden, die die Innovation ersticken oder den Wettbewerb behindern würden. Darüber hinaus werden sektorspezifische Diskussionen mit einschlägigen Interessenträgern der Daten-Wertschöpfungskette geführt.

4. HAFTUNG

Ein weiteres, sich neu abzeichnendes Thema ist die Anwendung der geltenden Haftungsregelungen in der Datenwirtschaft auf Produkte und Dienste, die aus neu entstehender Technik wie Internet der Dinge, Fabriken der Zukunft und automatisierten vernetzten Systemen hervorgehen. Das Internet der Dinge ist ein ständig wachsendes Netz alltäglicher Objekte, wie Uhren, Fahrzeuge und Thermostate, die mit dem Internet verbunden sind. Autonome vernetzte Systeme, wie selbstfahrende Fahrzeuge, handeln unabhängig vom Menschen, haben kognitive Fähigkeiten und interpretieren ihr Umfeld. Bei dieser neu entstehenden Technik werden mit Hilfe von Sensoren unterschiedlichste Daten erfasst, die häufig benötigt werden, damit das Produkt oder der Dienst funktioniert.

All diese Innovationen sind zwar geeignet, die Sicherheit und Lebensqualität zu erhöhen, doch sind bei keinem Gerät Konzeptionsfehler, Fehlfunktionen oder Manipulationen auszuschließen. Gründe hierfür können in der Übermittlung fehlerhafter Daten durch einen Sensor liegen, etwa aufgrund eines Softwarefehlers, Anbindungsproblemen oder des nicht ordnungsgemäßen Betriebs des Geräts. Es liegt im Wesen dieser Systeme, dass es schwierig werden kann, die genaue Ursache für ein Problem zu finden, das Schäden hervorruft, woraus sich die Frage ergibt, wie gewährleistet werden kann, dass diese Systeme für den Nutzer sicher sind, dass die Gefahr von Schäden möglichst gering bleibt, und wer für auftretende Schäden haftet.

Daher ist es von zentraler Bedeutung für das Entstehen der Datenwirtschaft, wie sowohl den Nutzern als auch den Herstellern solcher Geräte in Bezug auf ihre potenzielle Haftung Sicherheit gegeben werden kann.

4.1. EU-Haftungsregelungen

Im Zivilrecht wird grundsätzlich zwischen zwei Arten rechtlicher Haftung unterschieden: vertragliche Haftung, bei der sich die Schadenshaftung aus dem Vertragsverhältnis

zwischen den Parteien ergibt, und außervertragliche Haftung[28], bei der Haftungsfragen außerhalb eines Vertrags geklärt werden. Eine wichtige Art der außervertraglichen Haftung ist die Produkthaftung. Auf EU-Ebene legt die Richtlinie über die Haftung für fehlerhafte Produkte (85/374/EWG) (die „Produkthaftungsrichtlinie“) die Grundsätze für die verschuldensunabhängige Haftung fest: Entsteht einem Verbraucher durch ein fehlerhaftes Produkt ein Schaden, haftet der Hersteller möglicherweise auch dann, wenn kein fahrlässiges oder fehlerhaftes Handeln seinerseits vorliegt. Es kann jedoch schwierig werden oder unklar sein, wie die Bestimmungen dieser Richtlinie[29] im Hinblick auf das Internet der Dinge und autonome vernetzte Systeme (z. B. Roboter) angewandt werden sollen. Die Gründe hierfür liegen in den Merkmalen dieser Systeme, beispielsweise in der komplizierten Wertschöpfungskette eines Produkts oder eines Dienstes, mit gegenseitigen Abhängigkeiten zwischen Lieferanten, Herstellern und anderen Dritten; in der Ungewissheiten über die Rechtsnatur von Geräten des Internets der Dinge, z. B. ob es sich bei ihnen um Produkte, um Dienste oder um zusammen mit einem Dienst verkaufte Produkte handelt; oder in der Autonomie dieser Technik.

Die Kommission hat eine umfassende Bewertung der Produkthaftungsrichtlinie eingeleitet, um festzustellen, wie sie insgesamt funktioniert und ob ihre Vorschriften, die für ein anderes Umfeld entwickelt worden waren, nach wie vor für die neu entstehenden Techniken, wie das Internet der Dinge und autonome vernetzte Systeme, geeignet sind.

4.2. Mögliche Ansätze für die Zukunft

Ziel der Kommission ist es, die Rechtssicherheit im Hinblick auf die Haftung im Zusammenhang mit neu entstehender Technik zu stärken und so ein innovationsfreundliches Umfeld zu schaffen. Abgesehen vom Status quo[30] sind verschiedene Ansätze denkbar.

- **Risikoabhängige Konzepte:** Nach diesen Konzepten könnten die Marktteilnehmer haftbar gemacht werden, die große Risiken für andere verursachen, oder die am besten in der Lage sind, das Eintreten dieser Risiken zu minimieren oder zu vermeiden.

- **Freiwillige oder verbindliche Versicherungssysteme:** Solche Systeme könnten mit den vorstehend genannten Haftungskonzepten gekoppelt werden. Sie würden dafür sorgen, dass die geschädigten Parteien entschädigt würden (z. B. der Verbraucher). Bei diesem Konzept müssten Unternehmen Rechtsschutz für die von ihnen getätigten Investitionen erhalten, während die Geschädigten sicher sein müssen, dass sie einen angemessenen Schadenersatz erhalten oder für den Schadensfall angemessen versichert sind.

---

28 Die EU-Haftungsregelungen beziehen sich nur auf die außervertragliche Haftung.

29 Verweise auf die verschuldensunabhängige Haftung von Herstellern im Falle von fehlerhaften Produkten finden sich in anderen Rechtsvorschriften zur Produktsicherheit, etwa in der Richtlinie über Funkanlagen (2014/53/EU), der Verordnung über Medizinprodukte, in der Maschinenrichtlinie (2006/42/EG) und in der Richtlinie über die allgemeine Produktsicherheit (2001/95/EG).

30 Die Kommission könnte einen Leitfaden zur Anwendung der EU-Haftungsvorschriften auf das Internet der Dinge und die Robotik herausgeben.

Bei jedem Konzept gilt es, die Handlungen der Individuen zu berücksichtigen, die die Technik nutzen, und insbesondere festzustellen, welche Rolle die Nutzer dieser Technik spielen sollen.

Die Kommission wird die Interessenträger zur Frage der Eignung der geltenden EU-Haftungsregelungen für das Internet der Dinge und automatisierte vernetzte Systeme sowie zu möglichen Konzepten konsultieren, mit denen die derzeitigen Probleme mit der Haftungsfrage gelöst werden können. Außerdem findet eine parallele öffentliche Konsultation zur Gesamtbewertung der Anwendung der Produkthaftungsrichtlinie statt. Die Kommission wird die Ergebnisse auswerten und Handlungsoptionen für künftige Maßnahmen ausloten.

5. DATENÜBERTRAGBARKEIT, INTEROPERABILITÄT UND NORMEN

Weitere mit der Datenwirtschaft neu auftretende Fragen betreffen die Übertragbarkeit nicht personenbezogener Daten, die Interoperabilität von Diensten für den Datenaustausch und geeignete technische Normen für die Umsetzung einer sinnvollen Übertragbarkeit.

5.1. Übertragbarkeit von nicht personenbezogenen Daten

Datenübertragbarkeit bedeutet, dass Verbraucher und Unternehmen ihre Daten leicht von einem System zu einem anderen übertragen können. Für den Wechsel fallen in der Datenwirtschaft in der Regel nur geringe Kosten an und damit sind die Zugangshürden auch niedrig. Mit der Datenschutz-Grundverordnung werden Privatpersonen das Recht haben, die dem Diensteanbieter zur Verfügung gestellten personenbezogenen Daten von diesem in einem strukturierten, weit verbreiteten maschinenlesbaren Format zu erhalten, um sie an einen anderen Anbieter weitergeben zu können[31].

Für nicht personenbezogene Daten besteht derzeit jedoch noch keine Pflicht, wenigstens ein Mindestniveau an Datenübertragbarkeit zu gewährleisten, auch nicht für weit verbreitete Online-Dienste wie die der Cloud-Hosting-Anbieter. Dies ist zum Teil darauf zurückzuführen, dass die Anforderungen an die Datenübertragbarkeit technisch anspruchsvoll und kostenaufwendig sein können, da Daten von verschiedenen Anbietern derselben Dienste möglicherweise auf unterschiedliche Art und Weise gespeichert werden.

Eine sinnvolle Übertragbarkeitsregelung für nicht personenbezogene Daten müsste auch weiter gefasste Überlegungen zur Datenverwaltung berücksichtigen, wie beispielsweise die Transparenz für Nutzer, die Verwaltung des Zugangs und die Interoperabilität, damit verschiedene Plattformen so verknüpft werden können, dass Innovationsanreize entstehen.

[31] Artikel 20.

5.2. Interoperabilität

Erwägungen der Datenübertragbarkeit sind häufig eng mit der Frage der Dateninteroperabilität verbunden, die es unterschiedlichsten digitalen Diensten durch entsprechende technische Spezifikationen ermöglicht, Daten nahtlos auszutauschen. In der Richtlinie über Informationen des öffentlichen Sektors und in den entsprechenden Leitfäden (wie dem europäischen Interoperabilitätsrahmen) wird die Bedeutung aussagekräftiger und standardisierter Metadaten betont, die nach einem bewährten Vokabular erstellt werden, das die Suche und die Interoperabilität erleichtert. Die Richtlinie über die Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) und ihre Interoperabilitätsverordnungen und Leitfäden für Geodatendienste und Geodaten, darunter auch Daten aus der Sensorüberwachung, findet derzeit auf Geodaten des öffentlichen Sektors Anwendung[32].

Bei Online-Plattformen erleichtert beispielsweise die Dateninteroperabilität nicht nur den Wechsel, sondern auch die gleichzeitige Nutzung mehrerer Plattformen (so genanntes „Multi-Homing“) sowie einen breiten Datenaustausch über verschiedene Plattformen hinweg, was die Innovation in der Digitalwirtschaft vorantreiben kann.

5.3. Normen

Strategien für die Übertragbarkeit sind nur wirksam, wenn sie durch geeignete technische Normen unterstützt werden, damit die Übertragbarkeit technisch neutral und sinnvoll umgesetzt werden kann. Die Kommission hat sich verpflichtet[33], geeignete Normen zu unterstützen, mit denen die Interoperabilität, die Übertragbarkeit und die Sicherheit von Cloud-Diensten verbessert werden können, indem die Arbeit von Open-Source-Gemeinschaften besser in den Normungsprozess auf europäischer Ebene integriert wird. Beispiele für dieses Konzept sind die TOSCA-Spezifikationen für Cloud-Anwendungen, mit denen die Übertragbarkeit und das Betriebsmanagement von Cloud-Anwendungen und -Diensten[34] verbessert werden sollen, sowie die technischen Spezifikationen und Leitlinien der INSPIRE-Durchführungsverordnungen[35].

5.4. Mögliche Ansätze für die Zukunft

Mögliche Ansätze für den künftigen Umgang mit den vorstehenden Fragen beinhalten Folgendes:

- **Ausarbeitung von Empfehlungen für Vertragsklauseln, um den Anbieterwechsel zu vereinfachen:** Da sich die Übertragbarkeit von Daten und der Wechsel des Datendiensteanbieters gegenseitig bedingen, könnte die Ausarbeitung von Standardvertragsklauseln geprüft werden, die den Diensteanbieter verpflichten, für die Übertragbarkeit von Kundendaten zu sorgen.

[32] Von Maschinen erzeugte Daten sind „Geodaten“, da Sensoren in der Regel auch ihre unmittelbare Position oder ihre Standortdaten zusammen mit dem Messwert angeben.

[33] COM(2016) 176 final: IKT-Normungsschwerpunkte für den digitalen Binnenmarkt.

[34] https://www.oasis-open.org/committees/tosca

[35] INSPIRE-Vorschriften: http://inspire.ec.europa.eu/inspire-legislation/26

- **Weiterentwicklung der Rechte auf Datenübertragbarkeit:** Ausgehend von dem in der DS-GVO festgelegten Recht auf Datenübertragbarkeit und den vorgeschlagenen Vertragsklauseln für die Bereitstellung digitaler Inhalte, könnte ein weitergehendes Recht auf Übertragbarkeit nicht personenbezogener Daten insbesondere im Geschäftsverkehr zwischen Unternehmen eingeführt werden, wobei dem Ergebnis der laufenden Beurteilung zentraler Teile des EU-Marketing- und Verbraucherrechts gebührend Rechnung zu tragen wäre[36].

- **Sektorspezifische Erprobung von Normen:** Für die Entwicklung eines tragfähigen Konzepts für normierte Übertragbarkeitsvorschriften könnten sektorspezifische experimentelle Ansätze verfolgt werden. Hier wäre es naheliegend, verschiedene Interessenträger wie beispielsweise Normungsorganisationen, die Industrie, Techniker und Behörden einzubeziehen.

Die Kommission wird eine Konsultation zu diesen Fragen unter den Interessenträgern durchführen und abhängig davon festlegen, ob weitere Maßnahmen, möglichst in der vorstehend genannten Form entweder einzeln oder in Kombination ergriffen werden müssen.

6. ERPROBUNGEN UND TESTS

Praktische Erprobungen spielen in der Datenwirtschaft eine wichtige Rolle, wenn es darum geht, neu auftretende Probleme zu untersuchen. Dabei wird geprüft, inwieweit derartige Testläufe und Experimente über das Programm Horizont 2020 gefördert werden können.

Bevor Schlussfolgerungen über die Eignung möglicher Lösungen für den Datenzugang und die Haftung gezogen werden können, sollten gemeinsam mit den Interessenträgern zu diesen Fragen Testläufe in einem realen Umfeld durchgeführt werden. Benötigt wird eine europäische Lösung, die sich auf die Zusammenarbeit der Mitgliedstaaten und die Durchführung gemeinsamer Erprobungen stützt.

Für solche Testläufe käme angesichts der grenzüberschreitenden Dimension dieses Sektors die kooperative, vernetzte und automatisierte Mobilität[37] in Frage.

In mehreren Mitgliedstaaten laufen bereits Projekte zur Entwicklung kooperativer Systeme und zur Automatisierung auf einem höheren Niveau[38]. Im Rahmen dieser Projekte werden Fahrzeuge miteinander und mit der straßenseitigen Infrastruktur, wie Ampeln und Verkehrszeichen, vernetzt. Zudem will die Kommission mit einer Gruppe interessierter Mitgliedstaaten zusammenarbeiten, um einen Rechtsrahmen zu schaffen, mit dem Erprobungen auf der Grundlage einheitlicher Vorschriften über den Datenzugang und die Haftung durchgeführt werden können. Um den Zugang zu einem ausreichend großen Datenvolumen zu ermöglichen, sollten sich die Versuche auf 5G-

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

[37] Siehe COM(2016) 766 vom 30.11.2016.

[38] Siehe COM(2016) 766. Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme.

Technik stützen sowie in nahtloser Koexistenz mit bereits vorhandenen Technologien und nach dem Grundsatz der Komplementarität[39] durchgeführt werden.

Ein weiteres interessantes Experiment liefert der Geodatensektor – ein Datenökosystem, das derzeit im Umfeld des Erdbeobachtungsprogramms und weltweit drittgrößten Datenlieferanten Copernicus entsteht. Die Kommission ist derzeit mit der Ausarbeitung innovativer Lösungen befasst, wobei sie sich vor allem mit dem Datenzugang, der Interoperabilität und der Vorhersehbarkeit beschäftigt, um so die Entwicklung von auf Raumdaten basierenden Anwendungen zu unterstützen.

7. SCHLUSSFOLGERUNG

Für den Aufbau einer Datenwirtschaft benötigt die EU einen politischen Rahmen, damit Daten über die gesamte Wertschöpfungskette hinweg für wissenschaftliche, gesellschaftliche und industrielle Prozessen genutzt werden können. Aus diesem Grund wird die Kommission zu den in dieser Mitteilung behandelten Fragen einen umfassenden Dialog mit den Interessenträgern führen. Eingeleitet wird dieser Dialog mit einer öffentlichen Konsultation. Die Fragen des Datenzugangs und der Haftung werden auch in einem realen Umfeld der kooperativen, vernetzten und automatisierten Mobilität geprüft.

Hinsichtlich des freien Datenverkehrs wird sich die Kommission auch in Zukunft entsprechend dem vorstehend erläuterten Konzept mit dieser Frage befassen, damit der Grundsatz des freien Datenverkehrs in der EU, gegebenenfalls auch durch vorrangige Durchsetzungsmaßnahmen, vollständig zum Tragen kommt. Ferner wird die Kommission weiterhin den freien Datenverkehr beobachten, Fakten sammeln und, falls notwendig, weitere Initiativen in Erwägung ziehen.

Abhängig von den Ergebnissen des Dialogs mit den Interessenträgern wird die Kommission auch entscheiden, ob weitere Maßnahmen zu neu entstehenden Fragen notwendig sind und entsprechende Lösungen vorschlagen. In diesem Zusammenhang wird die Erprobung unter realen Bedingungen möglicherweise eine Rolle spielen.

[39] Siehe COM(2016) 588. 5G für Europa: ein Aktionsplan.