Response to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data

by

European Digital Rights initiative

drafted by

Bits of Freedom
together with other members

23 December 2009

Introduction

1. European Digital Rights Initiative ("**EDRi**") welcomes the opportunity to provide input on the European Commission's consultation on the legal framework for the fundamental right to protection of personal data.

2. EDRi concludes that there are considerable challenges to the existing data protection framework. Amongst those challenges are:

   - the ever increasing amount of personal data being collected and processed by governments and private entities;
   - the introduction of obligatory data retention and centralized storage and processing in various contexts;
   - the increasing attempts by governments to share personal data internally and have private entities share personal data with the government, thereby gaining access to personal data for purposes unrelated to those for which the data was collected originally;
   - the growing gap between the rising number of information security threats and the ability of data processors to address these threats;
   - the rapidly advancing data processing and profiling technologies becoming available and being applied to personal data;
   - the considerable inconsistencies in terms of interpretation and application of data protection law between EU Member States; and
   - the systematic shortcomings in terms of enforcement and independent oversight of the existing legal framework in combination with developments mentioned above, both in terms of capacity vis-a-vis the growth in personal data processing and in terms of quality.

3. These developments pose a significant and growing threat to the privacy of each individual taking part in the information society now and in the years to come. EDRi would, in short, recommend that the following measures be taken:

   - Stronger principles ensuring data minimisation should be introduced;
   - Stronger principles ensuring transparency should be introduced;
   - Stronger principles ensuring security of personal data should be introduced;
   - The interpretation of the term "personal data" should be clarified;
   - Administrative oversight and enforcement should be strengthened; and
   - Civil enforcement should be strengthened.

4. These recommendations will be further explained below.

Recommendations

5. The current European legal framework, i.e. primarily the Data Protection Directive 95/46/EC ("**DPD**"), is a first step in the right direction, but by itself does not provide a sufficiently robust framework to address the challenges identified above in the coming years. EDRi thus proposes to review the DPD, but simultaneously wishes to underline that such a review should obviously lead to *more and better* protection of personal data, instead of less.

6. In order to ensure a robust and better functioning data protection framework in the European Union in the coming years, EDRi calls upon the European legislator to restate the importance of the current legal framework and take at least the following measures:

Include stronger principles ensuring data minimisation

A) A revision of the DPD should include stronger principles ensuring the minimisation of the collection and processing of personal data. The criterion that data collected should be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (cf. Art. 6 DPD) has proven to be an inadequate threshold for judging legitimate versus illegitimate collection of personal data. Firstly, this standard should be made more strict, by allowing only the collection of data which is "strictly necesary" for these purposes. Secondly, the "legitimate interest"-test (cf. Art. 7 sub f DPD) under which most of these purposes are evaluated should be interpreted so as to minimise the collection and processing of personal data. Data controllers can now easily broaden the scope of the "purposes" for which the data is collected by including a variety of different purposes in their privacy policies. Whether those purposes are allowed is most often evaluated under the "legitimate interests"-test, the scope of which can be broad and is at any rate not sufficiently clear. It should be made clear that only a very limited set of purposes fall within the scope of this provision.

Including stronger principles ensuring transparency with regard to personal data

A) A revision of the DPD should include stronger principles ensuring transparency with regard to data being collected. Art. 10 and 11 DPD now only prescribe the provision of very limited information to the data subject. It should be clarified that the controller or his representative should be obliged to (i) indicate in an easily accessible and user-friendly way how long they store personal data, (ii) keep logs of each time personal data is being accessed or processed, and (iii) provide data subjects access to the logs pertaining to their own data. Controllers should not be allowed to charge reimbursement of administrative costs related to the exercise of the right of access to data (cf. Art. 12 DPD), as this currently

poses an undue burden to data subjects seeking such access in certain member states. In addition, a controller or his representative should be obliged to use up-to-date technology to enable the data subject to exercise the right to access and correction granted to it under the DPD in the most user-friendly and cost-effective way possible. It should also be ensured that the rights of access and correction not only regard all personal data "directly" related to the data subject, but also regard the identities and general profiles (i.e. not pertaining to one specific person) created on the basis of such personal data.

Principles ensuring security

B) A revision of the DPD should include stronger principles ensuring the security of personal data being collected. Currently, the controller is obliged to "implement appropriate technical and organizational measures" ensuring "a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" (cf. Art. 17 DPD). This in practice provides an insufficiently strict standard, especially in view of the fact that it is impossible to assess the risks related to the nature of personal data in isolation. Instead, a level of security conforming to the highest standards of the art should be applied in all instances where the collection or processing of personal data is involved. In addition, a data breach notification obligation relating to all databases of personal data should be included in the DPD (cf. the limited envisaged data breach notification in Directive 2002/58/EC as amended by Directive 2009/136/EC – the ePrivacy Directive). The introduction of such an obligation is already suggested in recital 59 of Directive 2009/136/EC.

Guidance on interpretation of the term "personal data"

C) A revision of the DPD or other measure giving guidance on the interpretation of the DPD should make clear that the current collection of personal data by online service providers does indeed fall within the scope of the DPD. There has been uncertainty among certain data protection authorities ("**DPAs**") whether IP-addresses should be considered personal data under the DPD. Given the increasing use of IP-addresses as instruments for creating a digital profile of customers by online service providers, this would lead to the undesired conclusion that such data would not fall within the DPD. More generally, as a result of progress in de-anonymisation technology, data which currently may be considered anonymous, could next year be considered personal data. The term "personal data" should consequently be interpreted sufficiently broadly in order to also encompass those situations where data could in the near future become "personal data".

Strengthening administrative oversight and enforcement

D) A revision of the DPD should strengthen administrative oversight and enforcement of the rights and obligations following from the DPD. First of all, the independence of DPAs from government and industry should be explicitly guaranteed in the Directive. The DPD should prescribe that DPAs should have the power to enforce all relevant rights and obligations laid down in the DPD (and not only a selection thereof) with appropriate sanctions. In addition, sanctions which may be imposed by DPAs for infringements should have a sufficiently deterrent effect. An example: the illegal sale of personal data by T-Mobile employees led UK's Justice Minister Michael Wills to call for custodial sentences to prevent the trade in illegal data.[1] Measures should be taken to ensure that DPAs have sufficient resources including staffing and financial resources to perform the tasks assigned to them under the DPD. For significant governmental legislative or technological developments which would involve the collecting and processing of personal data, a privacy impact assessment should be made obligatory, before such developments can go through.

Strengthening civil enforcement

E) In addition to such strengthening of public enforcement, a revision of the DPD should include further incentives allowing for a robust framework of civil enforcement of the rights and obligations following from the DPD, in line with the growing importance and value of personal data. As mentioned above, the possibility of (minimal) reimbursement for controllers who respond to data subjects exercising their rights of access and correction should be abolished. Furthermore, the entitlement of the data subject to compensation from the controller for damage suffered in civil proceedings (cf. Art. 23 DPD), should be strengthened, by inclusion of statutory damages. These should reflect the increasing value of personal data and the increasing damage which can be done by improper collection, processing or disclosure thereof. For example, in the United Kingdom very few claims for compensations have to date been made by individual data subjects. Where actions have been brought, the courts have made it clear that compensation is only available to an individual who suffers damage "by reason of" a data controller's contravention of a Data Protection Act requirement. Where no such “direct” damage can be proven, no compensation will be payable. In addition, the DPD should oblige member states to allow data subjects to start class actions (or “collective redress”) to claim damages, as the individual damages may in some cases be prohibitively small, but the liability which gave rise to the damage is is very similar.

Endorsements

7. In addition, EDRi wishes to endorse the following documents:

[1] See http://news.bbc.co.uk/2/hi/uk_news/8364421.stm.

- Considering the global nature of data protection, EDRil would like to endorse the 'Madrid Privacy Declaration', as recently adopted by a broad coalition of civil society organizations, privacy advocates, experts and individuals (attached as **Annex 1**).[2]

- EDRi would like to further endorse the submission of 10 June 2009 by Patrick Breyer, in the context of this consultation (attached as **Annex 2**).[3]

8. EDRi remains available to further explain the above at your earliest convenience. You can contact EDRi through:

Joe McNamee - Advocacy Coordinator
Tel: +32 2 550 4112
E-Mail: joe.mcnamee@edri.org

* * *

[2] See Civil Society Madrid Privacy Declaration, 3 November 2009, available online at , signed and strongly endorsed by EDRI.
[3] Available online at: http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/citizens/breyer_patrick_de.pdf

Annex 1

The Madrid Privacy Declaration

3 November 2009
Madrid, Spain

Affirming that privacy is a fundamental human right set out in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other human rights instruments and national constitutions;

Reminding the EU member countries of their obligations to enforce the provisions of the 1995 Data Protection Directive and the 2002 Electronic Communications Directive;

Reminding the other OECD member countries of their obligations to uphold the principles set out in the 1980 OECD Privacy Guidelines;

Reminding all countries of their obligations to safeguard the civil rights of their citizens and residents under the provisions of their national constitutions and laws, as well as international human rights law;

Anticipating the entry into force of provisions strengthening the Constitutional rights to privacy and data protection in the European Union;

Noting with alarm the dramatic expansion of secret and unaccountable surveillance, as well as the growing collaboration between governments and vendors of surveillance technology that establish new forms of social control;

Further noting that new strategies to pursue copyright and unlawful content investigations pose substantial threats to communications privacy, intellectual freedom, and due process of law;

Further *noting* the growing consolidation of Internet-based services, and the fact that some corporations are acquiring vast amounts of personal data without independent oversight;

Warning that privacy law and privacy institutions have failed to take full account of new surveillance practices, including behavioral targeting, databases of DNA and other biometric identifiers, the fusion of data between the public and private sectors, and the particular risks to vulnerable groups, including children, migrants, and minorities;

Warning that the failure to safeguard privacy jeopardizes associated freedoms, including freedom of expression, freedom of assembly, freedom of access to information, non-discrimination, and ultimately the stability of constitutional democracies;

Civil Society takes the occasion of the 31st annual meeting of the International Conference of Privacy and Data Protection Commissioners to:

(1) Reaffirm support for a global framework of Fair Information Practices that places obligations on those who collect and process personal information and gives rights to those whose personal information is collected;

(2) Reaffirm support for independent data protection authorities that make determinations, in the context of a legal framework, transparently and without commercial advantage or political influence;

(3) Reaffirm support for genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information and for meaningful Privacy Impact Assessments that require compliance with privacy standards;

(4) Urge countries that have not ratified Council of Europe Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible;

(5) Urge countries that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible;

(6) Urge those countries that have established legal frameworks for privacy protection to ensure effective implementation and enforcement, and to cooperate at the international and regional level;

(7) Urge countries to ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with its collection;

(8) Recommend comprehensive research into the adequacy of techniques that deidentify; data to determine whether in practice such methods safeguard privacy and anonymity;

(9) Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate; and

(10) Call for the establishment of a new international framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions.

(At the time of the annual meeting of the Privacy and Data Protection Commissioners' conference in Madrid, more than 100 civil society organizations and privacy experts had signed the Madrid Privacy Declaration. More information about the Declaration, including translations, is available at **thepublicvoice.org/madrid-declaration)**

Annex 2

Patrick Breyer

VORSCHLÄGE ZUR VERBESSERUNG DES DATENSCHUTZES

I. Verbesserter Datenschutz

1. Einführung eines Rechts auf anonyme Nutzung von Diensten der Informationsgesellschaft

Begründung: Nur im Schutz der Anonymität sind sensible Recherchen und Tätigkeiten im Internet überhaupt möglich (z.B. Recherchen von Journalisten oder Menschen in einer Notlage wie Drogenabhängige).

Werbefinanzierten Anbietern ist eine anonyme Zugangsmöglichkeit nicht unzumutbar, weil sie für diese Zugänge ein (zusätzliches) Entgelt erheben können, welches die entgangenen Einnahmen aus personenbezogener Werbung ausgleicht. Die Abrechnung kann über anonyme vorausbezahlte Guthabenkarten erfolgen (z.B. "paysafecard").

Formulierungsvorschlag: "Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Diensten der Informationsgesellschaft und ihre Bezahlung anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die anonyme Bereitstellung ist zumutbar, wenn Dienste dieser Art am Markt anonym angeboten werden, es sei denn, dass die besonderen Verhältnisse des Diensteanbieters entgegen stehen. Der Nutzer ist über die Möglichkeit der anonymen Inanspruchnahme zu informieren."

(vgl. § 13 Abs. 6 TMG)

2. Einführung eines Rechts darauf, Dienste der Informationsgesellschaft nutzen zu können, ohne dass der Anbieter jeden Klick oder jede Eingabe personenbeziehbar aufzeichnet.

Begründung: Wie oben. Es besteht kein Widerspruch zur Richtlinie zur Vorratsdatenspeicherung, weil diese nur TK-Anbieter betrifft.

Formulierungsvorschlag: "Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur verarbeiten, soweit dies erforderlich ist, um die Inanspruchnahme des Dienstes zu ermöglichen und abzurechnen (Nutzungsdaten)." (vgl. § 15 Abs. 1 TMG)

3. Klarstellung, dass IP-Adressen personenbezogene Daten sind.

Begründung: Unternehmen wie Google behaupten bis heute, das von ihnen aufgezeichnete Nutzerverhalten sei nicht personenbezogen, obwohl zumindest staatliche Behörden die Identität des Nutzers anhand seiner IP-Adresse problemlos in Erfahrung bringen können. Die bestehende Rechtsunsicherheit über den Personenbezug von IP-Adressen beeinträchtigt den Datenschutz im Internet.

Formulierungsvorschlag: "Nutzungsdaten sind insbesondere Merkmale zur Identifikation des Nutzers einschließlich Internet-Protocol-Adressen, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Dienste der Informationsgesellschaft."

4. Information über die Aufbewahrungsdauer personenbezogener Daten.

Begründung: Nur wenn der Betroffene darüber informiert ist, wie lange einzelne Anbieter seine Daten typischerweise aufbewahren, kann er eine wirklich freie Entscheidung darüber treffen, ob und welchen Anbieter einer Leistung er in Anspruch nehmen will. Nur auf diese Weise kann ein Wettbewerb um datensparsame Angebote entstehen. Dass sich die Unterrichtung auch auf "die mögliche Dauer der Datenspeicherung"

erstrecken muss, meint auch die Artikel 29-Datenschutzgruppe (Dokument WP 37 vom 21.11.2000, 65). Ohne Zeitabgabe kann der Nutzer nicht erkennen, ob eine Speicherung einen Monat oder zehn Jahre lang erfolgt.

Formulierungsvorschlag für Artikel 10 RiL 95/46/EG - neu -:

"Die Mitgliedstaaten sehen vor, daß die Person, bei der die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,

b) *Welche Daten wie lange und zu welchen Zwecken verarbeitet werden,*

c) ..." (unverändert)

5. Vorformulierte Einwilligungsklauseln müssen einer Angemessenheitskontrolle unterworfen werden.

Begründung: Besonders Anbieter von Diensten der Informationsgesellschaft nutzen in der Praxis verbreitet das Schlupfloch der elektronischen Einwilligung, um sich den ausgewogenen gesetzlichen Regelungen über die Verarbeitung von Nutzerdaten zu entziehen. Die – meist unklar formulierte und mehrere Seiten lange – Einwilligungserklärung, welcher der Nutzer zustimmen muss, bedingt das Datenschutzrecht gleichsam insgesamt ab, indem sie eine unbefristete und unbeschränkte Erfassung, Nutzung und Weitergabe sämtlicher Daten über die Nutzer erlaubt. Dieser Zustand ist unhaltbar. Die deutschen Gerichte haben bereits entschieden, dass Einwilligungsklauseln einer Angemessenheitskontrolle unterliegen (grundlegend BGH vom 19.09.1985, Az. III ZR 213/83 – Schufaklausel).

Lösungsvorschlag: In die Richtlinie 98/27/EG über unangemessene Klauseln in Verbraucherverträgen müssen vorformulierte Klauseln über die Einwilligung in die Verarbeitung personenbezogener Daten aufgenommen werden. Unwirksam sein müssen Einwilligungsklauseln, wenn sie den von der Datenverarbeitung Betroffenen unangemessen

benachteiligen oder wenn sie mit wesentlichen Grundgedanken einer gesetzlichen Regelung, von der sie abweichen, nicht zu vereinbaren sind.

II. Verbesserte Durchsetzung der geltenden Datenschutzgarantien

1. Einführung eines Verbandsklagerechts für Verbraucher- und Datenschutzverbände, damit sie gegen datenschutzwidrige Praktiken klagen können.

Begründung: Bei von Einzelnen angestrengten Prozessen wegen datenschutzwidriger Praktiken - etwa im Fall Voss ./. T-Online - gibt es immer wieder Finanzierungsschwierigkeiten; außerdem wird das Urteil von der Gegenseite oftmals nur für den jeweiligen Kläger umgesetzt und nicht für alle Kunden.

2. Klarstellung, dass Datenschutzbestimmungen auch dem Schutz eines fairen Wettbewerbs dienen.

Begründung: Die Einhaltung des Datenschutzrechts ist wettbewerbsrelevant, weil sich hiergegen verstoßende Unternehmen im Wettbewerb mit datenschutzkonform arbeitenden Konkurrenten einen unlauteren Vorteil durch Rechtsbruch verschaffen. Bisher sind die Gerichte in Deutschland der Meinung, dass Datenschutzvorschriften nicht wettbewerbsschützend seien. Das Wettbewerbsrecht ist aber ein effizientes, unbürokratisches und erfolgreiches Instrument, das auf den Bereich des Datenschutzes erstreckt werden sollte.

3. Einführung einer Herstellerhaftung für den Fall, dass unsichere Produkte zu Datenschutzverletzungen führen (Produkthaftung)

Begründung: Im Softwarebereich wäre es sinnvoll, die Produkthaftung von Herstellern informationstechnischer Produkte auf Vermögensschäden zu erstrecken, die dadurch entstehen, dass ein Produkt nicht wirksam (Stand der Technik) vor Computerattacken oder Datenverlust geschützt ist. Dann würden Softwarehersteller für die Folgen ihrer Sicherheitslücken

("Bugs") haften, die schon oft für Verluste persönlicher Daten und von Betriebsgeheimnissen gesorgt haben. Das Haftungsrecht ist ein sehr effizientes Rechtsdurchsetzungsinstrument, wie sich etwa im Bereich der Arbeitssicherheit gezeigt hat. Es sollte auch für den Datenschutz nutzbar gemacht werden.

4. Verschuldensunabhängige Haftung für Datenschutzverletzungen mit pauschaler Entschädigungssumme

Die Datenverarbeiter sollten den Betroffenen auch für immaterielle Schäden haften (z.B. Sorge um einen möglichen Missbrauch ihrer Daten infolge einer Datenpanne), und zwar verschuldensunabhängig.

Ein Regelwert für den immateriellen Schaden sollte festgelegt werden (z.B. 200 Euro pro Person). Entschädigungszahlungen wegen Datenpannen könnte der für die Verarbeitung Verantwortliche dann vom Hersteller ersetzt verlangen (siehe Punkt 3 oben), wenn ein unsicheres Produkt für den Schaden verantwortlich ist.

Begründung: Durch die Einführung einer Haftung für Datenpannen samt pauschaler Entschädigungssummen wären große Datenverarbeiter gezwungen, sich gegen Datenschutzverletzungen zu versichern. Durch die Versicherungsprämie hätten sie ein eigenes finanzielles Interesse daran, die Schadenswahrscheinlichkeit zu senken. Auf dem Gebiet der Unfallversicherung hat ein solches System bereits zu einem drastischen Rückgang der Zahl der Arbeitsunfälle geführt.

5. Privacy by design: Kommerzielle informationstechnische Produkte dürfen nicht so voreingestellt sein, dass der Verwender gegen Datenschutzrecht verstößt.

Begründung: Computerprodukte müssen mit einer sicheren und datensparsamen Grundeinstellung ausgeliefert werden. Dies ist derzeit leider bei den - vorherrschenden - amerikanischen Produkten nicht der Fall, weil es in den USA bekanntlich im privaten Bereich keinerlei Datenschutzgarantien gibt. Kommerziellen Anbietern informationstechnischer Produkte ist es jedoch zumutbar, Produkte für den europäischen Markt mit datenschutzkonformen Voreinstellungen auszuliefern. Es ist auch gesamtwirtschaftlich sinnvoller, wenn der Hersteller sein Produkt rechtskonform gestaltet als wenn sämtliche Abnehmer das Produkt erst rechtskonform umgestalten müssen.

6. Einführung von Informationspflichten bei Datenschutzverletzungen

Begründung: US-amerikanische Erfahrungen zeigen, dass eine Informationspflicht über Datenpannen eine abschreckende Wirkung entfaltet und Vorbeugemaßnahmen der Datenverarbeiter fördert.

7. Maßnahmen zur Gewährleistung der Datensicherheit müssen dem Stand der Technik entsprechen.

Begründung: In den letzten Monaten sind immer wieder schwerwiegende Datenpannen mit Millionen von Betroffenen bekannt geworden, die hätten vermieden werden können, wenn die Verarbeitungssysteme auf dem Stand der Technik gewesen wären (z.B. durch Anwendung von Updates).

Formulierungsvorschlag für Artikel 17 (1) RiL 95/46/EG - neu:

"Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen die zufällige oder unrechtmässige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere

wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmässigen Verarbeitung personenbezogener Daten erforderlich sind.

Diese Maßnahmen müssen *dem Stand der Technik entsprechen und* ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist."

8. Benachteiligungsverbot bei Gebrauchmachen von Datenschutzrechten

Begründung: In der Praxis werden unabdingbare Regelungen des Datenschutzrechts immer wieder dadurch umgangen, dass Unternehmen mit einer ordentlichen Kündigung reagieren, wenn Betroffene von ihren gesetzlich garantierten Rechten Gebrauch machen. Zu diesen unabdingbaren Betroffenenrechten zählt insbesondere das Recht, Auskunft über die zur eigenen Person gespeicherten Daten verlangen zu dürfen sowie die Rechte auf Berichtigung, Löschung und Sperrung personenbezogener Daten.

Formulierungsvorschlag Richtlinie 95/46/EG: "Der der für die Verarbeitung Verantwortliche darf den Betroffenen nicht benachteiligen, weil dieser in zulässiger Weise von Rechten aus dieser Richtlinie Gebrauch macht. Wenn im Streitfall der Betroffene Tatsachen glaubhaft macht, die eine Benachteiligung im Sinne des Satzes 1 vermuten lassen, trägt der Verantwortliche die Beweislast dafür, dass andere, sachliche Gründe die Behandlung des Betroffenen rechtfertigen."

9. Einrichtung einer "Stiftung Datentest" nach dem Vorbild der "Stiftung Warentest", um verschiedene Anbieter von Dienstleistungen einer Art zu vergleichen im Hinblick auf die Menge der jeweils erhobenen personenbezogenen Daten, die Datenverwendung und -weitergabe (etwa ins Ausland, an Auskunfteien oder zu Werbezwecken) und die Datensicherheit.

Begründung: Verbraucher können heutzutage realistischerweise nicht überblicken, was einzelne Anbieter mit ihren Daten machen. Auf dem Gebiet der Qualitätssicherung hat sich in Deutschland das Modell der "Stiftung Warentest" bewährt, die Produkte testet, vergleicht und benotet. Wenn es eine "Stiftung Datentest" gäbe, könnten Verbraucher sich ausgehend von deren Urteil leicht für ein datenschutzfreundliches Produkt entscheiden. Hersteller würden schon präventiv für mehr Datenschutz sorgen, um eine Empfehlung zu erzielen und schlechte Bewertungen zu vermeiden.

Patrick Breyer
P.Breyer@daten-speicherung.de

Mi 10.06.2009 13:30