



# Stellungnahme

## des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union COM(2017) 495 final

Stellungnahme Nr.: 4/2018

Berlin, im Januar 2018

### Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierehoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Michael Friedmann, Hannover
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

### Zuständig in der DAV-Geschäftsführung

- Ina Kitzmann

### Ansprechpartner in Brüssel

- Rechtsanwältin Eva Schriever, LL.M.

**Deutscher Anwaltverein**  
Littenstraße 11, 10179 Berlin  
Tel.: +49 30 726152-0  
Fax: +49 30 726152-190  
E-Mail: [dav@anwaltverein.de](mailto: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](mailto:bruessel@eu.anwaltverein.de)  
EU-Transparenz-Registernummer:  
87980341522-66

## **Verteiler**

---

### Deutschland

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

### Europa

Europäische Kommission  
- Generaldirektion Justiz  
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament  
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres  
- Rechtsausschuss  
- Ausschuss für Binnenmarkt und Verbraucherschutz  
- Ausschuss für Industrie, Forschung und Energie

Rat der Europäischen Union  
Ständige Vertretung der Bundesrepublik Deutschland bei der EU  
Justizreferenten der Landesvertretungen  
Rat der Europäischen Anwaltschaften (CCBE)  
Vertreter der Freien Berufe in Brüssel  
DIHK Brüssel  
BDI Brüssel

Presse

Frankfurter Allgemeine Zeitung

Süddeutsche Zeitung GmbH

Berliner Verlag GmbH

Redaktion NJW

Juve-Verlag

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 mit derzeit rund 65.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

**Das Ziel der Europäischen Kommission, einen freien Datenfluss in Europa zu fördern, verdient Unterstützung. Diesem Anliegen entspricht es, mitgliedstaatliche Vorschriften einzudämmen, die Provider dazu verpflichten, Daten ausschließlich in dem jeweiligen Mitgliedsstaat zu speichern.**

### **Dienstleistungsfreiheit**

Schon jetzt sind mitgliedstaatliche Bestimmungen, die zu einer Datenspeicherung im Inland verpflichten, im Hinblick auf die europäische Dienstleistungsfreiheit problematisch. Im Gesetzgebungsverfahren zur Einführung des § 113 b TKG vertrat die Europäische Kommission den Standpunkt, dass die für die Vorratsdatenspeicherung in Deutschland vorgeschriebene Inlandsspeicherung europarechtswidrig sei. Aus ähnlichen Gründen hat der DAV in seiner Stellungnahme [2/2017](#) kritisiert, dass § 43 e Abs. 4 BRAO den Anwaltskanzleien die Beauftragung von Dienstleistern aus anderen EU-Mitgliedsstaaten erschwert, da für eine solche Beauftragung Anforderungen aufgestellt werden, die für die Beauftragung inländischer Dienstleister nicht gelten.

### **Lokalisierungspflichten in autoritären Staaten**

Lokalisierungspflichten sind auch über die EU hinaus in einem menschenrechtlichen Kontext problematisch, da sie ein typisches gesetzgeberisches Instrument autoritärer Staaten sind und der staatlichen Kontrolle und Überwachung des Daten- und Internetverkehrs dienen. China und Russland haben weitreichende Lokalisierungspflichten eingeführt. Man darf hoffen, dass die Mitgliedsstaaten der EU derartigen Vorbildern nicht folgen.

Clouddienste sind technisch oft so ausgestaltet, dass sich die gespeicherten Daten auf Rechner in unterschiedlichen Rechenzentren, vielfach auch auf Rechner in

verschiedenen Ländern der Welt verteilen. Eine staatliche Überwachung dieser Dienste wird hierdurch erschwert. Lokalisierungspflichten sollen in autoritären Staaten die Überwachung erleichtern.

### **Beschränkung auf nicht-personenbezogene Daten**

Weder im Hinblick auf die Dienstleistungsfreiheit noch hinsichtlich des Schutzes der Freiheiten europäischer Bürger lässt sich die von der Kommission vorgeschlagene Begrenzung der Verordnung auf nicht-personenbezogene Daten begründen. Unter dem Gesichtspunkt der Dienstleistungsfreiheit sind Lokalisierungsbestimmungen für personenbezogene Daten genauso problematisch, wie dies bei nicht-personenbezogenen Daten der Fall ist. Soweit es um den Schutz von Daten europäischer Bürger vor einem erleichterten staatlichen Zugriff geht, besteht bei personenbezogenen Daten größerer Regelungsbedarf, als dies bei nicht-personenbezogenen Daten der Fall ist.

Mit einer Regelung, die ausschließlich für nicht-personenbezogene Daten gelten soll, betritt die Kommission im Übrigen „Neuland“. Der Personenbezug ist ein ausschließlich datenschutzrechtlicher Begriff, der ausschlaggebend ist für den Anwendungsbereich des Datenschutzes. Die Bestimmungen würden somit für alle Daten gelten, die nicht durch das Datenschutzrecht geschützt sind.

Dem Entwurf liegt die Vorstellung zugrunde, dass es Lokalisierungsbestimmungen des mitgliedstaatlichen Rechts gibt, die ausschließlich für nicht-personenbezogene Daten gelten. Ob dies tatsächlich in nennenswertem Umfang der Fall ist, ist zweifelhaft. Wie das Beispiel der Vorratsdatenspeicherung zeigt, werden Lokalisierungspflichten oft auf der Annahme beruhen, dass es um besonders schutzwürdige, sensible Daten geht. Schon aus diesem Grund wird die weit überwiegende Zahl von Bestimmungen über eine Lokalisierungspflicht maßgeblich für Daten mit Personenbezug gelten, sodass die vorgeschlagene Verordnung nicht anwendbar wäre.

## Unterscheidbarkeit personenbezogener und nicht-personenbezogener Daten

Anders als in früheren Jahren lässt sich heute nicht mehr trennscharf zwischen personenbezogenen und nicht-personenbezogenen Daten unterscheiden. Das maßgebliche Kriterium ist – nach geltendem Datenschutzrecht – die „Bestimmbarkeit“ einer Person, auf die sich ein Datum bezieht. Diese „Bestimmbarkeit“ wird durch die **voranschreitende Computertechnik** immer einfacher. Ein „Mann, 53, Anwalt, 10115 Berlin“ ist zwar auf den ersten Blick anonym, lässt sich aber mittels leicht verfügbarer Zusatzinformationen und mithilfe von Algorithmen ohne größere Schwierigkeiten identifizieren.

Parallel zu den sich verbessernden technischen Möglichkeiten der Re-Identifizierung wird der Begriff des Personenbezugs von den Gerichten, Datenschutzbehörden und Kommentatoren **immer weiter ausgelegt**. Nach der DSGVO ist eine namentliche Identifizierung für einen Personenbezug nicht mehr erforderlich. Vielmehr reicht es, dass sich Daten auf eine Person beziehen, die sich in einer Personenmenge von anderen Personen unterscheiden (individualisieren) lässt („singling out“), auch wenn eine namentliche Identifizierung unmöglich ist. Auch pseudonyme Daten gelten zudem nach der DSGVO als personenbezogen.

Vielfach lässt sich bei einem Datum nicht sicher vorhersagen, ob ein Personenbezug vorhanden ist. Stellt man – wie der EuGH in seiner Breyer-Entscheidung (EuGH vom 19.10.2016, Rs. C-582/14) – auf den genauen **Verarbeitungskontext** ab, kann ein und dasselbe Datum in dem einen Moment anonym sein („nicht-personenbezogen“), im nächsten Moment jedoch in den Händen eines Dritten personenbezogen.

Relativierungen des Personenbezuges erschweren jede trennscharfe Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten. Das Problem zeigt sich auch in der schwierigen Frage, wann Geodaten personenbezogene Daten sind.

Wie schwierig es ist, normativ-abstrakt eine Kategorie von Daten zu definieren, auf die das Datenschutzrecht nicht anwendbar ist, zeigte vor einigen Jahren die Diskussion um Google Street View. Bis zu dieser Diskussion war es für die meisten

Datenschutzrechtler selbstverständlich, dass „**Sachdaten**“ als Gegenbegriff zu „Personendaten“ nicht dem Datenschutzrecht unterliegen. In den Debatten um Google Street View wurde jedoch deutlich, dass sich bei der Kategorisierung von Daten nicht mehr überzeugend begründen lässt, dass „Sachdaten“ generell und ohne Rücksicht auf die näheren Umstände keinen Personenbezug haben.

In jüngerer Zeit gibt es eine ähnliche Diskussion um den Begriff der „**Maschinendaten**“, der zunehmend als Gegenbegriff zu „Personendaten“ verwendet wird. Datenschutzrechtlich lässt sich auch diese Datenkategorie nicht trennscharf vom Datenschutzrecht abgrenzen. Die Daten eines Fahrzeugs können stets auch Bezug zu dem Fahrer, Eigentümer oder Halter des Fahrzeugs haben. Die Daten eines Kühlschranks haben Bezug zu dessen Nutzern. Und die Daten einer Maschine haben Bezug zu der Person, die die Maschine programmiert, lenkt und steuert.

#### **Unklarheiten bei Art. 4**

Gemäß Art. 4 Abs. 1 des Entwurfs sind gesetzliche Bestimmungen untersagt, die eine Lokalisierungspflicht für Daten ohne Personenbezug vorsehen. Normadressat sind auch die Mitgliedsstaaten, die in Art. 4 Abs. 3 verpflichtet werden, gesetzliche Vorschriften aufzuheben, die gegen Art. 4 Abs. 1 des Entwurfs verstoßen.

Es sollte klargestellt werden, ob sich einzelne bereits mit Inkrafttreten der Verordnung gemäß des Anwendungsvorrangs des Unionsrechts auf die vorrangige Verordnung berufen können und den Mitgliedstaaten daneben die Möglichkeit verbleibt widersprechendes nationales Recht innerhalb der in Art. 4 Abs. 3 genannten Frist zu ändern.

Art. 4 zwingt die Mitgliedsstaaten überdies, zwischen gesetzlichen Lokalisierungspflichten zu unterscheiden, die für personenbezogene Daten gelten, und gesetzlichen Lokalisierungspflichten für Daten ohne Personenbezug. Eine derartige Unterscheidung dürfte in keinem EU-Mitgliedsstaat üblich sein. Jeder Mitgliedsstaat müsste somit bestehende gesetzliche Lokalisierungspflichten dahingehend analysieren, ob sie in die eine (Personenbezug) oder andere (kein Personenbezug) Kategorie fallen.

Art. 4 lässt unklar, ob eine Lokalisierungspflicht nach der Verordnung schon dann nicht angeordnet werden darf, wenn nicht auszuschließen ist, dass sie sich auch auf personenbezogene Daten bezieht. Einen solchen Fall dürfte es kaum geben, sodass die vorgeschlagene Verordnung bei dieser Lesart vollständig ins Leere laufen würde. Sollte es der Kommission um eine Schwerpunktbetrachtung gehen, nach der darauf abgestellt wird, welche der beiden Datenkategorien (mit oder ohne Personenbezug) im Vordergrund der jeweiligen Regelung steht, kommt eine solche Betrachtung in Art. 4 nicht hinreichend zum Ausdruck.

### **Datenportabilität**

Art. 6 soll Rahmenbedingungen für eine erleichterte Datenportabilität schaffen. Präzise Regelungen einer solchen Portabilität sollen der Selbstregulierung überlassen bleiben. Statt – wie Art. 20 DSGVO – ein „Recht auf Datenübertragbarkeit“ zu schaffen, setzt Art. 6 auf freiwillige Verhaltensregeln der Wirtschaft. Statt unterschiedliche Regelungen für die Datenübertragbarkeit bei personenbezogenen Daten und bei Daten ohne Personenbezug zu schaffen, sollten – vor einer neuen Regelung – die praktischen Erfahrungen mit Art. 20 DSGVO abgewartet werden.