

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. Dezember 2011

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.

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 Verbotsprinzip, dass Kommunikation grundsätzlich verboten ist, wenn personenbezogene Daten verwendet werden. Dies schränkt die Kommunikationsfreiheit in bedenklicher Weise ein. Das Verbotsprinzip 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 Verbotsprinzip 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 Persönlichkeitssschutzes 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 Datenschutzerklärung 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-Dohrn
Vorsitzender der DGRI e.V.

Dr. Eugen Ehmann
Leiter Fachausschuss Datenschutz