

20g Meltzian
VII4 - 15. Ser - 2 62
Lis 21.2.

Glaser, Anika

Von: Sylke Eich [seich@boetticher.com]
Gesendet: Montag, 20. Februar 2012 16:54
An: PGDS; VII4
Cc: Dr. Anselm Brandi-Dohrn
Betreff: DGRI: Stellungnahme an BMI zum Entwurf einer EU-Datenschutz-VO
Anlagen: 120220 Stellungnahme DGRI (final).doc; Stellungnahme DGRI DatenschutzVO (final).doc



Deutsche Gesellschaft für
Recht und Informatik e.V.

Sehr geehrte Damen und Herren,
sehr geehrter Herr Dr. Meltzian,

in der Anlage finden Sie bitte die heutige Stellungnahme der DGRI e. V. nebst Anlage zu den Vorschlägen der EU-Kommission.

Mit freundlichen Grüßen

--

Sylke Eich

Büro Dr. Anselm Brandi-Dohrn

von Boetticher Hasse Lohmann - Partnerschaft von Rechtsanwälten

Oranienstraße 164, 10969 Berlin

Tel.: +49-30-61 68 94 09, Fax: +49-30-61 68 94 56

Vertrauliche E-Mail von/Confidential or privileged e-mail from

Sitz/Domicile: München, Amtsgericht München, PR 516

Liste der Partner/list of partners: <http://www.boetticher.com>



Deutsche Gesellschaft für
Recht und Informatik e.V.

DGRI e. V. • Emmy-Noether-Str. 17 • D-76131 Karlsruhe

Bundesministerium des Innern
Referat V II 4 - Datenschutzrecht

Per e_mail: PGDS@bmi.bund.de; VII4@bmi.bund.de

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

Telefon: +49-30-61 88 94 09
Telefax: +49-30-61 88 94 56
E-Mail: abrandi-dohrn@boettlicher.com

Berlin, 21. Februar 2012

Verordnung - KOM (2012) 11 - zur Ablösung der bisherigen EG-Datenschutzrichtlinie 95/46/EG
Richtlinie - KOM(2012) 10 - zur Ablösung des bisherigen Rahmenbeschlusses 2008/977/JI

Hier: Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI)

Sehr geehrte Damen und Herren,

Die Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) ist eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen im Bereich des IT-Rechts. Zu ihren Mitgliedern zählen Richter, Rechtsanwälte, Rechtswissenschaftler, Firmenjuristen der IT-Branche und IT-Techniker. Sie befasst sich mit Fragen im Bereich der Schnittstelle zwischen Informatik- und EDV-Recht einerseits sowie Recht und Wirtschaft andererseits. Sie fördert die Zusammenarbeit von Lehre, Forschung, Gesetzgebung und Praxis in allen Fragen der Informationstechnik. Sie begleitet Gesetzgebungsvorhaben als neutrale Institution und ist nicht den Partikularinteressen einzelner Unternehmen oder Branchen verpflichtet.

Die DGRI befasst sich – insbesondere über ihren Fachausschuss Datenschutz – seit vielen Jahren mit allen Fragen des Datenschutzes. Im Verlauf der vergangenen Jahre hat die DGRI ein wachsendes Unbehagen sowohl im Bereich der Wissenschaft, wie auf Seiten der Privatwirtschaft und auf Verbraucherseite festgestellt, dass die Regelungen zum Schutz persönlicher Daten im Verhältnis zwischen Privaten überaus kompliziert und auch für Fachleute kaum mehr handhabbar sind – um so weniger für die eigentlich Betroffenen, die privaten Verbraucher.

Die DGRI begrüßt das Bestreben der Kommission, das national sehr unterschiedliche Datenschutzrecht durch eine Verordnung europaweit zu vereinheitlichen und dadurch Unsicherheiten über die jeweils anwendbaren Regelungen erheblich zu reduzieren. Die DGRI regt jedoch an, bei der Neugestaltung des Datenschutzes in Europa die Gelegenheit zu nutzen, das Schutzkonzept einer grundsätzlichen Revision zu unterziehen. Die DGRI hat in diesem Zusammenhang schon gegenüber der EU-Kommission – durch die Stellungnahme vom 21.12.2011 – die Ergebnisse ihrer Diskussionen im Mitgliederkreis in thesenartiger Form vorgestellt, die wir in der Anlage beifügen.

Deutsche Gesellschaft für Recht und Informatik (DGRI) e.V.	Vorstand: Dr. Anselm Brandi-Dohrn (1. Vors.)
Geschäftsstelle: RA Prof. Dr. Rupert Vogel (Geschäftsführer)	Prof. Dr. A. Wiebe, Dr. Helmut Redeker (stellv. Vors.)
Emmy-Noether-Str. 17 • 76131 Karlsruhe	Bankverbindung: Sparkasse Karlsruhe
Tel.: (0721) 782027-29 • Fax: (0721) 782027-27	Konto-Nr.: 22 404 743 • (BLZ: 680 501 01)
E-Mail: kontakt@dgri.de • Internet: www.dgri.de	IBAN: DE2768050101 0022404743

Ergänzend weist die DGRI – wegen der Kürze der zur Verfügung stehenden Zeit nur gerafft – auf einige ausgewählte Aspekte des neuen Verordnungsentwurfs hin, die bei einer Überarbeitung Berücksichtigung finden sollten, wenn das Ziel einer grundsätzlichen Neukonzeption in diesem Stadium nicht mehr erreichbar sein sollte:

1. Zu Art. 2 des Entwurfs (Sachlicher Geltungsbereich): verfehlte Ausdehnung des Geltungsbereichs auch auf Behörden und öffentliche Einrichtungen

a) Regelungsvorschlag:

Art. 2 sollte um folgenden Absatz 4 ergänzt werden: *"Diese Verordnung findet keine Anwendung auf Behörden und öffentliche Einrichtungen"*.

b) Begründung:

Es ist zu begrüßen, dass durch das Regelungsinstrument einer Verordnung eine unionsweite Vereinheitlichung des Datenschutzes im Bereich der Wirtschaft erreicht werden soll. Dies kann den grenzüberschreitenden Wirtschaftsverkehr bedeutend erleichtern. Die Ausdehnung des Geltungsbereichs der Verordnung auch auf Behörden und öffentliche Einrichtungen ist jedoch in mehrfacher Hinsicht verfehlt:

- Diese Ausdehnung widerspricht der Intention der Verordnung, die ganz wesentlich wirtschaftspolitischer Natur ist und die das Vertrauen von Verbrauchern in Online-Einkäufe und neue Dienste stärken soll (so Ziffer 1 Mitte der Begründung zur Verordnung): Die Einbeziehung von Behörden und öffentlichen Einrichtungen ist ohne jede Relevanz für die Erreichung dieses Ziels.
- Diese Ausdehnung widerspricht dem Subsidiaritätsprinzip (siehe Art. 5 Absatz 3 AEUV) und dürfte deshalb zu entsprechendem Widerstand führen, der die Beratungen der Verordnung erheblich zeitlich verzögern wird. Die im Entwurf (siehe Ziffer 1 der Begründung) herangezogene Rechtsgrundlage des Artikels 16 Abs. 2 AEUV trägt vor dem Hintergrund des Subsidiaritätsprinzips nicht für den Erlass einer Verordnung, die auch den Bereich der Behörden und öffentlichen Einrichtungen einbezieht.
- Diese Ausdehnung würde dazu führen, dass für Daten in Dateien einerseits und Daten in Akten andererseits Regelungen völlig unterschiedlichen Detaillierungsgrades vorhanden wären. Das wäre den Betroffenen nicht zu vermitteln.

Die Verordnung soll den Bereich der Akten nicht erfassen, sondern sich auf den Bereich der Dateien beschränken (siehe Art. 2 Abs. 1). Akten sind jedoch bei Behörden und öffentlichen Einrichtungen auch heute noch von großer Bedeutung – weit mehr als in Wirtschaftsunternehmen.

Der vorgesehene sachliche Anwendungsbereich der Verordnung würde dazu führen, dass die im Bereich der Behörden und öffentlichen Einrichtungen besonders zahlreichen bereichsspezifischen Vorschriften (etwa die Regelungen des Sozialgesetzbuchs!) aufzuheben wären, soweit sie Dateien betreffen. Soweit sie dagegen Akten betreffen, könnten und müssten sie fortbestehen. Detaillierten (und im Wesentlichen bewährten!) nationalen Regelungen für Daten in Akten würden dann bis auf weiteres rudimentäre und pauschale Regelungen für Daten in Dateien gegenüberstehen.

2. Zur Befugnis der Kommission, delegierte Rechtsakte nach Maßgabe des Artikels 86 zu erlassen (In Artt. 1-21 vorgesehen, insbes. in Artikel 6 Abs. 5, Art. 9 Abs. 3 und Art. 20 Abs. 5; siehe auch die strukturell ähnliche Befugnis zur Durchführung von Rechtsakten im Verfahren gemäß Art. 87 Abs. 2, vorgesehen etwa in Art. 8 Abs. 4, Art. 12 Abs. 6, Art. 14 Abs. 8, Art. 15 Abs. 4, Art. 18 Abs. 3)

a) Regelungsvorschlag:

An allen Stellen, an denen eine Befugnis der Kommission zum Erlass delegierte Rechtsakte vorgesehen ist, sollte der Verordnungsentwurf um diejenigen Grundsätze ergänzt werden, die bei dem Erlass des jeweiligen delegierten Rechtsakts zu beachten sind.

b) Begründung:

Der Verordnungsentwurf leidet insgesamt daran, dass er einerseits alle Bereiche des Datenschutzes erfassen und mit unmittelbarer Geltung prägen will, andererseits auf zahlreiche Fragen keine konkreten Antworten enthält. Als Beispiel hierfür kann etwa die fehlende Regelung der Videoüberwachung gelten. Das Ausmaß der Rechtsprechung zu diesem Bereich zeigt, dass er enorme praktische Bedeutung hat und einer speziellen Regelung bedarf.

Diese Defizite lassen sich nicht dadurch ausgleichen, dass die Kommission irgendwann die von Anfang an unmittelbar geltenden Regelungen der Verordnung durch delegierte Rechtsakte entsprechend ergänzt. Dies widerspricht nicht nur dem Wesentlichkeitsgrundsatz des Art. 92 Abs. 1 UA 2 Satz 2 AEUV. Vielmehr wird dies - da der Erlass entsprechender Rechtsakte erheblich Zeit in Anspruch nehmen wird - über längere Zeit zu beträchtlicher Rechtsunsicherheit führen. Das konterkariert auch die wirtschaftspolitische Zielsetzung des Verordnungsentwurfs.

3. Zu Art. 4 Abs. 8 und zu Art. 7 des Entwurfs (Einwilligung)

a) Regelungsvorschlag Nr. 1:

Es sollte festgelegt werden, unter welchen Voraussetzungen vor allem im Online-Bereich konkludente Handlungen als "explizite Willensbekundung" im Sinn von Art. 4 Abs. 8 des Entwurfs anzusehen sind.

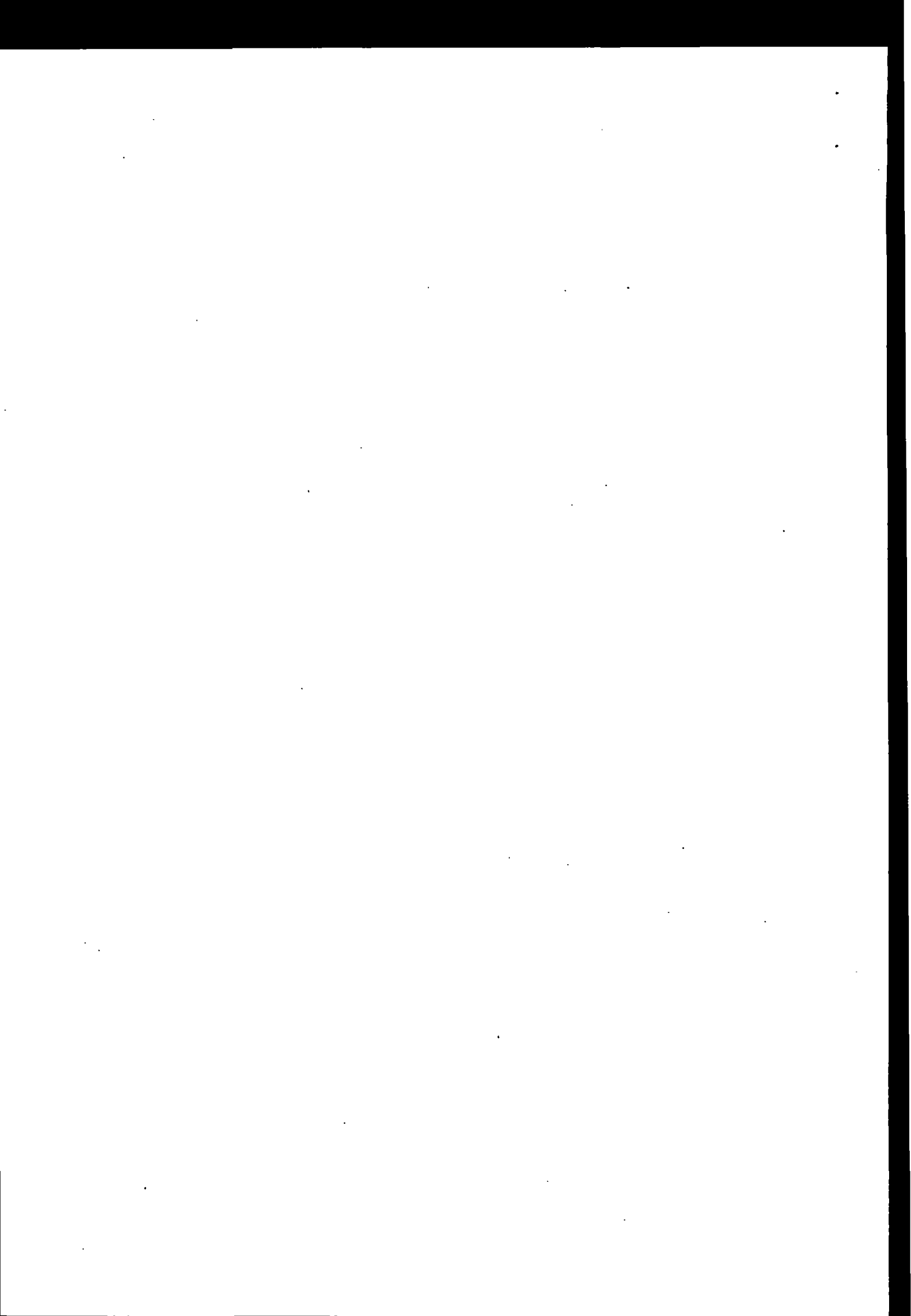
b) Begründung:

Die jetzt vorgesehene Notwendigkeit einer "expliziten Willensbekundung" im Rahmen einer Einwilligung hat ohne Zweifel den Vorzug großer Klarheit. Andererseits liegt in dieser Einschränkung eine erhebliche Erschwernis für das Einholen einer Einwilligung gerade im Online-Bereich. Wenn etwa auf die Kostenpflichtigkeit eines bestimmten Dienstes klar und eindeutig hingewiesen worden ist, dann muss es als Einwilligung gelten, wenn dieser Dienst in Anspruch genommen wird. Nach der jetzt vorgesehenen Regelung dürfte das nicht der Fall sein.

c) Regelungsvorschlag Nr.2:

Es sollte definiert werden, wann ein "erhebliches Ungleichgewicht" im Sinn von Art. 7 Abs. 4 vorliegt, das dazu führt, dass eine Einwilligung keine Rechtsgrundlage für eine Verarbeitung darstellen kann; zudem / zumindest sollte definiert werden, auf was sich das „erhebliche Ungleichgewicht“ beziehen muss.

Ferner sollte festgelegt werden, dass im Rahmen der Durchführung eines Beschäftigungsverhältnisses (nicht bei seiner Begründung) Einwilligungen wirksam erteilt werden können.



d) Begründung:

- Der jetzt vorliegende Regelungsvorschlag vermeidet im Gegensatz zu dem in Entwurf Nummer 56 (englische Version) noch enthaltenen Vorschlag jeglichen Bezug auf Beschäftigungsverhältnisse. Dennoch wird die Regelung in erster Linie auf Beschäftigungsverhältnisse bezogen werden.

Die Praxis zeigt, dass bei der Durchführung von Beschäftigungsverhältnissen die Nutzung von Einwilligungen teils unabdingbar ist. Das gilt für völlig alltägliche Situationen, die den Beschäftigten nicht unzumutbar belasten. Ein Beispiel bildet etwa das Einholen einer Einwilligung dazu, dass das eigene Bild auf die Homepage des Unternehmens gestellt wird (siehe dazu § 22 Kunsturheberrechtsgesetz). Die jetzige Fassung des Entwurfs würde dazu führen, dass solche Einwilligungen nicht mehr eingeholt werden können. Dies hätte die Folge, dass es Fotos von Mitarbeitern auf Unternehmens-Homepages nicht mehr geben dürfte, weil das geltende nationale Recht dies zwingend nur auf der Basis einer Einwilligung zulässt.

- Aber auch im privatwirtschaftlichen Bereich bei Kundenbeziehungen würde die derzeitige Regelung zu erheblichen Unsicherheiten führen:

Denn in vielen Kundenbeziehungen haben die Kunden, gerade Verbraucher, gegenüber dem Daten verarbeitenden Unternehmen keine Möglichkeit, in Vertragsverhandlungen die vertraglichen Bestimmungen im Detail auszuverhandeln. Dies ist oft auch weder gewollt noch wäre es – gerade im Massengeschäft des Internetgeschäfts – sinnvoll, entspricht in vielen Fällen vielmehr dem normalen und akzeptierten Wirtschaftsleben. Nach der jetzigen Formulierung des Entwurfs müsste aber wohl davon ausgegangen werden, dass zumindest was die Möglichkeit der ernsthaften Vertragsverhandlung angeht, in all diesen Fällen ein „wesentliches Ungleichgewicht“ vorliegt. Damit liefe der Verordnungsentwurf Gefahr, zur Unwirksamkeit von Einwilligungen in der überwiegenden Anzahl von Rechtsgeschäften des täglichen Lebens zu führen bzw. deren Wirksamkeit zumindest fraglich werden zu lassen (was aus Sicht des Wirtschaftsverkehrs ebenso inakzeptabel wäre).

Da jede Einwilligung ohnehin freiwillig erteilt werden muss, hat ein Kunde jedenfalls die Möglichkeit, seine Einwilligung explizit zu verweigern. Es stellt sich daher die Frage, ob neben dem (bewährten) Kriterium der Freiwilligkeit ein weiteres Kriterium nötig ist, das zudem mit einem unbestimmten Rechtsbegriff arbeitet.

Da im Entwurf die Rolle der Einwilligung (sinnvollerweise) gestärkt wird, sollte darauf geachtet werden, deren Erteilung möglichst einfach und (rechts-) sicher zu gestalten.

4. Zu Art. 15 des Entwurfs (Auskunftsrecht)

a) Regelungsvorschlag Nr. 1:

Die Regelung sollte um eine Ausnahme für den Fall ergänzt werden, dass Betriebs- und Geschäftsgeheimnisse geschützt werden müssen.

b) Begründung:

Die Regelung sollte einem Unternehmen nicht ermöglichen, unter Rückgriff auf die Verordnung Informationen über Konkurrenzunternehmen gewinnen zu können.

c) Regelungsvorschlag Nr.2:

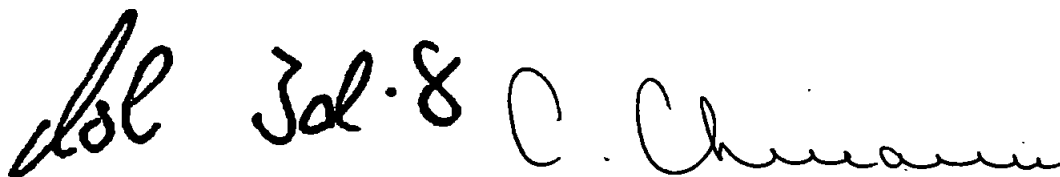
Die Regelung sollte um eine Sondervorschrift für Auskünfte über Score-Werte ergänzt werden.

d) Begründung:

Score-Werte sind in der Kreditwirtschaft, aber auch bei Mobilfunkanbietern und anderen Unternehmen von größter praktischer Bedeutung. Es führt daher zu vermeidbarer Rechtsunsicherheit, wenn Art. 15 nichts konkret dazu sagt, unter welchen Voraussetzungen eine Auskunft über Score-Werte gefordert werden kann.

Die ergänzende Rechtssetzungsbefugnis der Kommission in Abs. 4 der Vorschrift ist nicht ausreichend: Zum einen bestehen Zweifel, ob die Bestimmung zu einer solch speziellen Regelung ermächtigt. Zum anderen ist Abs. 4 nicht zu entnehmen, welche Grundsätze insoweit zu berücksichtigen wären.

Für Rückfragen und Ergänzungen steht Ihnen die DGRI gerne zur Verfügung.



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

Dr. Eugen Ehmann
Co-Leiter Fachausschuss Datenschutz

Dr. Robert Selk
Co-Leiter Fachausschuss Datenschutz
(an der Unterschrift gehindert)

Anlage



Deutsche Gesellschaft für
Recht und Informatik e.V.

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

Europäische Kommission
- GD Justiz, Grundrechte und Bürgerschaft –
Direktion C: Grundrechte und Unionsbürgerschaft
Herrn Direktor Dr. Paul Nemitz

B-1049 Brüssel

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

Per e_mail vorab: paul.nemitz@ec.europa.eu

Berlin, 21. Februar 2012

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation**)

Hier: Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI)

(Register-Nr. 21625424990-18 des Registers der Interessenvertreter der Europ. Kommission)

Sehr geehrter Herr Direktor Dr. Nemitz,
sehr geehrte Damen und Herren,

Die Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) ist eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen im Bereich des IT-Rechts; zu ihren Mitgliedern zählen Richter, Rechtsanwälte, Rechtswissenschaftler, Firmenjuristen der IT-Branche und IT-Techniker. Sie befasst sich mit Fragen im Bereich der Schnittstelle zwischen Informatik- und EDV-Recht einerseits sowie Recht und Wirtschaft andererseits. Sie fördert die Zusammenarbeit von Lehre, Forschung, Gesetzgebung und Praxis in allen Fragen der Informationstechnik. Sie begleitet Gesetzgebungsvorhaben als neutrale Institution und ist nicht den Partikularinteressen einzelner Unternehmen oder Branchen verpflichtet.

Die DGRI befasst sich – insbesondere über ihren Fachausschuss Datenschutz – seit vielen Jahren mit allen Fragen des Datenschutzes. Im Verlauf der vergangenen Jahre hat die DGRI ein wachsendes Unbehagen sowohl im Bereich der Wissenschaft, wie auf Seiten der Privatwirtschaft und auf Verbraucherseite festgestellt, dass die Regelungen zum Schutz persönlicher Daten im Verhältnis zwischen Privaten überaus kompliziert und auch für Fachleute kaum mehr handhabbar sind – um so weniger für die eigentlich Betroffenen, die privaten Verbraucher.

Deutsche Gesellschaft für Recht und Informatik (DGRI) e.V.	Vorstand: Dr. Anselm Brandi-Dohrn (1. Vors.)
Geschäftsstelle: RA Prof. Dr. Rupert Vogel (Geschäftsführer)	Prof. Dr. d. Heckmann, Dr. Helmut Redeker (stellv. Vors.)
Emmy-Noether-Straße 17 • 76131 Karlsruhe	Bankverbindung: Sparkasse Karlsruhe
Tel.: (0721) 78 20 27 – 29 • Fax: (0721) 78 20 27 - 27	Konto-Nr.: 22 404 743 • (BLZ: 680 501 01)
E-Mail: kontakt@dgri.de • Internet: www.dgri.de	IBAN: DE2768050101 0022404743

Die DGRI begrüßt das Bestreben der Kommission, das national sehr unterschiedliche Datenschutzrecht durch eine Verordnung europaweit zu vereinheitlichen und dadurch Unsicherheiten über die jeweils anwendbaren Regelungen erheblich zu reduzieren. Die DGRI hat auch die Vorschläge des *Deutschen Anwaltsvereins (DAV)*, der Vertretung der deutschen Anwaltschaft, die anregt, das Konzept des Datenschutzes zwischen Privaten einer grundsätzlichen Überprüfung zu unterziehen, im Kreis ihrer Mitglieder eingehend diskutiert.

Im Ergebnis dieser Diskussion schließt sich die DGRI den Vorschlägen des DAV – mit Anpassungen im Einzelnen – in vollem Umfang an. Dabei ist darauf hinzuweisen, dass die interne Diskussion natürlich noch andauert, weshalb wir in späteren Stadien der Normsetzung sicher erneut Stellung nehmen werden.

Die DGRI regt an, bei der Neugestaltung des Datenschutzes in Europa die Gelegenheit zu nutzen, um das Schutzkonzept einer Revision zu unterziehen. Dabei sind nachfolgende Grundsätze zu beachten, um so dem Datenschutz zu größerer Akzeptanz und Effektivität zu verhelfen:

1. Datenverarbeitung im Netz ist in den meisten Mitgliedstaaten eine Ausübung verfassungsrechtlich garantierter Grundfreiheiten. Daher bedarf es eines Ausgleichs zwischen Persönlichkeitsrechten und Kommunikationsfreiheiten. Neue Konfliktstrukturen erfordern neue Regelungen im nicht-öffentlichen Bereich. Dabei haben weder Persönlichkeitsrechte noch Kommunikationsfreiheiten einen natürlichen Vorrang. Das „Medienprivileg“ braucht mehr Konturschärfe. Deshalb ist wichtig, dass der VO-Entwurf, etwa in 3.3 der Einleitung sowie in Erwägungsgrund 46, 103 und 118 auch Art. 11 der Charta teils ausdrücklich, teils der Sache nach erwähnt. Allerdings erscheint (trotz der indirekten Einbeziehung in Art. 1 (1) der VO) die unmittelbare Berücksichtigung - in Form der Gegenüberstellung des Rechts aus Art. 11 der Charta und seiner Abwägung mit dem Recht auf „privacy“ - zu fehlen. Der Katalog des Art. 5 erscheint deshalb zu eng.
2. Daten sind ein Abbild sozialer Realität. Sie sind kein Schutzgut, das dem Einzelnen – eigentumsähnlich – zugeordnet ist. Folglich kann es im Datenschutzrecht nicht primär um den Schutz von Daten gehen. Es geht primär vielmehr um den Schutz von Persönlichkeitsrechten vor Beeinträchtigungen durch eine ungezügelter Verbreitung von Informationen. Der Bezug zum Persönlichkeitsrecht, das es zu wahren gilt, sollte daher in Art. 4 als Prinzip vorgeschaltet werden. „Privacy by design“ und „Privacy by default“ – sehr begrüßenswerte Einrichtungen – hängen logisch „in der Luft“, wenn sie nicht zum Zwecke der konkreten Durchsetzbarkeit, etwa auch in Gerichtsprozessen, auf einem materiellen Schutzgut, nämlich „privacy“ aufbauen. Einen wichtigen Schritt in diese Richtung stellt die stärkere Fokussierung auf die „Person“ (*data subject*) dar. Dieser Ansatz sollte noch ausgebaut werden.
3. Die Anwendbarkeit des gesamten Datenschutzrechts steht und fällt derzeit mit der Personenbezogenheit von Daten. Sind Daten personenbezogen, gilt das strenge Regime des Datenschutzrechts. Fehlt es am Personenbezug, sind Daten „vogelfrei“. Dieses „Schwarz-Weiß-Schema“ kann nicht richtig sein. Der Schutz von Persönlichkeitsrechten kann nicht davon abhängen, wie der Rechtsanwender den Begriff des „Personenbezugs“ versteht. Das Datenschutzrecht sollte einen weiten Anwendungsbereich haben und für alle Informationen gelten, die Persönlichkeitsrechte beeinträchtigen können. Insofern wird Art. 3 (2) der VO als Fortschritt begrüßt.
4. Nach derzeitigem Recht bedeutet das Verbotprinzip, dass Kommunikation grundsätzlich verboten ist, wenn personenbezogene Daten verwendet werden. Dies schränkt die Kommunikationsfreiheit in bedenklicher Weise ein. Das Verbotprinzip bedarf schon aus diesem Grund einer deutlichen Einschränkung und Verlagerung auf Kernbereiche des Persönlichkeitsrechts. Dies gilt umso mehr, wenn man von einem weiten Anwendungsbereich des Datenschutzrechts ausgeht. Die Grenzziehung zwischen zulässiger und unzulässiger Datenverarbeitung darf nicht einer uferlosen Abwägung mit vagen Begriffen und unvorhersehbaren Abwägungsergebnissen überlassen werden. Dies betrifft Art. 5 der VO, der insofern wesentlich zu weit ist bzw. die normale Informationsverarbeitung bei einvernehmlicher Kommunikation allzu sehr einengt bzw. formalisiert. Das Verbotprinzip mit Vorbehalt der Einwilligung oder Rechtsgrundlage wäre hingegen besonders geeignet für die Datenkategorien und Regelungen des Art. 8.

5. Nicht alle Daten sind gleich. IP-Adressen oder Gerätekennzeichen sind nicht in gleicher Weise zur Beeinträchtigung von Persönlichkeitsrechten geeignet wie Angaben zur Gesundheit oder zu sexuellen Neigungen. Die unendliche Vielzahl und Vielfalt von Informationen in der Informationsgesellschaft des 21. Jahrhunderts fordert eine differenzierte Herangehensweise und abgestufte Regelungen je nachdem ob es um „banale“ oder „sensible“ Informationen geht. Das Datenschutzrecht setzt in vielen Bereichen auf Rechte des Betroffenen gegen den Datenverarbeiter und bleibt auf diese Weise in einem Zwei-Personen-Verhältnis haften, das dem Verhältnis Staat/Bürger nachgebildet ist. Dies greift für den Bereich zwischen Bürgern zu kurz. Es bedarf einer Stärkung des präventiven Persönlichkeitsschutzes durch eine datensparsame Ausgestaltung von Verfahren. Verfahrensregeln können helfen, dass Technik so ausgestaltet wird, dass Persönlichkeitsrechte geschont werden.
6. Das Datenschutzrecht setzt vielfach auf Einwilligungen, die der Betroffene zur Legitimation der Datenverarbeitung erteilen muss. Im Massenverkehr des Internets lassen sich jedoch Einwilligungserfordernisse nur durch standardisierte, vorformulierte Einwilligungserklärungen erfüllen. Als zentrales Instrument zur Sicherung der Autonomie des Betroffenen erweisen sich Einwilligungserfordernisse unter diesen Bedingungen als ungeeignet. Der in Art. 5 (1) (a) in Verbindung mit Art. 7 der VO gewählte Ansatz ist deshalb in der Praxis nicht tragfähig. Daran ändert sich im Ergebnis auch dann nichts, wenn man die weiteren Tatbestände in Art. 5 berücksichtigt, die eine Verarbeitung rechtfertigen können, denn sie decken nur wenige Fallgruppen ab. Richtig wäre etwa, eine Einwilligung (nur) für Fälle vorzusehen, in denen Änderungen des ursprünglichen Zwecks der Verarbeitung erfolgen.
7. Statt die Selbstbestimmung vermeintlich durch vorformulierte Einwilligungserklärungen zu fördern, sollte das Datenschutzrecht verstärkt auf Transparenz setzen. Wie in vielen anderen Rechtsbereichen auch bedarf es präziser, verständlicher und leicht abrufbarer Informationen über den Umgang mit Informationen. Derartige Informationen lassen sich – wie bereits in der Praxis üblich – in Datenschutzerklärungen oder Datenschutzbestimmungen zusammenfassen. Das Datenschutzrecht sollte konkrete Anforderungen stellen an den Inhalt, die Gestaltung, die Auffindbarkeit und die Formulierung von Datenschutzbestimmungen. Im Hinblick auf die notwendige Verstärkung des Transparenzgedankens sind die Art. 9 ff der VO grundsätzlich sehr zu begrüßen. Dies gilt auch für Art. 16.
8. Ein zentraler Schwachpunkt des bestehenden Datenschutzrechts ist das Missverhältnis zwischen der Regelungstiefe und –dichte einerseits und dem Vollzug andererseits. Hier bedarf es der Abhilfe, und zwar vor allem durch erweiterte und verschärfte Haftungsnormen. Insofern erscheint Art. 75 der VO noch zu schwach. Auch Art. 77 erscheint nicht ausreichend. Es sollte zum einen klargestellt werden, dass bei Eingriffen in das Persönlichkeitsrecht auch der immaterielle Schaden zu ersetzen ist, zum anderen dafür eine Mindestpauschale (und insoweit auch eine Obergrenze) vorgesehen werden, da der Nachweis des Schadens oft sehr schwierig ist.
9. Das Datenschutzrecht ist über die Jahre ausgeufert und findet sich in einer Vielzahl verstreuter Regelungen. Selbst Experten haben Mühe, den Überblick zu behalten. Daher gilt es, bestehende Regelungen zu vereinfachen, stringent zu formulieren und das Datenschutzrecht insgesamt logisch einleuchtend zu strukturieren. Dem trägt die VO in wichtigen Punkten Rechnung und ist insoweit von großer Bedeutung. Allerdings fehlt eine Regelung, die dem Betroffenen - insbesondere dann, wenn er aktiv an elektronischen Medien, sozialen Netzwerken usw. mitwirkt - den Grad der Belastung seiner „privacy“, sowie das Maß der Transparenz auf einfache Weise und sofort bzw. stets – ähnlich einem Kontostand und/oder Ampel – vermittelt und zwar nicht erst auf Anfrage.

Für Rückfragen und Ergänzungen steht Ihnen die DGRI gerne zur Verfügung.

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

Dr. Eugen Ehmann
Leiter Fachausschuss Datenschutz

