DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

DGRI e. V. • Bahnhofstraße 10 • D-76137 Karlsruhe

European Commission
Directorate – General Justice
Unit C3 – Data protection
1049 Brussels
BELGIUM

Vorab per E-Mail: just-privacy-consultations@ec.europa.eu

Dr. Anselm Brandi-Dohrn, maître en droit
1. Vorsitzender
Rechtsanwalt
Oranienstraße 164, D-10969 Berlin

Telefon: +49-30-61 68 94 09
Telefax: +49-30-61 68 94 56
E-Mail: abrandi-dohrn@boetticher.com

Berlin, 14. Januar 2011

Online-Konsultation „Gesamtkonzept für den Datenschutz in der Europäischen Union"

Hier: **Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI e.V. - Registrier-Nr. 21625424990-18)**
Ihr Zeichen: **KOM(2010) 609**

Sehr geehrte Damen und Herren,

die *Deutsche Gesellschaft für Recht und Informatik e.V.* (DGRI) bedankt sich für die Gelegenheit zur Stellungnahme im Rahmen der am 04.11.2010 begonnenen Online-Konsultation zum „Gesamtkonzept für den Datenschutz in der Europäischen Union".

Gerne nutzt die Gesellschaft die Gelegenheit, den bei ihr versammelten Sachverstand erneut in den Diskussionsprozess einzubringen, wie sie dies bereits durch eine Stellungnahme im Vorfeld der „Targeted Private Stakeholders Consultation" vom 01.07.2010 getan hat.

Damit die Intentionen der DGRI besser einzuordnen sind, dürfen wir unsere Vereinigung zunächst kurz vorstellen:

Die ***Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)*** ist eine unabhängige, wissenschaftliche Vereinigung. Sie befasst sich mit Fragen im Bereich der Schnittstelle zwischen Informatik und EDV-Technik einerseits sowie Recht und Wirtschaft andererseits. Sie hat sich die Förderung der Zusammenarbeit von Lehre, Forschung und Praxis in den Bereichen

- Rechtsfragen der Informationsverarbeitung,
- Einsatz der Informationstechnik im Rechtswesen und
- Schaffung der rechtlichen Rahmenbedingungen für die Informationstechnik

zur Aufgabe gestellt. Ansprechpartner der Gesellschaft sind Wissenschaftler und Praktiker in dem so beschriebenen Tätigkeitsfeld sowohl aus dem Gebiet der Rechtswissenschaften als auch der Technik. Mit ihnen sucht die Gesellschaft den Austausch von Wissen, Erfahrungen und Meinungen.

Dies vorausgeschickt, nehmen wir, unter Mitwirkung des Fachausschusses Datenschutz, zu einzelnen Punkten des Gesamtkonzepts, die aus unserer Sicht von grundlegender Bedeutung sind, wie folgt Stellung:

Zu Ziffer 1 **Neue Herausforderungen für den Datenschutz:**

Ein verstärkter Schutz von Betroffenen durch eine Neugestaltung der EG-Datenschutzrichtlinie darf nicht zu einer Bevormundung der einzelnen Betroffenen führen. Auch Ist es nicht geboten, ihnen alle Risiken abzunehmen, die sie freiwillig eingegangen sind.

Den ohne Zweifel vorhandenen neuen Risiken für das Persönlichkeitsrecht bei Online-Aktivitäten, vor allem im Rahmen sozialer Netzwerke, stehen früher nicht vorstellbare Kontakt-, Selbstdarstellungs- und Gestaltungsmöglichkeiten des einzelnen Betroffenen gegenüber.

Es sollte nicht vergessen werden, dass niemand gezwungen wird, an sozialen Netzwerken teilzunehmen und dort von sich aus persönliche Daten zur Verfügung zu stellen. Wer dies tut und dabei für die Nutzung der Netzwerke in der Regel nichts zahlen muss, kann nicht völlig überrascht sein, wenn seine personenbezogenen Daten vom Betreiber des Netzwerkes wirtschaftlich genutzt werden, um das Netzwerk finanzieren zu können und dabei auch Gewinne zu erzielen.

Bei der Neugestaltung der Richtlinie ist deshalb im Hinblick auf soziale Netzwerke vor allem darauf zu achten, dass

1. der Betroffene auf Wunsch jederzeit feststellen kann, welche seiner personenbezogener Daten wo gespeichert sind und wozu sie genutzt werden;
2. Verarbeitungen und Nutzungen, die für den Betroffenen bei objektiver Betrachtung überraschend sind und mit denen er nicht rechnen muss, nur mit seinem Wissen und seiner expliziten Zustimmung erfolgen;
3. Betroffene, die die Folgen ihres Tuns nicht oder nicht voll abschätzen können (vor allem Kinder, möglicher Weise auch Menschen mit bestimmten geistigen Behinderungen) besonders geschützt werden.

Ziffer 1. kann durch Vorschriften zur Schaffung von Transparenz und der Regelung von Auskunftsrechten nachgekommen werden, Ziffer 2. beispielsweise durch Anlehnung an die Vorgaben zum wirksamen Einbeziehen von Allgemeinen Geschäftsbedingungen. Die in Ziffer 3. genannten Personengruppen können durch Sonderregelungen zum einen betreffend der Einwilligung geschützt werden,

zum anderen durch massiv beschränkte gesetzliche Erlaubnisse zur Verarbeitung deren personenbezogener Daten.

Bezüglich Ziffer 1 ist zu betonen, dass dem Betroffenen ein vollständiger Überblick über die zu seiner Person vorliegenden Daten möglich sein muss, ohne dass ihm ein unzumutbarer Aufwand entsteht. Soweit davon auszugehen ist, dass Betroffene bestimmte Speicherungs- und Nutzungsvorgänge in der Regel kennen wollen, ist daher Sorge zu tragen, dass sie diese Daten "auf Knopfdruck", also nahezu ohne Aufwand abrufen können. Für welche Daten dies zutrifft, könnte Gegenstand von Branchenregelungen sein, bei deren Formulierung auch Verbraucherverbände und ähnliche Organisationen zu beteiligen wären.

Zu Ziffer 2.1.1 Angemessener Schutz des einzelnen in allen Situationen

a. Der schon jetzt sehr weite Begriff der "personenbezogenen Daten" darf nicht noch weiter ausgedehnt werden.

Bei einer weiteren Ausdehnung des Begriffs würde es kaum noch Daten geben, bei denen keinerlei Bezug zu einem Betroffenen hergestellt werden kann. Letztlich wären fast alle irgendwo vorhandenen Daten als personenbezogen anzusehen. Das würde dazu führen, dass der Schutz des einzelnen nicht etwa gestärkt, sondern ganz im Gegenteil geschwächt würde.

Wenn die EG-Datenschutzrichtlinie nach einer weiteren Ausdehnung des Begriffs mehr oder weniger alle Daten erfassen würde, die existieren, müsste das allgemeine Schutzniveau der Richtlinie zwangsläufig abgesenkt werden. Sie wäre dann nämlich auch auf Situationen anzuwenden, in denen ein starker Schutz des Betroffenen nicht gerechtfertigt wäre und auch nicht akzeptiert würde. Das zeigt sich etwa bei Daten, die lediglich die räumliche Lage eines Grundstücks angeben und die üblicherweise in Registern verwendet werden, um ein Grundstück überhaupt identifizieren zu können.

Es wird daher angeregt, es bei dem – seit Jahren in der Praxis bewährten – relativen Ansatz zu belassen, also nur auf dasjenige Zusatzwissen und die Möglichkeiten abzustellen, das bzw. die der konkreten verantwortlichen Stelle zur Verfügung stehen, nicht auf das Wissen und die Möglichkeiten, die irgendjemand auf der Welt theoretisch hat oder haben kann (was ein praxisfremder absoluter Ansatz wäre).

Zudem sollte betont werden, dass es bei der Frage, mit welchem Zusatzwissen und –aufwand die jeweilige verantwortliche Stelle einen Personenbezug herstellen kann, nicht nur auf die dieser Stelle „vernünftigerweise" zur Verfügung stehenden und von dieser einsetzbaren Mittel ankommt, sondern es sich dabei jeweils auch um *legale* Mittel handeln muss. Dies führt zwar zu einer weiteren Einschränkung des Begriffs der personenbezogenen Daten. Jedoch greifen bei nicht-legalen Mitteln schon andere Sanktionen der Rechtsordnungen, etwa aus dem Strafrecht. Ferner wäre datenschutzrechtlich die Folge, dass die diesbezügliche Datenverarbeitung für sich genommen rechtswidrig ist. Zudem sollte Ausgangspunkt der Gesetzgebung nicht etwaiges nicht-legales Verhalten sein, vielmehr ist Ausgangspunkt ein rechtstreues Verhalten.

b. Festhalten am Anknüpfungspunkt der „personenbezogenen Daten"

Ein Festhalten am Begriff der „personenbezogenen Daten" erscheint geboten und zweckdienlich. Auf diesen Anknüpfungspunkt wird in den verschiedenen nationalen Rechtsordnungen zum Teil schon seit Jahrzehnten zurückgegriffen, es gibt entsprechend umfangreiche (nationale) Erfahrungen und Rechtsprechung dazu. Auch die EU-Datenschutz-Richtlinie von 1995 verwendet diesen Anknüpfungspunkt („*personal data*"), alle Mitgliedsstaaten haben diesen in ihre Datenschutzgesetzgebung übernommen, ebenso wie die Rechtsprechung der Europäischen Gerichte zu diesem Anknüpfungspunkt bereits Erfahrung sammeln konnte.

Die Ansicht, die an die „Privatheit" der Daten anknüpfen will („*privacy*"), übersieht, dass private Daten zwangsläufig nur eine Teilmenge der personenbezogenen Daten sind, denn Privatheit steht nach dem Rechtsverständnis der meisten Mitgliedstaaten nur natürlichen Personen zu: Private Daten sind damit immer auch personenbezogenen.

Es ist kein Grund ersichtlich, private Daten als Untergruppe der personenbezogenen Daten einem noch stärkeren oder zusätzlichen besonderen Schutz zu unterstellen, der über den Schutz personenbezogener Daten hinausgeht. Es erscheint vielmehr sinnvoller, den Schutz von personenbezogenen Daten als Obermenge möglichst hoch anzusetzen bzw. hoch zu belassen, so dass über diesen hohen Schutz etwaige Teilmengen, wie hier die privaten (personenbezogenen) Daten automatisch gleichstark mitgeschützt werden. Ansonsten entstünden neue Abgrenzungsprobleme mit den sensitiveren "privaten" Daten, wobei zu beachten ist, dass nicht alle privaten Daten zwingend (besonders) schützenswert sind und sich die Frage stellt, wann aus privaten (personenbezogenen) Daten öffentliche (personenbezogene) Daten werden und wie dieser Weg umkehrbar ist.

Es sollte daher bei dem bewährten und greifbaren Begriff der „personenbezogenen Daten" verbleiben.

Zu Ziffer 2.1.2 Mehr Transparenz für die von der Verarbeitung Betroffenen

Einem Betroffenen, der Transparenz darüber wünscht, was mit seinen Daten geschieht, ist es in der Regel zumutbar, selbst aktiv zu werden, um sich diese Informationen zu beschaffen.

Die Darstellung im Gesamtkonzept trennt nicht genügend zwischen der Frage,

- welche Informationen für den Betroffenen lediglich auf Wunsch verfügbar sein müssen und
- welche Informationen ihm die verantwortliche Stelle ohne besondere Aufforderung aktiv zur Verfügung stellen muss.

Beides muss deutlich unterschieden werden.

(a) Eine Sonderrolle sollten die oben erwähnten besonderen Personengruppen (Kinder, möglicher Weise auch bestimmte behinderte Personen), da von diesen unter Umständen nicht verlangt werden kann, selbst in ausreichendem Maße aktiv zu werden; bezüglich dieser sollte daher die verantwortliche Stelle aktiv werden müssen.

*(b) **Eine allgemeine Anzeigepflicht für Datenschutzverstöße, die allein an die Tatsache eines Verstoßes anknüpft, geht zu weit.***

Ausreichend erscheint eine Regelung, die sich an § 42 a BDSG orientiert.

Das Anzeigen aller Arten von Verstößen gegenüber den Aufsichtsbehörden, also auch solcher, die den Betroffenen letztlich gar nicht beeinträchtigen (etwa weil die Folgen eines Verstoßes inzwischen bereits behoben wurden) bindet die knappen Ressourcen der Aufsichtsbehörden in unnötiger Weise und ist daher abzulehnen.

Eine Anzeige von Verstößen „nur" den jeweils Betroffenen gegenüber kann dagegen sinnvoll sein.

Die größte Problematik wird insgesamt in der Definition des „Verstoßes" gesehen, gerade dann, wenn die Nichteinhaltung der Anzeigepflicht geahndet werden soll, was wiederum sinnvoll und nötig erscheint: Dann aber muss nach den verfassungsrechtlichen Regelungen über die Bestimmtheit strafrechtlicher Normen eine Norm ausreichend klar definieren, wann ein Verstoß vorliegt und wann nicht. Die Frage, ob eine bestimmte Datenverarbeitung (noch) zulässig ist oder aber (schon) nicht mehr, ist oft nicht einfach zu klären, etwa dann, wenn mit mehreren unbestimmten Rechtsbegriffen gleichzeitig gearbeitet werden muss („erforderlich", „angemessen") und/oder zusätzlich Abwägungen zu treffen sind bezüglich derer zwangsläufig eine gewisse Unsicherheit verbleibt.

Es wird angeregt, sich besonders mit der Frage zu beschäftigen, welche Verstöße zu einer Anzeigepflicht führen sollen, und insofern klare und eindeutige Vorgaben aufzustellen. Denkbar wäre ein Anknüpfen an bestimmte Arten von personenbezogenen Daten.

Zu Ziffer 2.1.5 Einwilligung

Es wird begrüßt, wenn die Anforderungen an eine wirksame datenschutzrechtliche Einwilligung präzisiert und gestärkt werden.

Jedenfalls bei der Novellierung der Richtlinie, gegebenenfalls aber auch im späteren Richtlinientext sollte zwischen

- der Einwilligung von Beschäftigten auf der einen Seite und
- der Einwilligung von Kunden auf der andere Seite

unterschieden werden - zu unterschiedlich sind die jeweiligen Grundkonstellationen:

- Auf der einen Seite der abhängige (weil schon in einem Vertragsverhältnis befindliche) Arbeitnehmer, mit dessen Personaldaten sein Arbeitgeber bestimmte Verarbeitungen durchführen muss oder will,
- auf der anderen Seite der Kunde, der die Wahl hat, ob er ein bestimmtes Angebot nutzt oder auf einen anderen Anbieter zurückgreift, der ihm bezüglich der Handhabung seiner Daten vertrauenswürdiger erscheint.

Für beide Bereiche sind EU-weit harmonisierte Anforderungen essentiell, da viele Unternehmen grenzüberschreitend tätig sind und es nicht vermittelbar ist, warum etwa bei einer gemeinsamen (EU-weiten) Personalabteilung die Anforderungen an eine Einwilligung der Arbeitnehmer aus dem Land A „schwächer" ausgestaltet sein darf als bei Mitarbeitern aus dem Land B.

(i) Im Bereich des Beschäftigtendatenschutzes wird es nicht möglich sein, alle auftretenden Fragen mittels Einwilligungen zu lösen. Zu fordern ist vielmehr, dass die Konzeption der Kommission um Überlegungen zu einem spezifischen Arbeitnehmerdatenschutzrecht auf EU-Ebene ergänzt wird. Ausschließlich nationale gesetzliche Regelungen oder der Rückgriff auf allgemeine Datenschutzregelungen der Europäischen Union reichen auf diesem Gebiet nicht mehr aus.

(ii) Bei Kundendaten gilt dies ebenfalls: Angebote beispielsweise im Internet richten sich oft an ein grenzüberschreitendes Publikum, gerade innerhalb des Binnenmarktes der EU mit seinen harmonisierten Verbraucherschutzregelungen. Das Erstellen, Vorhalten und ständige Pflegen und Aktualisieren von mehr als zwei Dutzend unterschiedlichen Einwilligungserklärungen an die jeweiligen nationalen Vorgaben verursacht unnötigen Aufwand bei den Betreibern, vor allem aber ist es einer übersichtlichen und transparenten Darstellung gegenüber den Kunden sehr abträglich. Durch eine Vollharmonisierung dieser Fragen kann ein einheitliches Niveau geschaffen werden.

(iii) Gleichzeitig mit der Präzisierung und Vereinheitlichung von Anforderungen an die eigentliche Einwilligung sollten die Anforderungen an deren Begleitpflichten präzisiert und harmonisiert werden, etwa zum Umfang, in dem ein Betroffenen vor Abgabe einer Einwilligung informiert/aufgeklärt werden muss: Denn es nützt wenig, wenn zwar die Einwilligungserklärung selbst präzisiert und vor allem harmonisiert ist, bei den einhergehenden Begleitpflichten aber wieder jeder Mitgliedsstaat eigene Regelungen schaffen könnte und damit die Harmonisierung des Einwilligungsvorgangs konterkarieren würde.

Dabei sollte auch berücksichtigt werden, dass es z. B. bei Telemediendiensten nicht immer ohne Weiteres möglich ist, die Kenntnis der Sachlage als Voraussetzung für eine Einwilligung herzustellen. Es erscheint angemessener, hier grundsätzlich auch das sogenannte Opt-out-Verfahren vorzusehen. Dafür braucht man standardisierte, einfach zu handhabende und für den Betroffenen transparente Regelungen. Hierbei sollte auch auf die Konsistenz mit den Regelungen im Bereich eCommerce (z. B. Wettbewerbsrecht) geachtet werden.

Bei der Präzisierung und Harmonisierung der Einwilligung und etwaiger Begleitpflichten sollten zudem die besonderen Anforderungen und Umstände bei Einwilligung von Minderjährigen beachtet werden. Sinnvoll erscheint, eine feste Altersgrenze einzuführen und/oder eine ausdrückliche Vertretungsbefugnis durch die Eltern o. Ä. zu regeln. Gerade bei den sozialen Netzwerken haben die Anbieter oft mit Minderjährigen zu tun – und zwar grenzüberschreitend -, ohne aber konkrete Vorgaben zu haben, welche Anforderungen an die Wirksamkeit der Einwilligung eines Minderjährigen gestellt werden.

Zu Ziffer 2.1.6 Schutz sensibler Daten

Der Begriff der sensiblen Daten sollte nicht um weitere Datenkategorien erweitert werden.

Eine solche Erweiterung könnte die unerwünschte Folge haben, dass die Datenschutzbemühungen künftig nur noch auf die dann sehr umfangreichen Arten sensitiver Daten konzentriert werden. Das Schutzniveau hinsichtlich der anderen Daten könnte dadurch sinken.

Zu Ziffer 2.1.7 Wirksame Rechtsbehelfe und Sanktionen

Eine umfassende gerichtliche Klagebefugnis von Datenschutzbehörden geht in die falsche Richtung und stellt keine adäquate Lösung dar.

Notwendig ist es vielmehr, den Datenschutzbehörden selbst ausreichende eigene Anordnungsbefugnisse zu geben. Sofern sie entsprechende Anordnungen treffen, hat der für die Verarbeitung Verantwortliche die Möglichkeit, die Rechtmäßigkeit einer solchen Anordnung gerichtlich überprüfen zu lassen. Unterlässt er dies, besteht keine Notwendigkeit, Gerichte zu involvieren.

Zu Ziffer 2.2.4 Mehr Verantwortung der für die Verarbeitung Verantwortlichen

Die Absicht, die Benennung unabhängiger Datenschutzbeauftragter zwingend vorzusehen, wird uneingeschränkt begrüßt.

Der Datenschutzbeauftragte im Unternehmen ist eine Institution der Selbstkontrolle. Diese Institution hat sich nicht nur in Deutschland bewährt, sondern wurde in den letzten Jahren vermehrt auch in anderen Mitgliedstaaten vorgesehen, wenn auch in der Regel nur auf freiwilliger Basis.

Es ist deshalb nachhaltig zu empfehlen, betriebliche Datenschutzbeauftragte verbindlich vorzusehen und dafür Meldepflichten gegenüber Datenschutzbehörden abzubauen. Das dient dem Abbau von Bürokratie und vermeidet unnötigen Aufwand.

Die Absicht, die weitere Förderung von Technologien zum Schutz der Privatsphäre und der Möglichkeiten für die konkrete Umsetzung des Privacy-by-Design-Konzepts zu prüfen, wird begrüßt. Insbesondere werden zuverlässige, einfache Verfahren für Signatur und Verschlüsselung von Daten benötigt. Hierfür sind vollharmonisierte Standards für handhabbare Authentisierungs- und Verschlüsselungsverfahren und -systeme erforderlich.

Zu Ziffer 2.4.1 Internationaler Datentransfer

Das Vorhaben der Kommission, das Verfahren zu vereinfachen und zu vereinheitlichen, wird uneingeschränkt begrüßt.

Dabei bietet es sich in Anbetracht der enorm gestiegenen Rolle der Auftragsdatenverarbeitung an, die derzeit damit verbundenen Restriktionen bei Dienstleistern in einem Drittland zu überdenken und das Modell einer Auftragsdatenverarbeitung insofern nicht mehr kategorisch auszuschließen. Dies gilt umso mehr, wenn der Dienstleister in einem Drittland gemäß den Vorgaben der Kommission als „sicher" gilt, etwa durch Unterzeichnung des EU-Standardvertrags.

Darüber hinaus sind unverändert Regelungen für den Datenverkehr innerhalb eines Konzerns oder einer Unternehmensgruppe nötig und zwar wiederum sowohl betreffend Personaldaten wie auch Kundendaten. Derzeit sind in der Praxis diesbezügliche Datenflüsse oft kaum oder nur sehr schwer rechtmäßig darstellbar, was aber an der Realität vorbeigeht: Nahezu jedes Unternehmen mit mehreren Tochterfirmen verfügt über eine zentrale Personalabteilung und/oder über eine zentrale Kundendatenbank. Dieser Realität kann sich ein Unternehmen in einer globalisierten Welt auch künftig nicht entziehen.

Es wird als sehr dringlich erachtet, hierfür explizite Regelungen zu schaffen, gerade auch im Hinblick auf Konzerne im internationalen Kontext: Denn selbst dann, wenn diese nur in Mitgliedsstaaten der EU tätig sind, haben sie mit verschiedenen, zum großen Teil zudem höchst unterschiedlichen nationalen datenschutzrechtlichen Vorgaben zu diesem Thema zu tun, was dem Gedanken des freien Warenverkehrs massiv widerspricht.

Dr. Anselm Brandi-Dohrn
Vorsitzender der DGRI e.V.

Dr. Eugen Ehmann
Fachausschuss Datenschutz

Dr. Robert Selk
Fachausschuss Datenschutz