

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 Guthabekarten 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 angestregten 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](mailto:P.Breyer@daten-speicherung.de)

Mi 10.06.2009 13:30