

IM BLICKPUNKT: Informationelle Selbstbestimmung



Datenschutz





Informationelle Selbstbestimmung

Seit 2010 kann man bei Google Street View die 20 größten Städte Deutschlands virtuell begehen - neun davon in Nordrhein-Westfalen. Bevor die abfotografierten Rundumansichten der Straßenzüge veröffentlicht wurden, musste Google Gesichter und Autokennzeichen unkenntlich machen. Knapp 250.000 Bürger(innen) nahmen zusätzlich das Recht wahr, ihr Haus verpixeln zu lassen, auch wenn es sich bei Häuserfassaden nicht direkt um personenbezogene Daten handelt.

Aber ist das Angebot wirklich eine Gefahr für die Privatsphäre? Viele der verpixelten Häuser sind trotzdem im Netz zu betrachten, auf Fotos, die Privatleute mit Geodaten versehen und auf Fotoplattformen hochgeladen haben. Für Kriminelle sind Angaben zur Abwesenheit von Hausbesitzern, die sich entsprechenden Einträgen in sozialen Netzwerken entnehmen lassen, ohnehin viel interessanter. Mehrere Millionen Deutsche lassen Unternehmen durch ihre Kundenkarten freiwillig Rückschlüsse auf ihre Lebensverhältnisse ziehen. Und auch wer sich wann wo aufhält, verraten unsere Mobiltelefone schon längst.

Fragen des Datenschutzes stellen sich in vielen Lebensbereichen – online wie offline. Nicht immer ist die Lage eindeutig und nicht alle datenschutzrechtlich bedenklichen Entwicklungen werden so öffentlich diskutiert wie Street View.

IM BLICKPUNKT: Informationelle Selbstbestimmung erklärt die rechtlichen Grundsätze des Schutzes personenbezogener Daten in Deutschland, zeigt datenschutzrechtliche Problembereiche und Herausforderungen in der digitalen Welt auf, gibt Hintergrundinformationen zu Profilbildung und Tipps für den alltäglichen Umgang mit den eigenen personenbezogenen Daten.

Datenschutz

Die Gesetzeslage

Im Volkszählungsurteil von 1983 definierte das Bundesverfassungsgericht erstmals das Recht auf informationelle Selbstbestimmung als Teil des im Grundgesetz verankerten allgemeinen Persönlichkeitsrechts, welches wiederum aus dem Recht auf freie Entfaltung der Persönlichkeit und der Menschenwürde resultiert. Jeder Einzelne soll, so das Bundesverfassungsgericht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können (BVerfGE 65, 1). Vorangegangen waren dem Urteil zahlreiche Proteste und Prozesse gegen das Vorgehen bei der für 1983 geplanten (und schließlich im Jahr 1987 durchgeführten) Volkszählung.

Das Datenschutzrecht soll die informationelle Selbstbestimmung gewährleisten und den Einzelnen vor dem Missbrauch persönlicher Daten schützen. In Deutschland ist der allgemeine Datenschutz für Bundesbehörden und Unternehmen durch das Bundesdatenschutzgesetz (BDSG), für öffentliche Stellen der Länder durch die Landesdatenschutzgesetze geregelt. Hinzu kommen spezifische Datenschutzregelungen für Bereiche wie Polizei, Kreditwesen oder Telekommunikation.

Links

- Volkszählungsurteil des Bundesverfassungsgerichts von 1983.
Kurzlink: www.grimme-institut.de/d/313602
- Bundesdatenschutzgesetz – Text und Erläuterung.
Kurzlink: www.grimme-institut.de/d/519037
- Datenschutzgesetz Nordrhein-Westfalen.
Kurzlink: www.grimme-institut.de/d/159644
- Datenschutzrichtlinien der Europäischen Union 95/46/EG und 2002/58/EG.
Kurzlink: www.grimme-institut.de/d/718976
- Richtlinie zur Vorratsdatenspeicherung der Europäischen Union 2006/24/EG.
Kurzlink: www.grimme-institut.de/d/808486

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (BDSG § 1 Abs. 1). Zu den personenbezogenen Daten gehören insbesondere Name, Adresse, Geburtsdatum, Geburtsort, Familienstand, Kfz-Kennzeichen, Telefonnummer oder E-Mail-Adresse. Strengere Regelungen gelten für als besonders sensibel erachtete Daten, zu denen Angaben über die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gesundheit und Sozialleben gehören. Personenbezogen sind Daten immer dann, wenn sie mit dem Namen der betroffenen Person verbunden sind oder sich in sonstiger Weise, d.h. aus ihrem Zusammenhang oder mittels Zusatzwissen, ein Bezug zur Identität der Person herstellen lässt.

Grundsätze des Datenschutzes

Die Datenschutzgesetze regeln nicht den Schutz von Daten, etwa durch technische Maßnahmen, sondern den Schutz des Einzelnen vor der unbegrenzten Verarbeitung ihn betreffender Daten. Sie beschränken, welche Daten wie und in welchem Kontext über eine Person erhoben werden dürfen. Grundlegend im Datenschutz ist das sogenannte Verbot mit Erlaubnisvorbehalt: Personenbezogene Daten dürfen nur erhoben werden, wenn die betreffende Person in die Datenerhebung, -nutzung und -verarbeitung aus freier Entscheidung eingewilligt hat oder ein Gesetz dies ausdrücklich gestattet.

Weiter gilt das Prinzip der Datenvermeidung und Datensparsamkeit. Demnach sollen keine oder so wenig personenbezogene Daten wie möglich verarbeitet und genutzt werden. Das Prinzip der Erforderlichkeit verlangt, dass nur diejenigen Daten erhoben, gespeichert und verarbeitet werden dürfen, die für die Erfüllung der jeweiligen Aufgabe unbedingt nötig sind. Ist beispielsweise die Abwicklung eines Geschäfts erfüllt, müssen die Daten gelöscht werden. Der Grundsatz der Zweckbindung legt fest, dass personenbezogene Daten nur zu den Zwecken verarbeitet werden dürfen, zu denen sie erhoben und gespeichert worden sind. Sobald Daten vorliegen, müssen Maßnahmen zur Gewährleistung der Datensicherheit ergriffen werden.

Transparenz muss darüber herrschen, welche verantwortliche Stelle Daten erhebt – auch bei der Videoüberwachung öffentlich zugänglicher Räume. Außerdem muss klar sein, zu welchem Zweck die Daten erhoben werden. Dem Betroffenen ist auf Anfrage unentgeltlich Auskunft über die Daten zu gewähren, die über ihn erhoben, gespeichert oder an Dritte weitergegeben wurden. Hier können aber andere Interessen (wie die öffentliche Sicherheit) Vorrang haben. Für den Fall von Datenpannen, bei denen den Betroffenen schwerwiegende Beeinträchtigungen drohen, besteht ihnen und den Aufsichtsbehörden gegenüber Informationspflicht. Verstöße gegen das Bundesdatenschutzgesetz werden größtenteils als Ordnungswidrigkeiten geahndet.

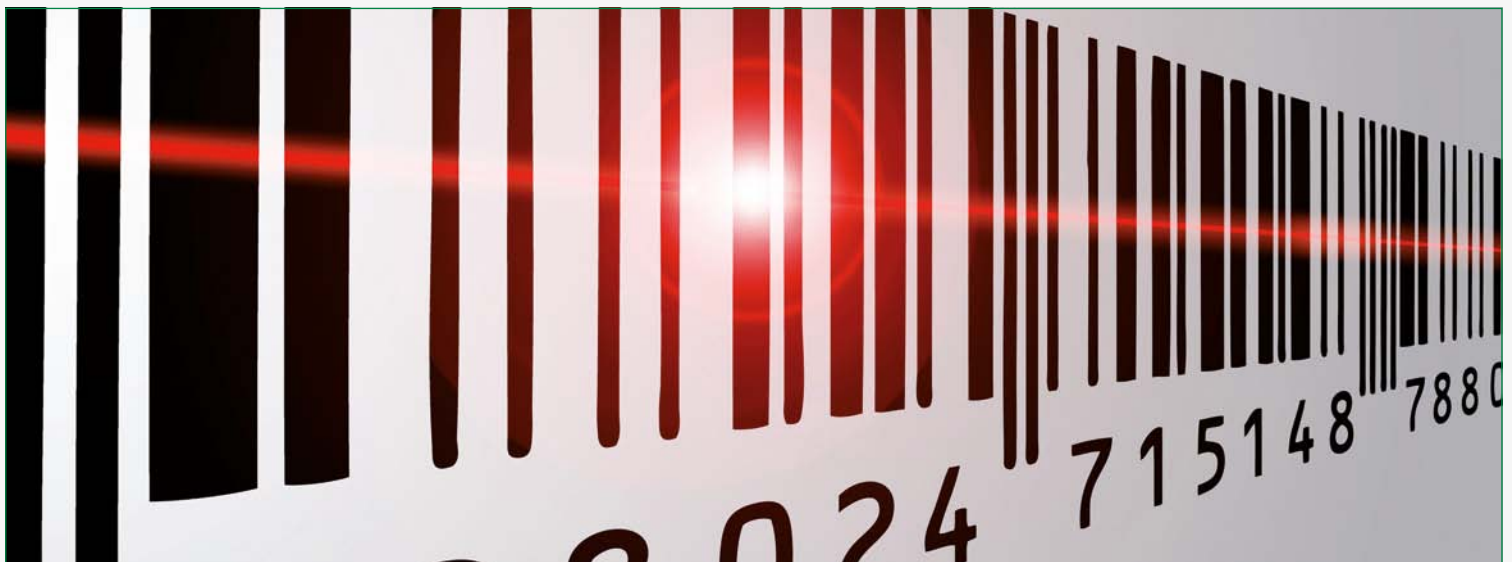
Einschränkungen und Herausforderungen des Rechts auf informationelle Selbstbestimmung

Zwischen der Volkszählung 1987 und dem Zensus 2011 hat sich nicht nur in den technischen Möglichkeiten der elektronischen Datenerfassung und -vernetzung einiges getan: Einerseits machten Überwachungs- und Bespitzelungsskandale in deutschen Unternehmen im Jahr 2009 eine Novellierung des BDSG nötig, während gleichzeitig von staatlicher Seite Mechanismen zu Überwachung und Informationsaustausch zur Terrorbekämpfung eingerichtet wurden. Andererseits sind mit der Verbreitung des Internets und globaler Dienste die Angabe von privaten Daten, ihre Veröffentlichung im Freundeskreis und Nutzerprofilbildung alltäglich und nicht immer vermeidlich geworden.

Die Rolle des Staates

Durch das BDSG erlegt sich der Staat selbst Regeln für den Umgang mit den personenbezogenen Daten seiner Bürger(innen) auf. Dabei hat er jeweils das Recht des Einzelnen auf informationelle Selbstbestimmung mit den legitimen Informationsinteressen von Staat und Gesellschaft in Ausgleich zu bringen. So wie der Datenfluss, insbesondere im Internet, nicht an Landesgrenzen Halt macht, gewinnt der Datenschutz auch im internationalen Kontext zunehmend an Bedeutung.

Eine Reihe von Richtlinien und internationalen Abkommen bestimmt staatenübergreifende Standards und Regelungen zum Datenaustausch. Zum Teil werden





hier vor allem Ziele der Verbrechens- und Terrorbekämpfung über das persönliche Recht auf informationelle Selbstbestimmung gestellt. Entgegen der Verpflichtung, Verbindungsdaten ihrer Kunden zu löschen, sobald sie nicht mehr für die Rechnungsstellung benötigt werden, sollen nach der EU-Richtlinie zur Vorratsdatenspeicherung Telekommunikationsunternehmen dazu verpflichtet werden, eine Reihe von Daten für mindestens sechs Monate zu speichern. Darunter sind: angerufene und gewählte Telefonnummern sowie Gesprächszeiten, Internet-Verbindungsdaten wie die IP-Adresse und beim Mobilfunk zusätzlich Standortdaten des Nutzers. In Deutschland wurde das Gesetz zur Umsetzung der Richtlinie 2010 vom Bundesverfassungsgericht gekippt. Ende Mai hat die EU-Kommission Deutschland wegen der Nichtumsetzung vor dem Europäischen Gerichtshof verklagt.

Während bei der Vorratsdatenspeicherung keine Inhalte der Kommunikation erhoben werden, erlaubt die Onlinedurchsuchung bei der Verfolgung schwerwiegender Straftaten das Abhören von Internet-Telefonie (VoIP) und das Mitlesen von Chatprotokollen und E-Mails. Kritisiert wurde der dafür verwendete sogenannte Bundes- oder Staatstrojaner, weil er mehr Informationen übermitteln kann als gesetzlich erlaubt ist. Im Zuge der Terrorbekämpfung erlaubt die EU im PNR-Abkommen (passenger name record) die automatische Übermittlung und jahrelange Speicherung von Passagierdaten an die US-Heimatschutzbehörde. Aus den Buchungs- und Flugdaten werden dann Profile errechnet, aufgrund derer Fluggäste die Einreise in oder der Überflug von amerikanischem Gebiet verwehrt werden können. Das SWIFT-Abkommen ermöglicht den USA Einsicht in die Speicherung bestimmter Überweisungsdaten europäischer Kunden.

Internationale Privatwirtschaft

Während sich Deutschland und die EU bei den internationalen Abkommen Einschränkungen der informationellen Selbstbestimmung von anderen Ländern auferlegen lassen, bestimmen im privatwirtschaftlichen Bereich zunehmend internationale Konzerne, was sie mit den Daten ihrer Kunden tun – entgegen den Bestimmungen des BDSG oder der EU-Datenschutzrichtlinie.

An sich ist die Übermittlung von personenbezogenen Daten in Länder, die über keinen europäischen Standards entsprechenden Datenschutz verfügen, nach EU-Recht verboten. Davon sind auch amerikanische Unternehmen betroffen. Treten sie allerdings dem Safe-Harbor-Abkommen zwischen EU und USA bei, können sie Daten deutscher Nutzer(innen) in den USA speichern und verwenden. Ob sich die Firmen an diese Minimalregelungen halten, wird in den USA allerdings kaum überwacht.

So stehen amerikanische Unternehmen und Internet-Dienste in Deutschland immer wieder wegen ihrer „hausgemachten“ Datenschutzrichtlinien in der Kritik. Google führt seit 2012 alle Daten aus seinen verschiedenen Angeboten zu Nutzerprofilen zusammen; zu welchem Zweck dies geschieht und was mit den Daten passiert, ist unklar. Eine Möglichkeit, die Profilbildung zu verhindern oder einzuschränken (engl. Opt-Out) besteht nicht: Wer nicht zustimmt, kann viele Google-Angebote nicht nutzen. Zweckgebundenheit und Erforderlichkeit stehen auch in Frage, wenn sich beispielsweise Spiele-Apps für Smartphones oder Social Games bei der Installation Zugriff auf Gesprächsdaten genehmigen.

Profilbildung

Kundenkarten und Bonuspunkteprogramme locken im Austausch für personenbezogene Daten mit Rabatten oder Prämien. Wer sie einsetzt, legt den beteiligten Unternehmen und dritten Partnern sein Konsumverhalten für Marktforschungs- und Werbezwecke offen. Im Internet ermöglichen Cookies – kleine Dateien, die Nutzeraktivitäten protokollieren – die Erstellung von Interessens- und Bewegungsprofilen. Oft reicht das Anklicken eines Angebots aus, um sofort auch auf anderen Websites mit Werbung für das Produkt konfrontiert zu werden. Auch aus den Daten, die der Computer ohne Zutun des Nutzers übermittelt, lassen sich Profile für personalisierte Werbung bilden: Die IP-Adresse verrät den Standort des Nutzers, der Browser die Sprache und das Betriebssystem verrät, womit wir surfen. Solches Targeting und Tracking machen das Gerät, nicht aber den Nutzer identifizierbar. Ob es sich damit um personenbezogene Daten handelt, ist strittig. Ist der Nutzer aber gleichzeitig

bei sozialen Netzwerken oder anderen Diensten angemeldet, wird unser Surfverhalten mit dem dortigen Profil verknüpft und Werbeangebote oder Suchergebnisse werden auch an Geschlecht, Alter oder angegebene Vorlieben angepasst.

Privates Umfeld

Werden personenbezogene Daten zu familiären oder rein persönlichen Zwecken erhoben, unterliegen sie dem BDSG nicht. Besonders in sozialen Netzwerken kann dies zum Problem werden, wenn andere – oft ohne böse Absicht – personenbezogene Daten über ihre Freunde veröffentlichen. Aber auch die Daten, die man selbst über sich im Netz veröffentlicht, lassen viele Rückschlüsse auf die eigene Person zu. Durch Verknüpfungen und Markierungen in sozialen Netzwerken sind Personen eindeutig zu lokalisieren und identifizieren – auch für Dritte wie den (zukünftigen) Arbeitgeber. Wer sein Geburtsdatum oder seine E-Mail-Adresse zusammen mit dem eigenen Namen veröffentlicht, läuft Gefahr, dass andere Online-Profile in seinem Namen anlegen – als Spaß unter Freunden oder Identitätsmissbrauch.

Standortbezogene Dienste (engl. location-based services) wie foursquare ermöglichen es, Freunde zu orten oder anzugeben, mit wem man unterwegs ist. Sie machen aber auch andere darauf aufmerksam, dass man gerade nicht zu Hause ist. Datenschutzrechtlich besonders kritisch sind Funktionen wie der Freundefinder, der es facebook erlaubt, automatisch Einladungs-E-Mails an das gesamte Adressbuch eines facebook-Nutzers zu verschicken, auch wenn die eigenen Freunde mit dem Netzwerk nichts zu tun haben wollen. Grundsätzlich gilt: Wer Bilder, Videoaufnahmen oder private Daten von anderen Personen ins Netz stellt, muss die betroffene Person um Erlaubnis bitten.

Verschwimmen von Online- und Offline-Welt

Neue technische Entwicklungen bieten Möglichkeiten, unser alltägliches „Offline“-Leben immer genauer zu erfassen. Globale Positionierungssysteme (GPS) dienen zur Orientierung beim Autofahren, sind aber mittlerweile auch in fast jedem Smartphone integriert. Was etwa bei der Suche nach Vermissten hilfreich ist, kann aber genauso zur Erstellung von Bewegungsprofilen missbraucht werden. RFID-Technik (Radio Frequency Identification) findet immer häufiger Verwendung in Verpackungen, Eintrittskarten, Ausweisdokumenten, zum Beispiel seit 2011 im neuen Personalausweis.

Die auf den kleinen Chips gespeicherten Daten lassen sich unbemerkt aus wenigen Metern Entfernung auslesen. Sie eignen sich nicht nur zur intelligenten Inventur, Logistik und Zugangskontrolle, sondern auch zur eindeutigen Identifizierung oder gar Verfolgung von Personen. Videoüberwachung an öffentlichen Orten erhöht für manche das Sicherheitsgefühl und kann die Strafverfolgung erleichtern. Gleichzeitig liefert sie viele Daten über den Aufenthaltsort von Menschen und kann dabei tief in die Privatsphäre eingreifen. Die Videobilder können auch mit Techniken der Gesichtserkennung kombiniert werden, die mitt-

lerweile nicht mehr nur an Flughäfen, sondern auch im privaten Bereich in sozialen Netzwerken und auf Foto-Plattformen eingesetzt werden.

Tipps für den alltäglichen Umgang mit personenbezogenen Daten

Wer sein Recht auf informationelle Selbstbestimmung wahrnehmen möchte, muss zwischen den positiven Chancen neuer technischer und medialer Entwicklungen und den zweifellos bestehenden Risiken des Missbrauchs der gesammelten und verfügbaren Daten über die eigene Person abwägen. Grundsätzlich gilt: Kaum ein Dienst oder Angebot im Internet ist wirklich gratis; wir bezahlen mit unseren Daten. Für den alltäglichen Umgang mit den eigenen Daten helfen ein paar Regeln:

- Gehen Sie online und offline zurückhaltend mit Ihren persönlichen Daten um und füllen Sie nur die zur Geschäftsabwicklung nötigen Pflichtfelder aus.
- Fragen Sie sich, welchen tatsächlichen Mehrwert Sie von der Preisgabe Ihrer Daten haben.
- Erkundigen Sie sich genau, wer welche Daten von Ihnen haben will und prüfen Sie, wer hinter Preisausschreiben und Umfragen steckt.
- Beachten Sie die Datenschutzbestimmungen und das Kleingedruckte in (Online-)Verträgen und willigen Sie nicht ein, dass Ihre Daten weitergegeben werden. Ist ein Widerspruch nicht möglich, sollte man sich nach datenschutzfreundlicheren Alternativen zum betreffenden Angebot umsehen.

Links

- Das virtuelle Datenschutzbüro ist eine Informationsplattform deutscher Datenschutzinstitutionen und weiterer Partner zu Datenschutzthemen.
www.datenschutz.de
- Das Bundesamt für Sicherheit in der Informationstechnik gibt Tipps für sicheres Surfen im Netz.
www.bsi-fuer-buerger.de
- Im Online-Lexikon des Fachmagazins „Datenschutz Praxis“ werden über 20.000 Fachbegriffe aus dem Bereich Datenschutz erklärt.
www.datenschutz-praxis.de/lexikon/
- Der FoeBud e.V. (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) aus Bielefeld vergibt seit 2000 jährlich mit den Big Brother Awards Negativpreise an öffentliche Stellen und Unternehmen, die die informationelle Selbstbestimmung von Bürger(inne)n einschränken oder auf andere Weise Prinzipien des Datenschutzes verletzen.
www.foebud.org
- Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz.
www.thm.de/zaftda/
- In der Reihe IM BLICKPUNKT sind Ausgaben zu den Themen „Werbung im Internet“, „Hier und Jetzt im Netz“ über ortsbezogene Internetdienste und „Bezahlen im Web“ erschienen.
www.grimme-institut.de/imblickpunkt

Links

- Der Arbeitskreis Vorratsdatenspeicherung informiert auf seiner Website über die aktuelle Lage im Streit um die verdachtsunabhängige Speicherung von Telekommunikationsdaten in Deutschland und zeigt, wie datensparsame Kommunikation funktioniert.
www.vorratsdatenspeicherung.de
- Die interaktive Grafik „Verräterisches Handy“ zeigt, wie aus auf Vorrat gespeicherten Verbindungsdaten und frei verfügbaren Inhalten aus dem Netz ein detailliertes Bewegungsprofil des Politikers Malte Spitz entsteht.
www.zeit.de/vorratsdaten

- Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vermittelt Grundwissen zum Datenschutz interaktiv.
www.bitkom-datenschutz.de
- Das nicht-kommerzielle Browser-Spiel „Data Dealer“ macht unter dem Motto „legal, illegal, scheißegal“ auf die Praktiken der Datensammler aufmerksam. Ziel des Spiels ist es, aus Nutzerdaten von sozialen Netzwerken, Umfragen, Gewinnspielen oder Kundenkarten so viele Persönlichkeitsprofile wie möglich zu erstellen.
www.datadealer.net

- Erstellen Sie sichere Passwörter aus großen und kleinen Buchstaben sowie Sonderzeichen mit mindestens 10 Stellen und erneuern Sie diese regelmäßig.
- Übernehmen Sie auch Verantwortung für die Daten anderer und fragen Sie nach, bevor Sie Bilder oder Kontaktdaten Ihrer Freunde weitergeben.

Datensparsames Surfen

- In allen gängigen Browsern kann man unter „Einstellungen“ das Setzen von Cookies einschränken beziehungsweise sie automatisch nach jeder Sitzung löschen lassen. Außerdem bieten sie Möglichkeiten, private Sitzungen zu starten, nach denen alle Daten wie besuchte Seiten, Textfeldeingaben oder Passwörter gelöscht werden.
- Um Profilbildung einzuschränken, nutzen Sie nicht nur Dienste eines Anbieters, verwenden Sie unterschiedliche Browser für verschiedene Zwecke und melden Sie sich nicht bei allen Diensten mit derselben E-Mail-Adresse an.
- Beschränken Sie in sozialen Netzwerken den Personenkreis, der Zugang zu Ihren Profilinformativen hat, sonst sind Ihre Angaben unter Umständen für die ganze Netzöffentlichkeit sichtbar.
- Nach § 13 Absatz 6 des Telemediengesetzes (TMG) haben Diensteanbieter „die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“.

Dem Recht auf informationelle Selbstbestimmung entsprechend sind Behörden und Unternehmen verpflichtet, Ihnen Auskunft über die Daten zu gewähren, die über Sie erhoben, gespeichert oder weitergegeben wurden. Nutzen Sie diese Möglichkeit und bestehen Sie gegebenenfalls auf Änderung, Löschung oder Sperrung der entsprechenden Daten. Die Einhaltung datenschutzrechtlicher Vorschriften durch Behörden und Unternehmen zu kontrollieren, ist Aufgabe der Datenschutzbeauftragten des Bundes und der Länder und

der EU. An diese Stellen kann sich jede(r) Bürger(in) mit Beschwerden oder Fragen zur Wahrung des Rechts auf informationelle Selbstbestimmung wenden und wird gegebenenfalls an die jeweils zuständigen Stellen verwiesen.

Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2 – 4, 40213 Düsseldorf
Postfach 20 04 44, 40102 Düsseldorf
Tel.: 0211-38424-0
E-Mail: poststelle@ldi.nrw.de
Web: www.ldi.nrw.de

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30, D-53117 Bonn
Tel.: 0228-997799-0
E-Mail: poststelle@bfdi.bund.de
Web: www.bfdi.bund.de

Impressum

Die Erstellung dieser Broschüre wurde von der Ministerin für Bundesangelegenheiten, Europa und Medien des Landes Nordrhein-Westfalen gefördert. Sie kann kostenlos unter www.grimme-institut.de/imblickpunkt heruntergeladen werden.

Grimme-Institut
Gesellschaft für Medien, Bildung und Kultur mbH
Eduard-Weitsch-Weg 25 • D-45768 Marl
Tel: +49 (0) 2365 9189-0 • Fax: +49 (0) 2365 9189-89
E-Mail: info@grimme-institut.de
Internet: www.grimme-institut.de

Text: Cathrin Bengesser
Redaktion: Annette Schneider
Gestaltung und Layout: Georg Jorczyk
Bildquellen: lassedesignen (S. 1 u. 2), Jürgen Fälchle (S. 1. u. 3), semisatch (S. 1 u. 4); alle Fotolia.com

Redaktionsschluss: Juni 2012