

14. Januar 2011

## **Gesamtkonzept für den Datenschutz in der Europäischen Union**

**Stellungnahme des Verbraucherzentrale Bundesverbandes**

**Im Rahmen der Konsultation der EU zur Mitteilung KOM(2010) 609**

Register ID: 2893800753-48

Verbraucherzentrale Bundesverband e.V. – vzbv  
Fachbereich Wirtschaft und Internationales  
Markgrafenstr. 66  
10969 Berlin  
[wirtschaft@vzbv.de](mailto:wirtschaft@vzbv.de)  
[www.vzbv.de](http://www.vzbv.de)

---

## **Gesamtkonzept für den Datenschutz in der Europäischen Union**

Der Verbraucherzentrale Bundesverband (vzbv) bedankt sich für die Möglichkeit zur Stellungnahme über ein Gesamtkonzept für den Datenschutz in der Europäischen Union.

Der Datenschutz ist mit der digitalen Welt zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Anpassung des Datenschutzes an die technischen Entwicklungen in der digitalen Welt ist notwendig. Eine Präzisierung schon geltender Regelung kann dem Datenschutz noch mehr Biss verleihen. Dies gilt insbesondere hinsichtlich der Transparenz, der Einwilligung, der Definition von personenbezogenen Daten. Eine Präzisierung des anwendbaren Rechts erleichtert den Datenschutzbehörden und Unternehmen die Durchführung. Die Durchsetzung geltenden europäischen Rechts gegenüber hier tätigen nicht-europäischen Unternehmen muss forciert werden. Datenschutz ist Verbraucherschutz. Verbraucherverbände müssen die Verbraucher auch bei diesem Thema mit kollektivrechtlichen Instrumenten vertreten können.

### **2.1. Stärkung der Rechte des Einzelnen**

#### **2.1.1 Angemessener Schutz des Einzelnen in allen Situationen**

Der Verbraucherzentrale Bundesverband e.V. fordert die EU Kommission auf, in Umsetzung der Charta der Grundrechte der Europäischen Union und der Europäischen Menschenrechtskommission die Rechte der einzelnen Nutzer / Bürger konsequent ins Zentrum der Ausgestaltung des Gesamtkonzepts für den Datenschutz in der Europäischen Union zu stellen. Ausgangspunkt der Betrachtungen und Ausgestaltung des Datenschutzes ist zwingend das Individuum und sein Recht auf Souveränität über seine Daten auch und gerade in der digitalen Welt

#### **Personenbezogene Daten**

Der Verbraucherzentrale Bundesverband e.V. unterstützt eine weite Definition des Begriffs der personenbezogenen Daten, wie sie in der Richtlinie und in den Auslegungen der Art. 29 Gruppe existiert. Die Auslegungen enthalten die notwendige Flexibilität, um auf technische Entwicklungen eingehen zu können. Um den datenverarbeitenden Stellen und auch den Nutzern eine bessere rechtliche Klarheit zu geben, könnten Leitlinien der Art. 29 Gruppe, die dem Stand der Entwicklung der Technik angepasst werden können, eine Hilfestellung sein. Damit die Nutzung der personenbezogenen Daten aus Nutzersicht transparent bleibt, muss die Zweckbindung ihrer Erfassung dargelegt werden.

Auch Daten, die als einzelne Daten ohne Personenbezug sind, können im Kontext mit anderen Daten, also insbesondere im Rahmen einer Profilbildung, zu einem personenbezogenen Datum werden. Verschiedene Untersuchungen haben bereits gezeigt, wie leicht mit bereits existierenden Techniken Daten personenbeziehbar werden. Der Verbraucherzentrale Bundesverband e.V. hat in einer Tagung zum Thema behavioural targeting, „Wenn die Wirtschaft beim Surfen zuschaut“, auf die Probleme

durch insbesondere die Kombination verschiedener Techniken hingewiesen<sup>1</sup>. Der Verbraucherzentrale Bundesverband e.V. fordert die Kommission auf, ein grundsätzliches Verbot der Profilbildung (mit Erlaubnisvorbehalt) festzuhalten als Grundlage dafür, die Souveränität der Nutzer durchzusetzen. Potenziell personenbeziehbare Daten müssen rechtlich eingeordnet werden.

Der Verbraucherzentrale Bundesverband e.V. unterstützt die Kommission in Ihrem Vorhaben, auch für neue Verfahren eine rechtliche Grundlage zu schaffen, so insbesondere ein Verbot mit Einwilligungsvorbehalt bei der Erfassung und Verarbeitung von Geodaten, Datamining und Weitere.

Analog zu den Datenschutzaufsichtsbehörden Deutschlands und der Art. 29 Gruppe sieht der Verbraucherzentrale Bundesverband e.V. statische und dynamische IP-Adressen als personenbeziehbare Daten. Die Einführung von IPv6, mit dessen Einführung mehr statische IP-Adressen zur Verfügung stehen, wird diesen Bezug verstärken. Der Verbraucherzentrale Bundesverband e.V. fordert die EU Kommission auf, hier eine Klarstellung in diesem Sinne vorzunehmen.

### **2.1.2 Mehr Transparenz für die von der Verarbeitung Betroffenen**

Der Verbraucherzentrale Bundesverband e.V. stimmt zu, dass Transparenz eine Grundvoraussetzung für die Souveränität des Einzelnen über seine Daten und einen wirksamen Datenschutz ist.

Der Verbraucherzentrale Bundesverband e.V. unterstützt die Einführung eines allgemeinen Transparenzgrundsatzes für die Verarbeitung personenbezogener Daten verbunden mit Pflichten hinsichtlich der Art und Form der Bereitstellung dieser Informationen.

In der Tagung des Verbraucherzentrale Bundesverband e.V. „Wenn die Wirtschaft beim Surfen zuschaut“ wurde in einem Gutachten sowie in praktischen Anwendungen gezeigt, dass bei einer Vielzahl der Anwendungen des behavioural targeting die Nutzer keine Kenntnis über den Einsatz der Techniken erlangen. Einige dieser Techniken sind auch mit Schutzvorrichtungen, die durchschnittlich informierte Nutzer ergreifen können, nicht zu blocken. In einer Untersuchung wurde überdies gezeigt, dass regelmäßig nicht wahrnehmbar auf die Nutzung dieser Techniken hingewiesen wurde.

Datenschutzerklärungen dienen nicht der Verbraucherinformation. Sie dienen vorwiegend zur rechtlichen Absicherung der datenverarbeitenden Stelle. Auf einigen Internetseiten wird eine Einwilligungsfiktion unterstellt: mit der Nutzung der Seite werden Datenschutzerklärungen akzeptiert, d.h. die Einwilligung zur Verarbeitung von Daten erteilt. Die Sprache ist an juristischen Notwendigkeiten ausgerichtet, nicht an einer Erklärung für Nutzer. Die Erklärungen sind regelmäßig nicht kontextuell gegeben sondern in einer zentralen Datenschutzerklärung.

Im Ergebnis bedeutet diese mangelnde Transparenz, dass Nutzer keine Kenntnis der Datenverarbeitung haben und keine informierte Einwilligung erteilen können – wenn sie denn danach gefragt werden.

Es gibt Beispiele für eine bessere Praxis auch bei einzelnen Plattformen/Unternehmen. Es gibt vielfältige Möglichkeiten, gerade auch die Techniken des Internets für gute

---

<sup>1</sup> Die Dokumente zur Tagung sind verfügbar unter: <https://www.vzbv.de/go/presse/1422/index.html>

Verbraucherinformationen in diesem Kontext zu nutzen. Bislang ist dies aber kein Standard und die Anreize für Unternehmen, sich hier vorbildhaft zu verhalten, sind nicht ausreichend gesetzt.

Analog zur Richtlinie über unfaire Geschäftspraktiken (UCP) sollten auch Formulierungen für Einwilligungen als unfair bzw. nicht in Übereinstimmung mit dem Datenschutzrecht festgelegt werden.

EU Standardmuster für Datenschutzhinweise können helfen, sollten aber nicht einfach die bisherigen Datenschutzerklärung ersetzen. Kontextbezogene und verständlichere Informationen zur Datenerhebung und –verarbeitung müssen ergänzend zur Verbesserung der Transparenz vorgesehen werden.

Hilfreich für Nutzer wäre auch – wie immer – eine nutzerfreundliche Formulierung der Richtlinie bzw. der Gesetze. Die Information über die Datenerhebung und –verarbeitung ersetzt jedoch keinesfalls die notwendige Einwilligung hierzu durch die Nutzer!

### **Spezifische Regeln für den Datenschutz für Kinder**

Bei der Wahrnehmung der Datenschutzrechte handelt es sich um Grundrechtsausübung, für die es keine starre Altersregel gibt. Gerade im Internet ist die Gefahr, dass die Gutgläubigkeit und Unerfahrenheit von Kindern und Jugendlichen ausgenutzt wird, besonders groß. Deswegen bedarf es auch im Interesse der Anwenderinnen und Anwender klarer Regeln auch für Regelungen, ab wann und unter welchen Voraussetzungen Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können.

Die Erhebung von Daten bei Kindern und Jugendlichen sollte besonderen Restriktionen unterliegen, die auch nicht durch eine Einwilligung aufgehoben werden können. Neben Restriktionen für die besonders geschützten sensiblen Daten sollte geprüft werden, in welchem Umfang Techniken wie behavioural tracking und Profilbildung besondere Regelungen für Kinder notwendig machen sollten.

Besondere Anforderungen an die Transparenz gelten sicher bei Angeboten für besonders schutzbedürftige Personengruppen wie Kinder/Jugendliche. Hier bietet es sich an, Informationen für Kinder/Jugendliche wie auch für deren Eltern vorzusehen.

### **Anzeigepflicht für Datenschutzverstöße**

Der Verbraucherzentrale Bundesverband e.V. unterstützt die Einführung einer allgemeinen Anzeigepflicht für Datenschutzverstöße. Diese sollte für private wie für öffentliche Stellen gelten und möglichst direkt an die Betroffenen erfolgen. Nutzer können so gegebenenfalls geeignete Gegenmaßnahmen ergreifen oder Rechte geltend machen.

Immaterielle Schäden sollten über die Einführung eines pauschalen Schadenersatzes geltend gemacht werden können, d.h. der Geschädigte muss nicht einen exakt bezifferten Schaden angeben. Ausreichend ist die Darlegung, dass ein immaterieller Schaden vorliegt.

### **2.1.3 Bessere Kontrolle des Betroffenen über seine Daten**

#### **Datensparsamkeit**

Der Verbraucherzentrale Bundesverband e.V. spricht sich für die Stärkung des Prinzips der Datensparsamkeit aus. Auch wenn bereits die geltende Richtlinie dieses Prinzip ausformuliert hat, wird es in der Realität nicht ausreichend zur Geltung gebracht.

Viele der neuen Technologien und Anwendungen generieren Massen an Daten, für die offenkundig weder rechtlich noch wirtschaftlich ein ausreichender Anreiz zur Vermeidung oder Löschung existiert.

Die Förderung von datenvermeidenden oder datenschützenden Technologien ist ein Ansatz zur Umsetzung.

Sogenannte „Privacy by default“ Lösungen sind verpflichtend einzuführen, d.h. die Grundeinstellungen von Internetdiensten müssen so gesetzt sein, dass ohne Veränderungen durch den Nutzer der größtmögliche Datenschutz gilt.

Es sollte eine Verpflichtung eingeführt werden, anonyme und pseudonyme Nutzungsmöglichkeiten von Internetdiensten anzubieten.

#### **Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung**

Die Erhebung, Verarbeitung und Nutzung von Daten muss insgesamt transparenter werden. Der Betroffene soll in die Lage versetzt werden, seine bestehenden Auskunftsrechte auch tatsächlich geltend machen zu können. Dazu muss er wissen, wer welche Daten zu welchem Zweck gespeichert hat.

Die größte Hürde besteht darin, dass der Betroffene oft keine Kenntnis davon hat, wer Daten über ihn hält. Die Auskunftsrechte laufen in diesen Fällen leer. Ebenso werden Daten oft unbemerkt erhoben, so zum Beispiel bei den Spuren, die jeder Surfer im Internet hinterlässt.

Transparenz ist zu erreichen, in dem der Verbraucher Herr über seine Daten bleibt – jederzeit und uneingeschränkt. Eine Möglichkeit hierfür ist die aktive, informierte und freiwillige Einwilligung in die Datennutzung

Teil der Rechts ist es auch, Einwilligungen zu widerrufen. Einwilligungen beinhalten regelmäßig die Weitergabe der Daten auch an Dritte. Ein Sammelrückruf für Einwilligungen sollte eingeführt werden. In der Regel werden von einem Anbieter auch Einwilligungen für die Weitergabe von Daten an Dritte eingeholt. Widerruft der Verbraucher seine Einwilligungen bei diesem Anbieter, ist der Widerruf jedoch nur für den jeweiligen Anbieter maßgeblich. Der Anbieter ist nicht dazu verpflichtet, den Widerruf weiter zu geben. Dieses Verfahren ist verbraucherunfreundlich. Die meisten Verbraucher werden sich nicht an das Kleingedruckte erinnern, in dem niedergelegt wurde, an welche Dritte die Daten weitergegeben wurden. Daher muss das Unternehmen, das die Einwilligung erhalten und die Daten an Dritte weitergeleitet hat, auch zur Weiterleitung des Widerrufs verpflichtet werden.

Fristen, in denen eine entsprechende Reaktion der datenverarbeitenden Stellen erfolgen muss, sind für eine effektive Nutzung dieses Rechts notwendig. Auch sollte festgelegt werden, dass die Hinweise auf die Rechte sowie auf die verarbeitende Stelle prominent zu finden sind. Ein Medienbruch darf nicht erzwungen werden, d.h. dass

eine Einwilligung elektronisch erteilt wurde, ein Widerspruch oder ein anderes Anliegen jedoch schriftlich erfolgen muss.

### **Recht auf Vergessen**

Personenbezogene Daten in der Onlinewelt sollten einem Verfallsdatum unterliegen, nach dessen Ablauf die Daten entweder automatisch gelöscht werden, oder der Betroffene aktiv und freiwillig einer weiteren Haltbarkeit mit erneutem Verfallsdatum zustimmt. Dies ist ein entscheidender Schritt hin zu einem neuen Recht auf „Vergesslichkeit des Netzes“.

Das Recht auf Vergessen darf nicht beschränkt sein auf das Recht zum Widerruf der Einwilligung oder dem Recht auf Löschung der Daten auf Antrag. Die Datensparsamkeit gebietet, dass Daten nach Erfüllung des Zwecks im Rahmen der Zweckbindung gelöscht werden. Darüber hinaus sollte es aber möglich sein, das Vergessen beziehungsweise Verfallsdaten technisch zu ermöglichen. Von automatischen Löschvorgaben von Einträgen in einem Content Management System bis hin zu Softwarelösungen mit Verschlüsselung und zeitlich befristeten Schlüsseln wurden bereits mehrere Ansätze in die Diskussion gebracht. Technische Lösungen müssen jedoch durch gesetzliche Vorgaben unterfüttert werden.

### **Datenübertragbarkeit**

Unternehmen schränken oft die Möglichkeit ein, vom Verbraucher eingestellte Daten auf eine andere Plattform oder ein anderes System zu migrieren. Ein Anbieterwechsel ist damit nahezu unmöglich. Ein Recht auf Datenportabilität sollte deshalb eingeführt werden. Von diesem Recht ist umfasst, dass Verbraucher ihre einmal auf einer Plattform abgelegten oder eingestellten Daten barrierefrei zu einer anderen Plattform „transportieren“ dürfen. Dies schließt die vollständige und rückstandslose Löschung auf der ersten Plattform ein. Damit das Recht nicht ins Leere läuft, müssen gemeinsame Datenstandards und Schnittstellen für die Datenportabilität definiert werden.

#### **2.1.4 Bewusstsein fördern**

Der Verbraucherzentrale Bundesverband e.V. sieht die besondere Bedeutung von Aufklärung zum Thema Datenschutz und bietet den Verbrauchern daher auch selbst solche Informationen. Die Kofinanzierung von Aufklärungsmaßnahmen zum Thema Datenschutz ist sicher eine Möglichkeit, mehr Informationen zu generieren.

Verbraucherinformationen in vielen Themenfeldern haben aber auch gezeigt, dass das Wissen um die Fakten allein nicht zwingend zu den erwünschten Ergebnissen führt. So führte z.B. die Information über falsches Ernährungsverhalten nicht zu einer verminderten Fettleibigkeit und besserer Ernährung. Ähnliche Muster zeigen sich auch im Bereich Datenschutz.

Informationen zum Datenschutz sind nur erfolgreich, wenn Vorbilder zum Beispiel beim Datenschutz durch den Staat existieren, die Information hinsichtlich Sprache, Kontextualität, etc. geeignet sind, Rahmenbedingungen wie Transparenz; wie die Kopplung von Einwilligungen zur Datenverarbeitung und Zugang zu Dienstleistungen; Einwilligungen, die so ausgestaltet sind, dass sie nicht wahrgenommen werden.

### **2.1.5 Gewährleistung der Einwilligung ohne Zwang und in Kenntnis der Sachlage**

Der Verbraucherzentrale Bundesverband e.V. sieht ebenfalls, dass die Einwilligungen oftmals nicht den Kriterien genügen. Präzisierungen könnten Anbietern Hinweise geben, wie Einwilligungen besser ausgestaltet sein sollten.

Ein Weg zu Transparenz und damit zu Verbrauchern, die die Folgen ihres datenbezogenen Verhaltens realistisch abschätzen können, ist die aktive, informierte und freiwillige Einwilligung. Hierzu bedarf es einer grundsätzlichen Opt-In Regelung, die nicht durch weitreichende Ausnahmen ausgehöhlt wird. Opt-In als Einwilligungsvorbehalt und Opt-In als positive Formulierung von Einwilligungserklärungen.

Die Einwilligung muss aktiv sein. Der Betroffene muss durch aktives, bewusstes Handeln zustimmen, damit die Einwilligung wirksam wird. Dies kann zum Beispiel digital durch aktives anklicken eines Kontrollkästchens oder schriftlich durch gesonderte Unterschrift geschehen. Nicht ausreichend sind konkludente Erklärungen über das Akzeptieren der AGB oder gar durch bloßes Nutzen einer Internetseite.

Einwilligungen in Datenerhebung und -verarbeitung müssen informiert erteilt werden. Der Betroffene muss vor Erteilung der Einwilligung wissen, welche Folgen seine Einwilligung hat. Hierfür muss er informiert werden, welche Daten zu welchem Zweck erhoben werden, wie diese verwendet werden und ob und an wen sie weitergegeben werden. Er muss über seine Rechte betreffend die Daten informiert werden. Der Betroffene muss darüber informiert sein, ob Daten erhoben werden, die er nicht selbst mitteilt, zum Beispiel Standortdaten, die das Mobiltelefon automatisch versendet oder Daten die während des Surfens im Internet im Hintergrund gespeichert werden. Die verantwortliche Stelle muss den Betroffenen über diese Dinge verständlich, lesbar und exponiert informieren.

Die Einwilligung muss freiwillig sein. Sie darf weder generalisiert noch gekoppelt werden oder zur Umgehung eines gesetzlichen Erhebungsverbotes eingeholt werden. Dies gilt im Besonderen für Daten, die durch die Nutzung von digitalen und mobilen Kommunikationsmitteln anfallen und die nicht bloß der technischen Funktionalität des Kommunikationsmediums dienen. Ein Kopplungsverbot ist zu definieren, das die Freiwilligkeit der Einwilligung sichert.

Die Einwilligung muss zeitlich begrenzt werden. Häufig kann der Verbraucher – auch trotz neuer Hinweis- und Dokumentationspflichten – nicht mehr nachvollziehen wohin seine einst erteilte Einwilligung gewandert ist. Auch verblasst das Bewusstsein der rechtlichen Konsequenzen einer einmal erteilten Einwilligung mit der Zeit, Das gerade bei der mittlerweile sehr großen Anzahl speziell an Werbeeinwilligungen, die bereits alltäglich sind. Einmal erteilte Einwilligungen behalten für die verantwortlichen Stellen auch nicht ewig einen geschäftlichen Nutzen. Die Datenbestände veralten vielmehr sehr schnell, sind aber nur mit einer gewissen Aktualität wirklich brauchbar. Daher sollte nach beispielsweise 2 Jahren die Einwilligung ihre Wirksamkeit verlieren, mit der Folge, dass die Daten entweder gelöscht werden müssen oder eine neue Einwilligung eingeholt werden muss.

Einwilligungen müssen nachgewiesen werden. Im Streitfall hat die verantwortliche Stelle nachzuweisen, dass eine Einwilligung vorliegt. Dies funktioniert in der Praxis häufig nicht. Die verantwortlichen Stellen behaupten häufig eine Einwilligung zu haben,

weisen diese aber nicht nach. Es muss eine gesetzliche Klarstellung erfolgen, dass dieser Anspruch besteht.

Das Setzen von Cookies und die Profilbildung müssen dem Einwilligungsvorbehalt unterliegen. Verbraucher werden derzeit regelmäßig ohne ihre Kenntnis ausgeforscht und die gesammelten Kenntnisse durch Anbieter ihnen gegenüber verwendet. Hierdurch wird die Position der Verbraucher den Anbietern gegenüber systematisch geschwächt. Die Erlaubnis zum Setzen von Cookies kann nicht durch den Hinweis auf die Browsereinstellungen ersetzt werden. Browsereinstellungen sind regelmäßig nicht datenschützend ausgestaltet und bestimmte Formen von Cookies sowie andere Technologien lassen sich hiermit nicht durch den Nutzer steuern.

Zu weiteren Forderungen des Verbraucherzentrale Bundesverband e.V. zum Thema Behavioural Tracking: <http://www.vzbv.de/go/dokumente/974/1/4/index.html>

### **2.1.6 Sensible Daten**

Der Verbraucherzentrale Bundesverband e.V. unterstützt, dass Gendaten als besonders sensible Daten eingestuft werden.

Auch die Nutzung von Geodaten sollte präzisiert werden. Aus ihnen lassen sich Bewegungsprofile erstellen, so dass sie einer besonderen Regelung bedürfen. Die Nutzung von Geodaten ermöglicht aber auch eine Reihe von Dienstleistungen, die von Verbrauchern gerne angenommen werden.

### **2.1.7 Wirksamere Rechtsbehelfe und Sanktionen**

Der Verbraucherzentrale Bundesverband e.V. unterstützt verschärfte Sanktionen gegenüber denjenigen, die Datenschutzverletzungen begehen. Bislang stehen Sanktionen in keinem angemessenen Verhältnis zu den möglichen Gewinnen unrechtmäßigen Verhaltens. Strafrechtliche Sanktionen sollten möglich sein.

Eine Befugnis zur Klage bei nationalen Gerichten sollte sowohl den Datenschutzbehörden und qualifizierten Verbänden offen stehen. Der Verbraucherzentrale Bundesverband e.V. kann die Rechte der Verbraucher stellvertretend für sie einklagen. Die Normen, auf die der Verband sich beziehen kann, sind in Deutschland im Unterlassungsklagengesetz festgelegt. Der Datenschutz ist hier bislang nicht explizit als Verbraucherschützende Norm festgelegt, so dass der Verbraucherzentrale Bundesverband e.V. nur eingeschränkt für Verbraucher beim Datenschutz die Instrumente des kollektiven Rechtsschutzes nutzen kann.

Überdies sollte eine Sammelklage auf Schadensersatz für Verbraucher auch für Verstöße gegen das Datenschutzrecht gelten.

## **2.2. Stärkung der Binnenmarktdimension**

Eine weitere Annäherung der nationalen Datenschutzrechte könnte den Unternehmen etwas mehr Sicherheit geben beim grenzüberschreitenden Austausch von Daten. Eine



Präzisierung des anwendbaren Rechts ist wünschenswert. Eine Harmonisierung ist hierfür nicht erforderlich. Eine Harmonisierung würde eine Weiterentwicklung des Datenschutzes erschweren, da der Wettbewerb um besseres Recht zwischen den Mitgliedsstaaten ausgeschaltet wird und derzeit schon existierende weitergehende Regelungen einer Harmonisierung zum Opfer fallen würden.

Aus der Sicht des Verbraucherzentrale Bundesverband e.V. bestehen die Schwierigkeiten für deutsche Verbraucher beim grenzüberschreitenden Datenschutz überwiegend in der Durchsetzung des Rechts gegenüber (insbesondere US-amerikanischen) Unternehmen ohne Niederlassung in der Europäischen Union. Hier wird ein großer Bedarf für Aktivitäten der EU Kommission gesehen.