BDI
Bundesverband der
Deutschen Industrie e.V.

BDI-Positionspapier Datenwirtschaft

Weniger ist mehr – über die Notwendigkeit einer neuen Datenregulierung

- Die Europäische Kommission hat mit ihrer Mitteilung zum „Aufbau einer europäischen Datenwirtschaft“ zur richtigen Zeit eine Diskussion darüber angestoßen, ob Verbesserungen am Rechtsrahmen zur Förderung einer europäischen Digitalwirtschaft und zur besseren Nutzbarmachung von Daten zum Wohle von Wirtschaft und Gesellschaft erforderlich ist.

- Der freie Fluss von Daten in der EU ist eine wichtige Voraussetzung für den Erfolg digitaler Geschäftsmodelle in Europa. Dank harmonisierter Datenschutzvorschriften ist dies zu weiten Teilen schon europäische Realität. Bestehende Datenlokalisierungsvorschriften in den Mitgliedstaaten, die den freien Fluss behindern, sind von der Europäischen Kommission umfassend auf ihre Notwendigkeit hin zu überprüfen.

- Neue gesetzliche Regelungen zu „Eigentum“ und Zugang zu (nicht-personenbezogenen) Daten sind bislang nicht erforderlich. In den meisten Fällen reichen individualvertragliche Regelungen aus, um flexible Datennutzungen zwischen den Beteiligten zu ermöglichen. Sinnvoll könnten darüber hinaus branchenspezifische Lösungen i.S.v Selbstverpflichtungen sein. Die Beschaffenheit des Zuganges zu nicht-personenbezogenen Daten muss daher umfassend in branchenspezifischen Workshops diskutiert werden.

- Das bestehende Haftungsregime ist auch in Zukunft geeignet, einen fairen Interessenausgleich zwischen Anwendern und Produzenten zu schaffen. Angesichts der zunehmend digitalen Beschaffenheit von Produkten gilt es, eine offene Diskussion über die Funktionsfähigkeit des bestehenden Haftungsregimes zu führen.

- Portabilität von Daten und Interoperabilität der Datenverarbeitungssysteme sind wichtige Voraussetzungen für die europäische Datenwirtschaft. Zur Erleichterung der Datennutzung bzw. zur Verbesserung ihrer Auffindbarkeit und Interoperabilität müssen branchenübergreifende Kriterien und Standards von der Industrie entwickelt werden. Verstärkte Förderung von entsprechenden Forschungsprojekten durch die EU ist zudem zu begrüßen.

Jan Christian Sahl | Abteilung Digitalisierung, Innovation und Gesundheitswirtschaft | T: +49 30 20281419 | j.sahl@bdi.eu | www.bdi.eu | Berlin, den 8. Juni 2017

Inhaltsverzeichnis

A. “free flow of data“ innerhalb der EU sicherstellen

Damit sich eine datenbasierte Wirtschaft in der EU voll entwickeln kann, ist es wichtig, dass Daten innerhalb der EU frei fließen können und nicht an Ländergrenzen Halt machen müssen. Dem können mitgliedstaatliche Gesetze, die eine Datenspeicherung (ausschließlich) im Inland vorschreiben, im Wege stehen. In Europa und auch weltweit sind in den vergangenen Jahren vermehrt neue Datenlokalisierungsvorschriften erlassen worden. Auch in Deutschland existieren einige gesetzliche Vorschriften, die eine Datenspeicherung im Inland vorschreiben. Bspw. verpflichtet etwa § 113b Abs. 1 TKG die Erbringer von Telekommunikationsdienstleistungen, bestimmte Verbindungsdaten ihrer Kunden im Inland zu speichern. Ein weiteres Beispiel findet sich etwa in § 146 Abs. 2 AO, wonach Unterlagen für die Buchführung in Deutschland aufzubewahren sind (Ausnahmen hierzu für die elektronische Buchführung finden sich allerdings in § 146 Abs. 2a AO). Insgesamt ist festzustellen, dass „free flow of data“ in der EU – vor allem aufgrund des harmonisierten Datenschutzrechts – schon weitgehend besteht. Zudem ist die Menge der in Deutschland von Datenlokalisierung betroffenen Daten eher gering und Lokalisierungsgesetze stellen die Unternehmen der deutschen Industrie bislang nicht vor größere Schwierigkeiten im Rahmen ihrer Digitalisierungsstrategien.

Aus Sicht des BDI ist es dennoch richtig, einen „free flow of data“ innerhalb der EU sicherzustellen und bestehende nationale Datenlokalisierungsvorschriften auf ihre Rechtfertigung im Einzelfall – jetzt und in Zukunft – hin zu überprüfen und gegebenenfalls abzuschaffen. Hierfür könnte die Pflicht zur Durchführung eines Notifizierungsverfahren vor der EU Kommission sinnvoll sein, falls Mitgliedsstaaten neue Lokalisierungsmaßnahmen einführen wollen. Weitergehende Instrumente bzw. die Einführung weiterer Grundfreiheiten erscheinen nicht erforderlich. Bereits heute müssen nationale Datenlokalisierungsvorschriften im Einklang mit geltendem EU-Recht sein. Insbesondere müssen sich diese an den europäischen Grundfreiheiten der Dienstleistungs- bzw. der Niederlassungsfreiheit messen lassen. Da Datenlokalisierungsvorschriften regelmäßig einen Eingriff in diese Grundfreiheiten bedeuten, müssen sie im Einzelfall gerechtfertigt, insbesondere verhältnismäßig sein. Die Europäische Kommission hat hierfür die Möglichkeit, die Mitgliedstaaten im Rahmen von Vertragsverletzungsverfahren auf nach ihrer Sicht ungerechtfertigte Datenlokalisierungsvorschriften hinzuweisen und diese – sollte ein Mitgliedstaat an den Vorschriften festhalten wollen – gegebenenfalls vom Europäischen Gerichtshof überprüfen und aufheben zu lassen. Grundsätzlich gilt auch hier: Notwendige Datenlokalisierungsvorschriften sollten europaweit harmonisiert und auf eine Mindestmaß reduziert werden. Dies würde einen Flickenteppich an unterschiedlichen Vorschriften wirksam verhindern und einen wichtigen Schritt auf dem Weg zum digitalen Binnenmarkt bedeuten.

Zudem ist zu beachten, dass der legitime Wunsch von Unternehmen, selbst einen Speicher- bzw. Verarbeitungsort für ihre Daten zu bestimmen, unangetastet bleiben muss. Untersuchungen belegen, dass es für deutsche Unternehmen bei der Auswahl von Cloud-Diensten zu den wichtigsten Kriterien gehört, dass die Unternehmensdaten ausschließlich auf Rechenzentren in Deutschland gespeichert werden (vgl. etwa Cloud-Monitor 2016 von Bitkom/KPMG). Es ist kommunikativ darauf zu achten, dass in den Unternehmen nicht der Eindruck entsteht, dass ein solches Kriterium in Zukunft ungültig würde. Dies könnte ansonsten dazu führen, dass deutsche Unternehmen zurückhaltender beim Einsatz von Cloud-Lösungen im Speziellen und der digitalen Transformation im Allgemeinen werden.

B. Vorerst keine Regeln für den „Eigentum“ und Zugang zu Daten erforderlich

In der Industrie 4.0 sind Daten ein Motor für Wirtschaftswachstum. Eine Vielzahl an Akteuren hat ein Interesse, Daten von und über Maschinen und Gegenständen (nicht-personenbezogene Daten) zu nutzen. Dies hat zu einer verstärkten Diskussion über die Rechte an diesen Daten geführt. Maschinendaten enthalten in der Regel keine Informationen über Menschen, sondern lediglich über Maschinen, die Umwelt oder industrielle Prozessabläufe. Sie bergen ein großes Potenzial für neue Geschäftsmodelle, insbesondere im B2B-Bereich. Es ist von dem Grundsatz auszugehen, dass die europäische Datenwirtschaft ihr volkswirtschaftliches Potenzial optimal entfalten kann, wenn möglichst viele der vorhandenen Daten durch möglichst viele Interessierte genutzt werden können. Voraussetzung dafür ist ein fairer Wettbewerb zwischen allen Marktakteuren zur Förderung von innovativen Geschäftsmodellen, in dem auch mittelständische Unternehmen und Start-ups Chancen haben. Die Diskussion über „Eigentum“ und Zugang zu diesen Daten wird vor allem deshalb geführt, weil es wenig einschlägige Rechtsvorschriften zu dieser Datenkategorie gibt. Anders als personenbezogene Daten unterliegen nicht-personenbezogene Daten nicht dem Datenschutzrecht. Auch andere Rechtsvorschriften (etwa des Urheberrechts, des Rechts der Geschäftsgeheimnisse, des allgemeinen Zivilrechts) sind nicht bzw. nur bedingt einschlägig. Rechte an diesen Daten sind nur rudimentär geregelt. Insbesondere existieren keine gesetzlichen Vorschriften, die eine vermögenswerte Zuordnung („Eigentum“) dieser Daten oder Zugangsrechte zu diesen definieren würden.

Der BDI sieht vorerst keine Notwendigkeit für eine horizontale Regelung der Zugangsfragen von nicht-personenbezogenen Daten. Es sollte grundsätzlich zuerst überprüft werden, ob der faire und diskriminierungsfreie Zugang zu Daten in einzelnen Branchen für Dritte ermöglicht wird und die Datennutzung durch Verträge zufriedenstellend gelöst werden kann. Bislang kann kein Marktversagen beobachtet werden, somit besteht auch keine Notwendigkeit für regulierende Eingriffe. Für ein solches Marktversagen müsste klar erkennbar sein, dass nicht-personenbezogene Daten von den Beteiligten nicht in ausreichendem Maße genutzt oder miteinander geteilt würden und dadurch wertvolles volkswirtschaftliches Potenzial der Datenökonomie verloren geht. Zu begrüßen ist außerdem, wenn sich einzelne Branchen im Sinne eines „Code of Conduct“ auf allgemeine, klare Datennutzungsregeln innerhalb ihres jeweiligen digitalen Ökosystems einigen. In Deutschland hat etwa die Automobilindustrie erste vielversprechende Vorschläge vorgelegt. Über diese Lösungen hinaus, sollte branchenspezifisch die Entwicklung digitaler Datenmärkte genau beobachtet und analysiert werden. Sollte dabei strukturelles Marktversagen in einzelnen Segmenten beobachtet werden können, müssten maßgeschneiderte legislative Lösungen entwickelt werden. Darüber hinaus sollte die EU Kommission entschieden und frühzeitig gegen sich entwickelnde Datenmonopole mithilfe des europäischen Kartell- und Wettbewerbsrecht vorgehen.

Der BDI sieht keine Notwendigkeit, (Eigentums-) Rechte an diesen Daten durch neue Rechtsvorschriften zu etablieren. Stattdessen empfiehlt es sich, die Frage der Datennutzung mit den beteiligten Unternehmen und Branchen anhand von Use-Cases offen zu diskutieren und der vertraglichen Ausgestaltung zu überlassen. Bereits in einem ersten Schritt ist unklar, wem ein „Eigentumsrecht“ an nicht-personenbezogenen Daten zukommen soll. In komplexen, datenbasierten Wertschöpfungsnetzwerken kommt eine Vielzahl von Akteuren für ein solches Zuordnungsrecht in Frage. Außerdem zeichnet sich gerade die digitale, datenbasierte Wirtschaft durch einen dynamischen Wandel aus. Eine starre, auf Jahre im Voraus festgelegte "*one size fits* all"-Regulierung läuft Gefahr, mit der Vielfalt und Unterschiedlichkeit innovativer digitaler Geschäftsmodelle zu kollidieren und diese gar unmöglich zu machen.

C. Derzeitiges Haftungsregime bis auf weiteres ausreichend

Das geltende Haftungsregime ist in seiner derzeitigen Fassung geeignet, einen fairen Interessenausgleich zwischen Anwender und Produzenten zu schaffen. Das aktuelle Haftungsregime kann auf innovative Produkte angewendet werden und ermöglicht auch hier grundsätzlich eine angemessene Lösung der Haftungsfragen. Durch die zunehmende Vernetzung von physischen Geräten wird jedoch der bestehende Rechtsrahmen herausgefordert, bspw. im Internet-of-Things (IoT) oder bei vollkommen automatisierten Fahrzeugen oder Anlagen. Angesichts der zunehmend digitalen Beschaffenheit von Produkten hat sich eine lebhafte Diskussion über die Funktionsfähigkeit und mögliche Anpassungsbedürftigkeit des bestehenden Haftungsregimes entwickelt.

Solange bestimmte Handlungen auf Personen zurückgeführt werden und Produktfehler einem bestimmten menschlichen Fehlverhalten zugeordnet werden können, kann die Abgrenzung von Risikosphären in Anwendung des derzeitigen Rechts der Rechtsprechung überlassen werden. Die Europäische Kommission schlägt in Ihrer Mitteilung „Building a EU Data Economy“ zwei konkrete Herangehensweisen vor, die sich gegenseitig unterstützen sollen. Dabei wird zwischen einem Risk-Generating Approach (ähnlich Gefährdungshaftung) und einem Risk-Management Approach unterschieden. Grundsätzlich gilt es, eine angemessene Risikoverteilung zu finden, die innovationsfreundlich und fair gegenüber allen Marktteilnehmern ist. Aufgrund der enormen Dynamik im IoT-Markt sollte jedoch von einer verpflichtenden Versicherung abgesehen werden.

Vorsicht ist außerdem dabei geboten, Produkt-Haftungsansprüche gegenüber Unternehmen aufgrund der Verfügbarkeit von Rohdaten zu begründen – auch wenn aus diesen Daten das Schadensereignis hätten vorausgesehen können. Es wird zukünftig häufiger der Fall sein, dass vernetzte Produkte ihre Betriebs- und Zustandsdaten regelmäßig auch an den Hersteller des Produkts senden. Die Hersteller dürfen dabei nicht in die Pflicht genommen werden, Datensätze vorausschauend hinsichtlich möglicher Fehler bzw. Schadensursachen zu Produkten auszuwerten. Aus Sorge vor möglichen Haftungsansprüchen würden Produkthersteller diese Daten überhaupt nicht auswerten, sich diese nicht verschaffen oder ihre Produkte nicht mit datengenerierenden Sensoren ausstatten. Dies hätte vielfältige Nachteile für die Entwicklung einer europäischen Datenökonomie zur Folge.

Aufgrund der enormen Komplexität können einzelne Unternehmen ab einer gewissen Interaktion und Interdependenz von software-gesteuerten Geräten nur bedingt Gewährleistung für das Funktionieren des Gesamtsystems übernehmen. Gerade für sicherheitskritische Anwendungen ist es jedoch entscheidend, das gesamte Ökosystem im Blick zu haben. Die Manipulationen von IoT-Produkten durch Cyberangriffe stellt das heutige Haftungsregime vor neue Herausforderungen. Wer haftet, wenn in Zukunft bspw. eine automatisierte Ampel oder eine elektronische Insulinpumpe von außen gehackt wird und schwere Unfälle bzw. Gesundheitsschäden verursacht? Hier können gemeinsam definierte und auf Risikoanalysen basierende Cybersicherheits-Richtlinien einen Beitrag leisten. Freiwillige Sicherheitskennzeichnungen können dabei zudem eine Wirksamkeitsvermutung ermöglichen. Dabei gilt es zu prüfen, in wie weit das Schließen von Sicherheitslücken Einfluss auf die Gewährleistung des Produktes hat. Aufgrund des sich ständig verändernden Zustandes von Software (durch Updates o.ä.) ist zudem eine statische Produktdefinition nicht zielführend.

Voraussetzung einer zielführenden Diskussion für ein zukünftiges Haftungsregime ist eine eindeutige und adäquate Abgrenzung inhaltlicher Konzepte. Bspw. können IoT-Geräte im Endkundenmarkt nicht mit Robotik in Industrieanlagen (B2C vs. B2B) verglichen werden; zudem muss zwischen vernetzten und vollautomatisierten Anlagen oder Fahrzeugen unterschieden werden. Die deutsche Industrie empfiehlt daher eine Abgrenzung aufgrund funktionaler Kriterien, die in einem gemeinsamen Arbeitsprozess zwischen EU-Kommission und der Wirtschaft gefunden werden müssen.

D. Portabilität, Interoperabilität und Standards

Portabilität, Interoperabilität und entsprechende Standards sind wichtige Faktoren für das Gelingen einer datenbasierten Wirtschaft. Wenn Daten nicht von einem Akteur auf den nächsten übertragen (Datenportabilität) bzw. dort aus technischen Gründen nicht verarbeitet werden können, kann dies das ökonomische und gesellschaftliche Datenpotenzial empfindlich beeinträchtigen. Ein hohes Maß an Datenportabilität verhindert darüber hinaus Lock-In-Effekte und stimuliert den Wettbewerb zwischen digitalen Diensten. Für den Bereich der personenbezogenen Daten enthält Art. 20 der Datenschutz-Grundverordnung bereits Vorschriften zugunsten der Verbraucher – diese haben ein ausdrückliches Recht auf Mitnahme bzw. direkter Übergabe ihrer personenbezogenen Daten von einem Anbieter auf einen anderen. Für Business-to-Business-Verhältnisse empfiehlt sich eine solche Regulierung bislang nicht. Es ist aus Sicht des BDI nicht erkennbar, dass im Bereich der nicht-personenbezogenen Daten marktversagensähnliche Probleme bestehen, die ein gesetzgeberisches Handeln rechtfertigen würden. So ist etwa für Unternehmenskunden ein Wechsel des Cloud-Anbieters bzw. die Mitnahme der dort gespeicherten Daten problemlos möglich und auch häufig Gegenstand der Cloud-Nutzung zugrundeliegenden Verträge.

Zur Erleichterung Datennutzung bzw. zur Verbesserung ihrer technischen und semantischen Auffindbarkeit und Interoperabilität müssen industrieübergreifende gemeinsame Metadaten-Schemata sowie die Verwendung kontrollierter (mehrsprachiger) Vokabulare entwickelt werden. Dabei können genormte Schnittstellen einen nahtlosen Austausch von Informationen begünstigen. Diese Aufgabe muss die Industrie mit bekannten Forschungsinstitutionen übernehmen. Sinnvoll ist ebenfalls die Förderung entsprechender Forschungsprojekte durch die EU. Auch bei der Priorisierung dieser Normungsaufgaben können europäische Institutionen unterstützen.