DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Stellungnahme der DGRI e.V. zur Überarbeitung der Europäischen Datenschutz-Richtlinie

I. Einleitung

Schon im Jahr 2009 hatte die *Europäische Kommission* mit intensiven Vorarbeiten für eine Revision der EG-Datenschutzrichtlinie begonnen. Teil dieser Vorarbeiten war eine „Konsultation zum Rechtsrahmen für das Grundrecht auf Schutz personenbezogener Daten". Dabei war es für alle interessierten Unionsbürger, Organisationen (Unternehmen wie Verbände) und Behörden möglich, im Zeitraum vom 9.7.–31.12.2009 Beiträge mit ihren Vorstellungen zur Fortentwicklung der EG-Datenschutzrichtlinie einzureichen. Drei Leitfragen standen im Mittelpunkt der Konsultation:

1. Welches sind aus Ihrer Sicht die Herausforderungen für den Datenschutz, besonders im Hinblick auf neue Technologien und Globalisierung?
2. Reichen die bestehenden rechtlichen Rahmenbedingungen für diese Herausforderungen aus?
3. Welche Maßnahmen wären sinnvoll, um den Anforderungen gerecht zu werden?

In Deutschland wurde dieser Konsultationsprozess nur recht wenig beachtet. Zum einen waren die drei Leitfragen sehr allgemein, um nicht zu sagen: zu allgemein formuliert. Vor allem aber waren die Aufmerksamkeit und die Kräfte der deutschen Datenschutzszene zu sehr durch die drei grundlegenden Novellen des Bundesdatenschutzgesetzes gebunden. Es verwundert daher nicht, dass aus Deutschland nur sehr wenige und nahezu durchweg äußerst allgemeine Stellungnahmen abgegeben wurden.[1]

Auf die geschilderte besondere Situation in Deutschland konnte die *Europäische Kommission* keine Rücksicht nehmen. Nach Ablauf der Frist für die Konsultation am 31.12.2009 nahm sie zunächst keine weiteren Stellungnahmen an. Dies führte dazu, dass auch eine Stellungnahme der DGRI einstweilen unterblieben war. Am 1.7.2010 fand in Brüssel eine ganztägige „Targeted Private Stakeholders Consultation" statt, bei der die *Europäische Kommission* ihre Vorstellungen dazu darlegte, wie der weitere Gang der Arbeiten zur Revision der EG-Datenschutzrichtlinie ablaufen soll.

Im Kontext dieser Veranstaltung ist die nachstehend abgedruckte Stellungnahme entstanden. Da aus organisatorischen und logistischen Gründen bei Weitem nicht alle Interessenten an der Veranstaltung teilnehmen konnten (die Teilnehmerzahl wurde seitens der *Europäischen Kommission* stark begrenzt), bot die *Europäische Kommission* nochmals die Möglichkeit, in einem engen Zeitfenster von zwei Wochen auch schriftliche Beiträge einzureichen. Diese Chance hat die DGRI über ihren Fachausschuss Datenschutz genutzt.

Zunächst hieß es, dass die *Europäische Kommission* schon im Herbst 2010 einen Entwurf für eine grundlegende Überarbeitung der EG-Datenschutzrichtlinie vorlegen werde. Einer Meldung der französischen Datenschutzbehörde (CNIL) vom 2.8.2010 ist aber zu entnehmen, dass offensichtlich Datenschutzbehörden verschiedener Länder gegenüber der *Europäischen Kommission* äußerten, die Überarbeitung nicht zu überstürzen, und mehr Zeit gefordert haben. Insofern soll es im Herbst 2010 lediglich noch einen Zwischenbescheid geben und erst in der zweiten Hälfte des Jahres 2011 einen überarbeiteten Entwurf. Dieses Thema dürfte daher die Datenschutzdiskussion noch die nächsten Jahre bis weit in das Jahr 2011 entscheidend prägen.

Die Stellungnahme des Fachausschusses Datenschutz der DGRI beschränkt sich bewusst auf wenige zentrale Punkte. Die von der *Europäischen Kommission* zur Diskussion gestellten insgesamt 60 Fragen[2] waren vor der schon erwähnten Veranstaltung am 1.7.2010 als eine Art Diskussionsleitfaden verbreitet worden. Im Interesse besserer Verständlichkeit werden die für die DGRI Stellungnahme ausgewählten Fragen jeweils zunächst inhaltlich skizziert (a), bevor der Text der DGRI Stellungnahme wiedergegeben wird (b).

II. Stellungnahme zu ausgewählten Fragen der Europäischen Kommission

Sehr geehrte Damen und Herren,

die *Deutsche Gesellschaft für Recht und Informatik* (DGRI) e.V., vertreten durch ihren Fachausschuss „Datenschutz", beantwortet ausgewählte Fragen bezüglich der Überarbeitung der Europäischen Datenschutzrichtlinie wie folgt:

1. Denkbare Ausweitungen des Begriffs der sensitiven Daten

a) Frage Nr. 3

Die Frage richtet sich darauf, ob die bereits vorhandenen Kategorien der „sensitiven Daten" soweit ausgedehnt werden sollen, dass sie auch folgende Bereiche abdecken:

- Biometrische und genetische Daten,
- Daten über die familiäre Abstammung einer Person,

1 Sämtliche eingegangenen Stellungnahmen können unter folgendem Link abgerufen werden: *http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm.*

2 Das Stakeholder's Consultation „Future of data protection" Background Paper der *Europäischen Kommission* ist abrufbar unter: *http://ec.europa.eu/justice_home/news/events/data_protection_regulatory_framework/background_paper_en.pdf.*

- Daten von Minderjährigen,
- Daten finanzieller Natur,
- weitere Daten (mit der Bitte, diese zu benennen).

Für den Fall, dass eine entsprechende Ausdehnung auf diese Bereiche vorgeschlagen würde, sollte dies auch entsprechend begründet werden.

b) Stellungnahme

Der Begriff sollte nicht erweitert werden. Eine Erweiterung könnte die unerwünschte Wirkung 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.

2. Schutz Minderjähriger

a) Frage Nr. 4

Hier wird danach gefragt, ob die personenbezogenen Daten von Minderjährigen besser geschützt werden sollten und falls ja, wie. Aufgeworfen wird in diesem Zusammenhang auch die weitere Frage, ob beim Schutz von Daten Minderjähriger eine einheitliche Altersgrenze von 18 Jahren zugrunde gelegt werden soll (in Übereinstimmung mit Art. 1 der UN-Konvention über die Rechte des Kindes).

b) Stellungnahme

Eine grundsätzliche Grenze betreffend der Verarbeitung von personenbezogenen Daten von Minderjähriger auf 18 Jahre wird nicht für sinnvoll erachtet: Denn auch und gerade die Daten von Minderjährigen, also Personen unter 18 Jahre, müssen sowohl im Arbeits-, insbesondere Ausbildungsverhältnis verarbeitet werden, können aber auch im Bereich des Kundendatenschutzes eine wichtige Rolle spielen. Letzteres ist beispielsweise dann der Fall, wenn es um die Werbung von Spielzeug-Produkten (*Playmobil, Lego*, etc.) geht, auch wenn sich diese an die Eltern richtet.

Als wichtig wird aber – gerade im Hinblick auf grenzüberschreitende Werbung – eine Regelung dazu erachtet, welche Voraussetzungen an eine von einem Minderjährigen abgegebene Einwilligungserklärung konkret gestellt werden; insofern kann auch die Einführung eines Mindestalters, ab dem erst eine datenschutzrechtliche Einwilligung erteilt werden kann, begrüßenswert sein, um Rechtssicherheit zu schaffen.

Dies gilt auch hinsichtlich der Frage der Vertretungsfähigkeit der gesetzlichen Vertreter eines Minderjährigen, insbesondere weil nach deutschem Recht die Einwilligung nicht als „normale Willenserklärung", sondern als eine Art höchstpersönliches Recht angesehen wird, für das umstritten ist, ob eine Vertretung überhaupt möglich ist. Denkbar wäre hier, unterhalb der Altersgrenze, ab der ein Minderjähriger selbst einwilligen darf, eine Vertretung zu erlauben.

3. Einführung eines Eigentumsrechts an Daten

a) Frage Nr. 7

Frage 7 richtet sich zum einen darauf, ob es nötig sei, die Einflussmöglichkeiten eines Betroffenen auf den Schutz seiner personenbezogenen Daten zu stärken. Zum anderen wird danach gefragt, ob die vorhandene Datenschutzgesetzgebung dadurch verbessert werden könne, dass ein „Eigentumsrecht" an den personenbezogenen Daten Betroffener eingeführt wird („Dateneigentum").

b) Stellungnahme

Ein solches Eigentumsrecht an den eigenen Daten könnte den Datenschutz eher schwächen. Der Druck auf das Individuum, über seine eigenen Daten gegen Geld zu verfügen, könnte dadurch wachsen. Es schützt das Individuum, wenn es über die eigenen Daten nicht in jeder Situation selbst bestimmen kann. Es würde zudem dem Recht auf informationelle Selbstbestimmung widersprechen, „mit einer Person untrennbar verknüpfte" Daten zu verkaufen, was bei einer Eigentümerschaft an personenbezogenen Daten aber eine Folge wäre. Spätestens dann, wenn der Erwerber sein „Daten-Eigentum" weiterveräußern will (was ihm bei einem Eigentumserwerb kaum verboten werden kann), werden die damit verbundenen Probleme sichtbar: Ein Weitergabeverbot würde dem Interesse des Betroffenen entsprechen, aber dem Eigentumsgedanken jeglicher Zivilrechtsordnung widersprechen.

Daten entziehen sich zudem einer zivilrechtlichen Eigentumsklassifizierung. Ebenso wenig wie Eigentum an Menschen möglich ist, kann damit Eigentum an deren personenbezogenen Daten möglich sein.

Es erscheint nicht sachgerecht, über den Datenschutz die jeweiligen nationalen Eigentumsbegriffe zu beeinflussen, auch im Hinblick auf die in den Mitgliedsstaatenverfassungsrechtlich gewährte Eigentumsgarantie.

4. Spezielle Regelungen zum Arbeitnehmer-Datenschutz

a) Frage Nr. 18

Frage Nr. 18 ist in drei Teile untergliedert. Für den Fall, dass Anlass bestehen sollte, bereichsspezifische Regelungen für die Verarbeitung personenbezogener Daten im Arbeitsleben zu schaffen, wird gefragt:

aa. Welche Themenbereiche sollen näher geregelt werden?

bb. Rolle der ausdrücklichen Einwilligung des Betroffenen: Erscheint sie als eine geeignete Rechtsgrundlage für die rechtmäßige Verarbeitung personenbezogener Daten im Arbeitsleben, auch im Hinblick auf das Ungleichgewicht zwischen Arbeitgeber und Arbeitnehmer?

cc. Bedarf es einer besonderen Regelung für die Verarbeitung spezifischer Daten wie z. B. biometrischer Daten, Daten aus Drogen- und Alkoholtests, Daten aus der Nutzung von Internet und E-Mail sowie Daten aus der Überwachung von Arbeitnehmern?

b) Stellungnahme

aa) Allgemein:

Aufgrund der grenzüberschreitenden Tätigkeit vieler EU-Unternehmen innerhalb der Grenzen der EU besteht in der Praxis großer Bedarf an möglichst einheitlichen datenschutzrechtlichen Vorgaben zum Umgang mit Arbeitnehmer-Daten. Die bisherige Privilegierung nach Art. 4 der EG-Datenschutz-Richtlinie im Sinne eines Sitzland-Prinzips bietet insofern nur in wenigen Fällen Hilfe, da diese nicht mehr greift, wenn im anderen Land eine Niederlassung besteht.

bb) Zu lit. aa.

Sehr wichtig wären Regelungen zur Übermittlung von Arbeitnehmer-Daten zwischen Konzerngesellschaften innerhalb der Grenzen der EU. Es ist ein typischer Fall, dass in einem Konzern etwa die Personalabteilung in der Holding oder zumindest einem einzigen Unternehmen konzentriert ist, oft auch dergestalt, dass die Personalabteilung nicht nur als Auftragsdatenverarbeiter, sondern im Rahmen einer Funktionsübertragung tätig ist. Der Datenfluss von und zu dem Unternehmen, bei dem die Personalabteilung sitzt, ist bisher stark reglementiert und oft nicht oder nur schwer möglich. Dies entspricht nicht den wirtschaftlichen Realitäten und stellt einen im internationalen Vergleich spürbaren Wettbewerbsnachteil dar. Es widerspricht auch der Idee des freien Datenverkehrs zumindest innerhalb der Grenzen der EU.

cc) Zu lit. bb.

Für bestimmte Fälle ist die Abgabe einer Einwilligung durch Arbeitnehmer nicht nur sachgerecht, sondern auch nötig. Gleichzeitig besteht gerade bei der Frage der Wirksamkeit einer Einwilligung im Arbeitsverhältnis sehr große Rechtsunsicherheit, da von den Arbeitsgerichten in Deutschland entweder einseitig oder zu pauschal die Freiwilligkeit der Einwilligung verneint wird. Trotz im Einzelnen zutreffender Bedenken in diese Richtung muss es aber – dem Grundrecht auf informationelle Selbstbestimmung entsprechend – möglich sein, dass auch ein Arbeitnehmer das Recht hat, über die Verwendung seiner Daten selbst zu bestimmen.

Regelungen dazu, in welchen Fällen eine Einwilligung im Arbeitsverhältnis jedenfalls möglich ist, wären daher begrüßenswert.

dd) Zu lit. cc.

Mindestregelungen zum Umfang besonderer Überwachungsdaten sind sinnvoll, um den grenzüberschreitenden Datentransfer innerhalb eines Konzerns bzw. einer Unternehmensgruppe rechtssicher regeln zu können. Gleichzeitig werden Mindestvorgaben als ausreichend erachtet, um den nationalen Staaten ausreichend Spielraum im Hinblick auf die jeweiligen arbeitsrechtlichen Vorgaben zu belassen.

Aus praktischen Gründen gilt dies insbesondere für die Nutzung von TK-Mitteln, insbesondere E-Mail und Internet, im Unternehmen.

5. Zum freien Datenverkehr

a) Frage Nr. 28

Frage Nr. 28 zielt darauf, ob eine Notwendigkeit gesehen wird, die Rechtsregeln für den Datenschutz auf EU-Ebene weitergehend als bisher zu harmonisieren. Ferner wird gefragt, ob es in diesem Zusammenhang Probleme in der Praxis gibt, die den freien Datenverkehr berühren.

b) Stellungnahme

Große praktische Probleme können derzeit – insbesondere betreffend Arbeitnehmerdaten (siehe oben zu Frage Nr. 18), da kaum mit Einwilligungen gearbeitet werden kann – bei Datenflüssen innerhalb einer Unternehmensgruppe / eines Konzerns bestehen.

Dies erscheint in vielen Fällen willkürlich und ungerechtfertigt, gerade weil es eine eher zufällige Entscheidung ist, eine Niederlassung als eigene GmbH (dann: Besonderheiten des Konzerns beachten) zu führen und nicht nur als (unselbstständige) Zweigniederlassung (dann: ein einheitlicher Betrieb). Häufig führen ausschließlich steuerliche Gründe zur Aufteilung eines Unternehmens in z. B. eine Holding mit mehreren Töchtern. Eine Behinderung des Datenverkehrs zwischen den Firmen ist dann nicht nachvollziehbar, gerade wenn das Personal innerhalb des Unternehmens / der neuen Unternehmensgruppeidentisch bleibt.

6. Abstimmung nationaler Genehmigungsprozeduren

a) Frage Nr. 54

Hier wird danach gefragt, ob es ein einheitliches Genehmigungsverfahren für Verträge oder verbindliche Unternehmensregelungen geben solle, die auf grenzüberschreitende Datenübermittlungen Anwendung finden. Dem Kontext nach bezieht sich diese Frage nur auf Datenübermittlungen in Drittstaaten.

b) Stellungnahme

Es wird immer wieder beklagt, dass Genehmigungsverfahren in verschiedenen Mitgliedsstaaten parallel durchlaufen werden müssen. Erwogen werden sollte folgende Lösung:

Sofern eine Genehmigung in einem Mitgliedsstaat erteilt wird, sollte sie auch in allen anderen Mitgliedsstaaten gelten. Da die Aufsichtsbehörden gemäß der Datenschutzrichtlinie verpflichtet sind, eng zusammenzuarbeiten, sollte dies kein Problem darstellen.

7. Daten juristischer Personen

a) Frage

Dieser Aspekt wurde im Fragenkatalog nicht gesondert erwähnt, sollte aber bei einer Überarbeitung der Datenschutzrichtlinie noch einmal überdacht werden.

b) Stellungnahme

Im Augenblick überlässt es die Richtlinie den Mitgliedsstaaten, in welchem Umfang sie Daten juristischer Personen in die Datenschutzbestimmungen einbeziehen wollen. In Deutschland ist dies vom Gesetzeswortlaut her nicht der Fall, in Österreich beispielsweise dagegen durchaus. Auch ist auf die Rechtsprechung des Bundesgerichtshofs zu verweisen, wonach Daten von Personengesellschaften, aber auch von „Ein-Mann-GmbH's" häufig als personenbezogene Daten des/der Gesellschafter(s)/ Geschäftsführers gelten. Die Folge ist, dass man einem Datenbestand mit „Business-Daten" nicht ansehen kann, ob personenbezogene Daten in diesem Sinn darin enthalten sind.

Innerhalb der gesamten Gemeinschaft sollten insoweit einheitliche Maßstäbe gelten.

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

Dr. Eugen Ehmann
Vorsitzender FA Datenschutz
DGRI e.V.

Dr. Robert Selk
Vorsitzender FA Datenschutz
DGRI e.V.