DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zu der Öffentlichen Konsultation der Europäischen Kommission zum Datengesetz und geänderten Vorschriften über den rechtlichen Schutz von Datenbanken

Stellungnahme Nr.: 50/2021 Berlin/Brüssel, im September 2021

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg (Berichterstatter)
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski

Ansprechpartnerin in Brüssel:

- Hannah Adzakpa, LL.M.

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Europa

Europäische Kommission
- Generaldirektion für Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament
- Ausschuss für Industrie, Forschung und Energie (ITRE)

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Bundesverband der Freien Berufe
Agence Europe

Deutschland

Bundesministerium des Innern, für Bau und Heimat
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Redaktion NJW
Juve-Verlag
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt

Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 62.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 252 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

A. Vorbemerkung

Die öffentliche Konsultation zum Datengesetz umfasst verschiedene Problembereiche, deren Zusammenhang teilweise nur schwer erkennbar ist. Einziger gemeinsamer Ansatzpunkt ist, dass sämtliche Problemkreise etwas mit der Datenwirtschaft zu tun haben. Demgemäß wird die Stellungnahme auf die einzelnen Problemkreise aufgeteilt. Es ist zu empfehlen, dass eine spätere Regulierung – soweit sie denn zielführend erscheint – nicht alle Problemkreise in einem einheitlichen Gesetzgebungsakt umfasst.

B. Zu den Problemkreisen

I. Austausch von Daten zwischen Unternehmen und Behörden im öffentlichen Interesse

Es gibt sicher eine ganze Reihe von Anwendungsfeldern, in denen Behörden ein Interesse an der Nutzung privater Datensammlungen haben und in denen sie ihr Handeln durch die Nutzung solcher privater Datensammlungen verbessern können. Umgekehrt verfolgen die Unternehmen, die solche Datensammlungen erstellen, damit grundrechtlich geschützte eigene Interessen. Darüber hinaus sind sie oft gesetzlich und/oder vertraglich verpflichtet, auch die Interessen Dritter, z.B. zum Schutz personenbezogener Daten, von Geschäftsgeheimnissen oder geistigem Eigentum zu wahren. Oft gebieten solche Interessen, solche Datensammlungen nicht mit Dritten, auch nicht mit Behörden zu teilen. Meist stehen hinter solchen Datensammlungen auch Investitionen, die es zumindest nahelegen, dass die Behörden für ihnen übermittelte Daten einen angemessenen Preis zahlen.

Auch ohne gesetzliche Regelungen steht es Behörden und Unternehmen frei, solche Daten zu teilen, wenn sie über den Umfang und die Bedingungen eines solchen Teilens

eine Einigung erzielen können, und es keine gesetzlichen oder vertraglichen Regelungen, etwa wegen Datenschutz- oder Geheimnisschutzinteressen Dritter gibt, die ein solches Teilen verbieten. Gesetzlicher Regeln bedarf es hier allenfalls dann, wenn bisher bestehende gesetzliche Hindernisse beseitigt werden sollen.

Anders ist dies dann, wenn das öffentliche Interesse an der Datennutzung so stark ist, dass einzelnen Unternehmen die Pflicht auferlegt wird, Datensammlungen mit Behörden zu teilen. Dies ist z.B. denkbar bei Emissionsdaten, um Luftverschmutzung und Klimaveränderung zu vermeiden. Es kann auch bei medizinischen Daten der Fall sein. Zu welchem Zweck dies der Fall ist und welche Daten betroffen sein können, muss aber im Einzelfall ermittelt werden. Nur an Hand des Nutzungszwecks und des Umfangs der betroffenen Daten kann überprüft werden, ob der mit einem solchen Zwang verbundene Eingriff in die Rechte des betroffenen Unternehmens sowie evtl. betroffener Dritter verhältnismäßig ist. Dies verlangt Regelungen im Einzelfall. Solche Regelungen sollten Normen vorbehalten bleiben, die das sachliche Problem regeln. Eine generelle Regelung in einem Datengesetz kann die notwendige Abwägung nicht treffen, weil sie weder Zweck noch Umfang des Eingriffs kennt.

II. Austausch von Daten zwischen Unternehmen

In diesem Bereich geht es vor allem um faire Bedingungen, zu denen insbesondere KMU Zugang zu Datensammlungen großer Unternehmen erhalten sollen.

Notwendigerweise muss damit ein Recht solcher KMU verbunden sein, den Zugang zu diesen Bedingungen auch zu erhalten, wenn dem keine geschützten Interessen Dritter z.B. am Schutz personenbezogener Daten, von Geschäftsgeheimnissen oder geistigem Eigentum entgegenstehen. Zur Vermeidung von Monopolen und Oligopolen, die allein durch die Herrschaft über große Datensammlungen entstehen oder perpetuiert werden, sind solche Regelungen sinnvoll. Es muss aber klar sein, dass es dabei primär um konkrete Ausprägungen kartellrechtlicher Grundüberlegungen geht. Dennoch ist eine Inhaltskontrolle aller Vertragsbedingungen sinnvoll, um der Entstehung von Monopolen schon entgegenzuwirken, bevor eine kartellrechtlich relevante Monopolsituation entstanden ist, die nachträglich nur schwer zu ändern ist. Sichergestellt werden muss außerdem, dass die betroffenen Unternehmen sich einer solchen Kontrolle nicht durch die Flucht in andere Rechtsordnungen entziehen können. Außerdem muss dafür

gesorgt werden, dass es nicht zu Doppelregelungen und Widersprüchen zwischen dem schon im Gesetzgebungsverfahren befindlichen Digital Markets Act (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) COM/2020/842 final) und den jetzt geplanten weiteren Regulierungen kommt.

III. Smart Contracts

Es besteht bei allen Unklarheiten im Detail unter Juristen im Wesentlichen Einigkeit, dass es sich bei Smart Contracts nicht um Verträge im Rechtssinne handelt, sondern um Programmcodes, die bei Eintritt eines bestimmten (vorprogrammierten) Ereignisses (z.B. bei einer Objektbewegung oder beim Erreichen einer bestimmten Messgröße für eine Temperatur, einen Füllstand etc.) ein anderes vorprogrammiertes Ereignis (z.B. eine Bestellung, Zahlung oder eine Übereignung) in Gang setzen sollen. Es handelt sich also um die automatisierte Abwicklung eines Rechtsgeschäfts (nicht notwendig eines Vertrags), welches als existent oder zeitgleich abgeschlossen vorausgesetzt wird. Soweit ersichtlich gilt dies auch für die anderen Zivilrechtsordnungen der Mitgliedstaaten der Europäischen Union.

Vertraglichen Charakter hat (außer dem zu vollziehenden Vertrag selbst) allein die Vereinbarung über den Einsatz und das Design der Software, die für die gewünschte Automatisierung sorgt. Dabei ist es eine Frage des jeweils anwendbaren Vertragsrechts, ob und wie die gewünschte Rechtsfolge tatsächlich automatisiert herbeigeführt werden kann (etwa über die Fiktion einer Erklärung oder die Figur der aufschiebenden Bedingung im deutschen Recht, §158 Abs. 1 BGB). Das gleiche gilt für die etwaige Anpassung oder Rückgängigmachung des Vollzugs (vgl. BGHZ 217, 33 für den elektronischen Bezahldienst PayPal).

Rechtlichen Regelungsbedarf im hier betrachteten Zusammenhang sehen wir nicht.

IV. Klärung der Rechte an nicht personenbezogenen Daten

Die Frage der rechtlichen Zuordnung von Daten bzw. großen Datensammlungen zu einzelnen Unternehmen/juristischen Personen wird seit langem diskutiert. Es konnte dabei für viele Fälle nicht geklärt werden, wem evtl. ausschließliche Rechte an solchen Daten zustehen, z.B. dem Nutzer oder dem Hersteller von Maschinen. Es fragt sich

überhaupt, ob die Zuordnung ausschließlicher Rechte an Einzelne der komplexen Interessensituation entspricht.

Für die im Fragebogen im Detail angesprochenen Ansprüche auf Zugang zu solchen Daten oder Nutzung solcher Daten für Dienstleistungen ist zunächst darauf hinzuweisen, dass sich diese Fragestellungen mit den unter II. erörterteten Problemen überschneiden. Auch hier geht es um den Zugang zu Datensammlungen Dritter. Es gibt aber bei den Daten im Internet of Things noch einige besondere Fragestellungen. Möglicherweise benötigen Unternehmen solche Daten, um den Nutzern des Internet of Things gegenüber Dienstleistungen zu erbringen, die ohne Kenntnis dieser Daten nicht erbracht werden können. Um Wettbewerb zu ermöglichen, müssen solche Daten für alle interessierten Unternehmen zugänglich sein – mit einer Grenze dort, wo die Zugänglichkeit der Daten Gefahren für die Produktsicherheit bedeuten oder die legitime Geheimhaltung von Geschäftsgeheimnissen gefährden. In diesen und anderen konkreten Situationen müssen zum Schutze des Wettbewerbs Zugangsrechte geschaffen werden.

Im Übrigen stellt sich die Frage in gleicher Weise auch bei personenbezogenen Daten – dort kommen nur die Rechte der Betroffenen als weitere Grenze einer Herausgabepflicht hinzu. Schließlich sind auch datenschutzrechtliche Rechtspositionen keine ausschließlichen Rechte an Daten.

Im Übrigen lassen sich gerade bei den im Internet-of-Things anfallenden Daten personenbezogene Daten und nicht personenbezogene Daten in der Praxis nicht rechtssicher unterscheiden. Insbesondere dürfte es schwer möglich sein, sicherzustellen, dass es in einer größeren Datenmenge keine personenbezogenen Daten gibt. Es wird dringend empfohlen, gerade hier keine gesonderte Regelung für nicht personenbezogene Daten zu treffen. Es besteht die Gefahr, dass die Regelung in der Praxis kaum genutzt wird, weil vorsichtshalber immer davon ausgegangen wird, dass es bei einem Begehren auf Datenzugang auch um den Zugang zu personenbezogenen Daten Dritter geht und schon deshalb kein Datenzugang gewährt bzw. keine Datennutzung ermöglicht werden kann.

V. Verbesserung der Übertragbarkeit von Cloud-Diensten für gewerbliche Nutzer

Es besteht ein massives Interesse von Nutzern daran, den Anbieter von in der Cloud genutzten Diensten wechseln zu können. Im Bereich des Outsourcing gibt es für vergleichbare Probleme schon seit Jahren vertragliche Regelungen, nach denen ein solcher Wechsel zu einem neuen Dienstleister vom bisherigen Dienstleister unterstützt werden muss. Im Bereich von Cloud-Lösungen scheinen sich solche Lösungen noch nicht durchgesetzt zu haben, vor allem, weil die Vertragsbedingungen hier meist von den Diensteanbietern gestellt werden und die Kunden nicht über die Verhandlungsmacht verfügen, eigene Bedingungen durchzusetzen. Meist wird nur vorgesehen, dass der Kunde seine Daten in einem gängigen Format abrufen kann oder sie ihm in einem gängigen Format in anderer Weise übermittelt werden. Dies reicht aber bei weitem nicht aus, um einen Wechsel zu anderen Anbietern möglich zu machen, weil z.B. die Übertragung von Arbeitsergebnissen der Cloud-Dienstleistungen dadurch nicht gesichert ist. Dies führt zu der wettbewerblich unerwünschten, technisch bedingten Situation, dass Kunden Anbieter nur sehr schwer wechseln können.
Sollte diese Situation bestehen bleiben, ist eine gesetzliche Lösung notwendig. Lösungen über Branchenempfehlungen haben sich bei vergleichbaren Situationen bislang in der Praxis nicht bewährt, weil sich nicht alle relevanten Marktteilnehmer daran gehalten haben. Eine solche Regulierung sollte allerdings auch Privatnutzer von Cloud-Diensten betreffen, weil sie sich in der gleichen Situation wie kleinere Unternehmen befinden. Sicher wäre dabei sinnvoll, in die gesetzliche Regelung nicht nur Grundsätze aufzunehmen, sondern konkrete Regelungen zum Umfang der Verpflichtung zu treffen. Dies kann allerdings nur in einem Umfang geschehen, der letztendlich technologieneutral ist, weil die Konkretisierung sonst den Anwendungsbereich der Norm zu sehr beschränkt.

VI. Ergänzung des Rechts auf Übertragbarkeit gemäß Art. 20 DSGVO

Hier geht es der Kommission um die Frage, ob personenbezogene Daten, die im Rahmen der Nutzung des Internet of Things erhoben und gespeichert werden, jederzeit an die Betroffenen übertragen werden können. Dabei geht es nicht darum, dass Betroffene die Daten jederzeit einsehen können, also um eine Konkretisierung des Auskunftsrechts nach Art. 15 DSGVO, das ja auch einen umfassenden Anspruch auf Überlassung von Kopien beinhaltet, sondern um eine Übertragung der Daten in

Erweiterung des Art. 20 DSGVO. Die meisten dieser Daten werden ja zur Durchführung und Abrechnung im Rahmen des IoT geleisteter Dienste erhoben und gespeichert – andernfalls wäre ihre Erhebung und Speicherung datenschutzrechtlich gar nicht zulässig. Solange die Daten für diese Dienste noch benötigt werden, können sie nicht an den Betroffenen übertragen werden. Erst bei Beendigung der Leistungsbeziehung sollten und könnten Sie an den Betroffenen bzw. den Vertragspartner herausgegeben werden. Insoweit müssten vertragliche Regelungen getroffen werden. Dabei ist auch zu berücksichtigen, dass in vielen Fällen Betroffene und Vertragspartner nicht identisch sind. Sachlich geht es um das gleiche Problem, das schon unter V. angesprochen wurde. Da es bei den Betroffenen (und in der Regel auch bei den Vertragspartnern) um Verbraucher geht, scheinen gesetzliche Regelungen sinnvoll.

Soweit die Daten nicht übertragen werden, müssen sie nach Art. 17 Abs. 1 Buchst. a DSGVO gelöscht werden.

VII. Novellierungsbedarf beim Schutz von Datenbanken

Die neuen Datensammlungen und die Nutzung von Big Data Techniken führen zu Novellierungsbedarf oder zumindest Klarstellungsbedarf bzgl. des gesetzlichen Schutzes von Datenbanken. Klarzustellen ist insbesondere, dass auch maschinell erzeugte Datensammlungen geschützt sein können. Darüber hinaus machen die neuen Techniken auch unstrukturierte Datensammlungen, die sich bei der Nutzung insbesondere technischer Geräte ergeben, zu erheblichen wirtschaftlichen Werten. Auch solche Datensammlungen müssen geschützt werden. Dies erfordert es, dass auch Investitionen in die Erzeugung solcher Daten als wesentliche Investition in die Datenbank angesehen werden müssen (wohl entgegen EuGH, Urt. v. 9. 11. 2004 - C-203/02, GRUR 2005, 244; Urt. v. 9. 11. 2004 - C-338/02 GRUR 2005, 252f.; Urt. v. 9. 11. 2004 - C-444/02, GRUR 254). Bezüglich der Datensammlung kann auch die Entnahme von nur 10% der Daten zu erheblichen wirtschaftlichen Gewinnen des Entnehmers auf Kosten des Inhabers der Datensammlungen führen. 10% der Daten sind nach der Ansicht des BGH kein wesentlicher Teil der Datenbank (BGH, Urt. v. 1.12.2010 – I ZR 196/08, GRUR 2011, 724). Daher bedarf auch die Eingriffs- und Schrankenregelung einer Überarbeitung, etwa bei der Bestimmung des Begriffs „wesentlicher Teil der Datenbank“. Soweit in der Praxis bzw. für bestimmte Daten oder Situationen zu beobachten ist, dass der Schutz exzessiv wird und dass diesem Exzess

beispielsweise mit dem Kartellrecht nicht oder im Einzelfall nicht in einer für die Marktakteure adäquaten Zeit beizukommen ist, sollte, bevor das Recht des Datenbankherstellers gar insgesamt in Frage gestellt wird, eher über schutzbeschränkende Mechanismen nachgedacht werden. Zu erwägen wäre insoweit, unberührt einer angemessenen Vergütung, den Schutz maßvoll zu begrenzen oder auch Anreize für eine zu vergütende Lizenzierung zu setzen. Demgegenüber bedarf es keiner Neuregelung der Schutzdauer des Datenbankrechts.

Der Schutz von Geschäftsgeheimnissen wird mit Recht im Zusammenhang mit dem Datenaustausch mit anderen Unternehmen angesprochen. Er ist essentiell für einen Datenaustausch, der sinnvoll von den beteiligten Unternehmen eingesetzt werden soll. Das ist nur durch einen ausreichenden Schutz möglich. Unabhängig von der Frage, ob der Geheimnisschutz dem Inhaber des Geheimnisses einen absoluten Schutz im Sinne eines absoluten Rechts gewährt oder nur einen Zugangsschutz, bleibt die Bedeutung der Geschäftsgeheimnisse unbestritten. Dies muss auch bei der Beurteilung des Schutzes von Datenbanken und der Nutzungsberechtigung daran berücksichtigt werden. Dabei muss der Schutz nach dem GeschGehG den Schutz nach den speziellen Gesetzen zum Schutz des Geistigen Eigentums ergänzen. Die Erfahrungen mit dem neuen GeschGehG müssen einfließen und ausgewertet werden.

VIII. Garantien für nicht personenbezogene Daten in internationalen Kontexten

Hier geht es um den Schutz von nicht-personenbezogenen Daten gegen den Zugriff durch Behörden von Drittländern. Hier ist es sinnvoll, Regeln einzuführen, die diesen Zugriff unterbinden, soweit es um Daten geht, die innerhalb der EU gespeichert werden. Ein Zugriff auf in Europa gespeicherte Daten darf auch aus völkerrechtlichen Gründen nur unter Einschaltung des jeweils betroffenen EU-Staats und unter Beachtung des dort geltenden Rechts zulässig sein.

Regeln für den Zugriff auf Daten zu nehmen, die außerhalb der EU gespeichert werden, sollten dagegen nicht getroffen werden. Hier müssen die Kunden von Cloud-Dienste-Anbietern selbst Vorsorge treffen, z.B., indem sie Sorge dafür tragen, dass die Daten nur innerhalb der EU gespeichert oder bei Verarbeitung außerhalb der EU sicher verschlüsselt werden. Jede andere Regelung wäre ein Eingriff in die Souveränität von

Drittstaaten, die im Gegensatz zur Situation bei personenbezogenen Daten nicht durch den Schutz von Grundrechten Dritter begründet werden kann.