Berlin, im Januar 2011
Stellungnahme Nr. 4/2011

abrufbar unter
www.anwaltverein.de

Stellungnahme des Deutschen Anwaltvereins

durch den Ausschuss Informationsrecht

zum

Gesamtkonzept für den Datenschutz in der Europäischen Union

Mitglieder des Informationsrechtsausschusses:

Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
Rechtsanwältin Isabell Conrad, München
Rechtsanwalt Niko Härting, Berlin (Berichterstatter)
Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
Rechtsanwalt Prof. Dr. Jochen Schneider, München
Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung:

Rechtsanwältin Tanja Brexl

Verteiler:

Europa:

- Europäische Kommission
    - Generaldirektion Justiz
- Europäisches Parlament
    - Rechtsausschuss
    - Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres
- Rat der Europäischen Union
- Ständige Vertretung Deutschlands bei der EU
- Rat der Europäischen Anwaltschaften (CCBE)
- Justizreferenten der Landesvertretungen

Deutschland:

- Bundesministerium des Innern
- Bundesministerium der Justiz

- Landesjustizverwaltungen

- Bundesrat
- Rechtsausschuss des Deutschen Bundestages
- SPD-Fraktion im Deutschen Bundestag
- CDU/CSU-Fraktion des Deutschen Bundestages, Arbeitsgruppe Recht
- Fraktionen BÜNDNIS 90/DIE GRÜNEN im Deutschen Bundestag
- FDP-Fraktion im Deutschen Bundestag
- Fraktion DIE LINKE im Deutschen Bundestag

- Vorstand und Geschäftsführung des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Vorsitzende des FORUMs Junge Anwaltschaft

- Deutscher Richterbund
- Bund Deutscher Verwaltungsrichter
- Deutscher Steuerberaterverband
- GRUR
- BITKOM
- DGRI
- Bundesverband der Freien Berufe

- Bundesrechtsanwaltskammer
- Bundesnotarkammer

- Deutscher Notarverein e. V.

- Redaktion NJW
- JUVE-Verlag
- ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 68.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene

---

Die Mitteilung der Kommission gibt Anlass zu einer Reihe von grundsätzlichen Anmerkungen:

1. Der Datenverkehr in der vernetzten Informationsgesellschaft führt zu **Risiken**, die in der Mitteilung eingehend analysiert werden. Dies gilt allerdings nicht nur für die private Datenspeicherung, sondern auch für die staatliche Überwachung. Dem Zugriff des Staates auf die „Spuren" der Kommunikationsbeziehungen müssen im Interesse der Bürgerrechte deutliche Schranken gesetzt werden.

2. Die vernetzte Kommunikation eröffnet auch **Chancen** für die ungehinderte Ausübung von Freiheitsrechten und ist daher ihrerseits schützenswert. Dies, insbes. die Informationsfreiheit als Gegengewicht, kommt in der Mitteilung nicht hinreichend deutlich zum Ausdruck.

3. Im nicht-öffentlichen Bereich ist das Verbot oder die Einschränkung der Datenverarbeitung im Normalfall mit einem Eingriff in **Freiheitsrechte** der datenverarbeitenden Person oder Stelle verbunden. Ein solcher Eingriff kann nur dann durch den Datenschutz legitimiert sein, wenn eine Abwägung der wechselseitigen Freiheitsrechte ergibt, dass der Datenschutz schwerer wiegt als die Freiheitsrechte der verarbeitenden Person oder Stelle. Dies gilt umso mehr, als der vernetzte Informationsaustausch es mit sich bringt, dass der Einzelne regelmäßig in eine **Doppelrolle** als Subjekt und Objekt der Datenverarbeitung gerät.

4. Für den durch **Art. 10 EMRK** geschützten Informations- und Meinungsaustausch ist die vernetzte Kommunikation unverzichtbar. Das Recht auf freie Meinungsäußerung schließt nach Art. 10 Abs. 1 Satz 2 EMRK die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriff öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Jede Reglementierung des Meinungs- und Informationsflusses im nicht-öffentlichen Bereich birgt die Gefahr eines Eingriffs in Art. 10 EMRK. Dies gilt auch dann, wenn die Reglementierung aus Gründen des Datenschutzes erfolgt.

5. Die latente Gefahr einer übermäßigen Einschränkung von Freiheitsrechten im Zeichen des Datenschutzes besteht ausschließlich im **nicht-öffentlichen Bereich** und stellt einen kardinalen Unterschied zum Datenschutz gegenüber staatlichen Stellen dar. Da der Schutz der Daten eines Bürgers im nicht-öffentlichen Bereich oft notwendig mit der Beschränkung von Freiheitsrechten verbunden ist, bedarf es klarer, praktikabler **Abwägungsregeln**.

6. Bei jedweder Abwägung ist zu berücksichtigen, dass eine Datenverarbeitung für den jeweils Betroffenen dann gefährlicher ist, wenn er in einem **Abhängigkeitsverhältnis** zu der Daten verarbeitenden Stelle steht. Im Verhältnis zwischen Arbeitgeber und Arbeitnehmer müssen für die Datenverarbeitung und –nutzung daher beispielsweise andere Regeln gelten als bei der Kommunikation unter Freunden und Bekannten in sozialen Netzwerken.

7. Jede staatliche Kontrolle der Datenverarbeitung kann im nicht-öffentlichen Bereich die Freiheitsrechte der Bürger gefährden. Dies gilt auch dann, wenn eine „unabhängige“ Stelle für die Kontrolle verantwortlich ist. Von einer Staatsferne bzw. **„Unabhängigkeit“** der Kontrollinstanz kann immer nur dann die Rede sein, wenn es um eine Kontrolle der staatlichen Datenverarbeitung geht. Wird dagegen einer Behörde die Befugnis eingeräumt, gegenüber Bürgern bzw. privaten Unternehmen Kontrollmaßnahmen zu ergreifen, handelt es sich um **hoheitliche Befugnisse**, die dieselben Fragen des Freiheitsschutzes aufwirft, die sich auch bei anderen staatlichen Maßnahmen stellen. Gegenüber dem Bürger ist der Staat stets Staat, auch wenn er sich in das Gewand einer „unabhängigen“ Stelle kleidet.

8. Wegen der staatlichen Kontrolle bzw. Aufsicht, die mit Maßnahmen einer Datenschutzbehörde verbunden sind, gerät das **Anwaltsgeheimnis** in Gefahr, wenn Verpflichtungen des Anwalts zur **„Rechenschaft**“ über den Umgang mit Daten erwogen werden. Die Kontrolle über den sorgsamen Umgang mit sensiblen Daten sollte Aufgabe der Stellen sein, die für die Überwachung pflichtgemäßen Handelns der Anwälte verantwortlich sind – das sind in Deutschland die Anwaltskammern. Der Datenschutz legitimiert keine staatlichen Kontrollen der anwaltlichen Berufsausübung. Das Anwaltsgeheimnis schützt die Vertraulichkeit der Kommunikation zwischen Mandant und Anwalt, gehört nach deutschem Verfassungsrecht zu den Grundbedingungen des Rechtsstaates und muss daher von jedweder staatlichen Kontrolle und Einsichtnahme frei bleiben.

9. Die vernetzte Kommunikation und die damit – jedenfalls theoretisch – oft mögliche Zusammenführung und Verknüpfung von Datenbeständen bringen es mit sich, dass ein großer Teil der im Internet verfügbaren Daten als **personenbezogen** angesehen werden kann, wenn man von einem weiten Begriff des Personenbezugs ausgeht. Je mehr Daten unter den Begriff fallen, desto mehr stellt sich die Frage, ob es nicht – im nicht-öffentlichen Bereich – einer stärkeren Differenzierung bedarf bei dem Schutz dieser Daten. Bei Gesundheitsdaten leuchtet es unmittelbar ein, dass diese Daten ohne Einwilligung des Betroffenen nur in eng zu definierenden Ausnahmefällen verarbeitet werden dürfen. Bei einer E-Mail-Adresse, die als personenbezogenes Datum anzusehen ist, fällt es dagegen schwer, einen einleuchtenden materiellen Grund zu benennen, weshalb der Adressinhaber gefragt werden muss, wenn die Adresse elektronisch gespeichert wird. Das **Einwilligungs-/Verbotsprinzip** gehört bei Daten, die ein selbstverständlicher Bestandteil der alltäglichen Kommunikation sind, abgeschafft.

10. Das Einwilligungs-/Verbotsprinzip lässt sich keinesfalls damit legitimieren, dass man von einer Art (eigentumsähnlichen) absoluten Verfügungsrecht des Betroffenen ausgeht. Daten „gehören“ einer Person nicht (allein), sie sind vielmehr (auch) ein **Abbild sozialer Realität** und als notwendiger Bestandteil der sozialen und gesellschaftlichen Interaktion schützenswert. Das Einwilligungs-/Verbotsprinzip darf nicht dazu führen, dass der soziale Interaktionsraum schleichend **„privatisiert“** und hierdurch die freie Kommunikation in einer demokratischen Gesellschaft behindert wird.

11. Das Einwilligungs-/Verbotsprinzip wird im Übrigen den Realitäten der Netzkommunikation nicht gerecht. Dies zeigt die Diskussion um die Anforderungen an einen **„informed consent“**: Kommunikation im Internet ist in weiten Bereichen Massenkommunikation. Wenn der Betreiber eines sozialen Netzwerks von einzelnen Nutzern Einwilligungserklärungen (benötigt und) verlangt, ist dies nicht anders realisierbar als durch vorgefertigte, standardisierte Erklärungen. Damit derartige Erklärungen noch den Sinn erfüllen können, dem Nutzer eine autonome Entscheidung zu ermöglichen, sind ausführliche und verständliche Erklärungen über die beabsichtigte Datennutzung unverzichtbar („informed consent“). Wenn der Nutzer

in Kenntnis transparenter Erläuterungen die Plattform nutzt, ist die Autonomie seines Handelns gesichert. Dies dann mit vorgefertigten (formelhaften) Einwilligungserklärungen zu verbinden, ist entbehrlich. Verstärkte **Transparenzregeln** und gesetzlich genauer geregelte Anforderungen an Datenschutzbestimmungen sollten in weiten Bereichen an die Stelle des Einwilligungs-/Verbotsprinzip treten.

12. Dass die 15 Jahre alte EU-Datenschutzrichtlinie den Herausforderungen des Internet nicht mehr in jeder Hinsicht gerecht wird, ist unbestritten. Dennoch sei abschließend darauf hingewiesen, dass es auch gute Gründe zu einer gewissen Zurückhaltung bei der Einführung neuer Regelungen geben mag. Dies betrifft die evtl. zu starke Berücksichtigung aktueller technischer und sozialer Phänomene. Insofern empfiehlt sich neben mehr abstrakter, genereller Regelung auch eine gewisse Zurückhaltung. Insbesondere unter jungen Menschen, die eine Welt ohne das Internet nicht mehr kennen, lässt sich beobachten, dass sich **Kommunikationsgewohnheiten** ändern; die wahrgenommenen Grenzen zwischen Privatem und Öffentlichem verschieben sich. Hinzu kommt die vielfach zu beobachtende Tendenz einer Minderheit von Internetnutzern, äußerst freigiebig, gelegentlich sogar **exhibitionistisch** sehr Persönliches in alle Welt zu verbreiten. Auch wenn dies den Mehrheitsgeschmack nicht trifft, ist auch unvernünftiges Verhalten durch die Freiheit der Entfaltung der Persönlichkeit geschützt. Neue Regelungen des Datenschutzes dürfen weder zu einer reglementierenden Bevormundung von Bürgern führen, die sich nach mehrheitlicher Auffassung unbesonnen oder geschmacklos verhalten. Eben so wenig sollte eine Neuregelung vorschnell tradierte Grenzen zwischen Privatem und Öffentlichem festschreiben, ohne den laufenden Wandel gesellschaftlicher Anschauungen abzuwarten und zu würdigen.