

# MEINE DATEN gehören mir!

Wissen Sie, welche Behörden und Firmen Ihre persönlichen Daten haben? Mehr als Sie denken, wie unser Selbsttest zeigte. Doch machtlos sind Sie dagegen nicht

VON CHRISTOPH SACKMANN & BENJAMIN HARTLMAIER

**N**ie habe ich so viel Post in meinem Briefkasten gehabt, wie ab dem Zeitpunkt, an dem ich beschloss, nachzuforschen, wer mich alles kennt. Fast täglich brachte der Postbote Briefe von Firmen, Behörden und Auskunftsteilen im In- und Ausland vorbei. Darin mein Name, meine Adresse, Geburtsdatum, Kontoverbindung, Telefonnummer, E-Mail-Adressen. 36 Stellen von Amazon bis zum Zoll hatte ich zuvor angeschrieben und um Auskunft über meine Daten gebeten. Das waren wahrscheinlich nicht einmal alle Unternehmen und Behörden, die mich kennen.

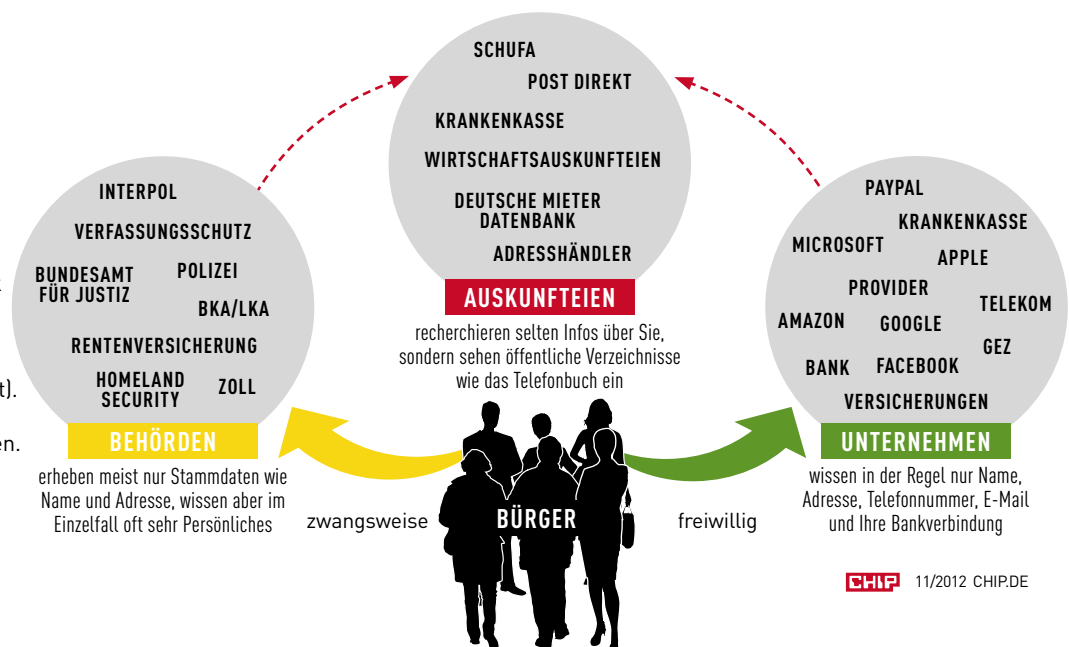
Einmal im Jahr hat jeder Bundesbürger das Recht, Auskunft über seine persönlichen Daten zu ersuchen: Was hat ein Unternehmen oder eine Behörde über mich gespeichert? Wie sind sie an diese Daten gekommen? Sind sie überhaupt korrekt? Viele Datenquellen sind offensichtlich. Klar, dass Facebook Ihre Freunde kennt oder Amazon Ihre Vorlieben für Horrorfilme. Damit lässt sich passgenaue Werbung

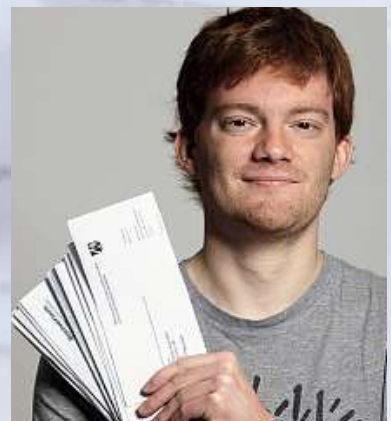
anbieten, das Geschäftsmodell vieler Internetunternehmen. Sie tauschen also Ihre Daten gegen einen meist kostenlosen Service ein. Das ist nicht verwerflich, Sie sollten sich aber bewusst machen, dass aus vielen Einzeldaten von Ihnen auch viele Rückschlüsse auf Ihre Lebensumstände möglich sind. Sie suchen bei Google nach Schwangerschaftstipps? Dann steht wohl Nachwuchs an. Kaufen Sie danach Windeln und Barbie bei Amazon, ist es wohl ein Mädchen geworden. Wohnen Sie zudem in einem teuren Stadtviertel, ist es jetzt wohl an der Zeit, Ihnen eher die Broschüre für die etwas teureren Rotweine zum Samstagabend zu schicken.

Letzteres ist die Geschäftsgrundlage von Wirtschaftsauskunftsteilen wie Bürgel, Arvato oder Boniversum. Die sammeln ähnlich wie die bekanntere Schufa alle möglichen öffentlichen Daten über Sie und verkaufen diese an Unternehmen. Das kann sich – neben Werbung im Briefkasten – auch zu handfesten Nachteilen auswirken. →

## DATENSAUGER & ADRESSHÄNDLER

In einigen Fällen haben Sie selbst die Kontrolle darüber, wer welche Daten von Ihnen bekommt, etwa wenn Sie Privatunternehmen (grün) wie Facebook freiwillig Informationen preisgeben. Behörden (gelb) fordern Infos meist zwangsweise von Ihnen ein. Keinen Einfluss haben Sie bei Auskunftsteilen (rot). Diese dürfen alles, was öffentlich über Sie bekannt ist, speichern und verwenden. Immerhin: Bei allen Stellen können Sie einsehen, was über Sie offenkundig ist und falsche Angaben korrigieren.





## SELBSTTEST

Ganze 36 Briefe schickte Christoph Sackmann ab – an das Bundeskriminalamt, die Rentenversicherung, Amazon, seine Bank, Homeland Security und viele mehr. Zurück kam ein Papierberg, denn mehr als die Hälfte der angeschriebenen Behörden und Unternehmen antwortete innerhalb weniger Wochen. Beruhigendes Ergebnis: Weder bei Interpol noch beim Verfassungsschutz sind seine persönlichen Daten gespeichert – oder sie werden noch geheimgehalten.

# WER kommt wie an welche Daten?

Anonym, freiwillig, zwangsweise – es gibt viele Arten, Sie genau kennenzulernen. Auch heimlich spionieren gehört dazu

Die meisten Daten geben Sie über sich preis, ohne dass Sie es merken. Bei jedem Webseitenaufruf werden zahlreiche Angaben übermittelt. Von welcher Webseite kommen Sie, welchen Browser verwenden Sie, welche Auflösung hat Ihr Bildschirm, auf welche Sprache ist Ihr System eingestellt – all das lässt sich mit Analyseprogrammen wie Google Analytics auswerten. Kaum ein Webseitenbetreiber verzichtet darauf, denn es ermöglicht eine zielgenaue Anpassung der Homepage an die Bedürfnisse der Kunden. Sind Sie etwa gerade in München, sind Ihnen die Groupon-Angebote aus Hamburg relativ egal. Manche Shops nutzen die Analyse aber auch für fiese Tricks: Sie empfehlen Kunden, die ihre Webseite per iPhone besuchen, teurere Produkte als anderen Nutzern. Wer sich ein iPhone leisten kann, ist schließlich wohlhabender, so die Logik dahinter. Allerdings werden alle Daten anonym erhoben – wechseln Sie das Gerät, vergisst die Webseite bereits, dass Sie ein teures Smartphone besitzen.

## Das Tauschgeschäft: Daten gegen Service

Amazon, PayPal und Co. hingegen müssen Sie für Geschäfte einwandfrei identifizieren können – schließlich soll das Paket bei Ihnen zu Hause ankommen und das Geld auf Ihrem Konto landen. Daher sind Sie bei fast allen Online-Angeboten gezwungen, grundlegende persönliche Daten anzugeben. Zu den Stammdaten gehören meist Name, Adresse und eine Kontoverbindung, eventuell noch Kontaktdaten wie Telefonnummer und E-Mail-Adresse. Mehr Informationen dürfte ein Shop laut Bundesdatenschutzgesetz (siehe Kasten rechts) auch gar nicht verlangen. Nur die persönlichen Daten darf er erheben, die für seine Geschäftszwecke benötigt werden. Ein Foto ist dafür ebenso überflüssig wie die Angabe von Hobbies. Das hindert freilich niemanden daran, freiwillig noch mehr über sich preiszugeben. Je besser ein Unternehmen Sie kennt, desto zielgenauer kann Werbung auf Sie ausgerichtet werden.

## Wieso liegt mein Kreditscore nicht bei 100%?

Sie möglichst genau zu kennen, ist auch das Geschäft von Auskunftsteilen und Adresshändlern außerhalb des Internets. Die Schufa etwa lebt davon, Ihre Kreditwürdigkeit einschätzen zu können. Deswegen verraten Banken dem Unternehmen, wann Sie ein Konto eröffnet haben, welche Kredite Sie aufgenommen haben und wie zuverlässig Sie die Raten bedienen – dem haben Sie mit der Vertragsunterschrift bei Ihrer Bank zugestimmt. Ihre Kreditwürdigkeit ergibt sich neben Ihrem individuellen Verhalten aber auch aus aggregierten Daten. Ein Beispiel: Ich selbst habe mir nie etwas zuschulden kommen lassen, trotzdem liegt mein Kreditscore nicht beim Maximalwert von 100% – schließlich gibt es andere Münchner, die seit zehn Jahren ein Girokonto besitzen und schon einmal säumig waren. Das senkt auch mein Ranking. „Wir betreiben aber kein Geo-Scoring und nutzen auch keine



## DAS DATENSCHUTZGESETZ SCHÜTZT NICHT IMMER

### WELCHE DATEN WERDEN GESPEICHERT?

#### Diese Daten dürfen gespeichert werden:

- Alle Daten, die Unternehmen oder Behörden für ihre Aufgaben und Geschäftszwecke benötigen
- Alle Daten, die Betroffene freiwillig angeben
- Alle Daten, die öffentlich zugänglich sind oder die Betroffene selbst veröffentlicht haben, auch im Internet
- Alle Daten, die für Forschungszwecke benötigt werden

#### Der Handel mit und Austausch von Daten ist erlaubt:

Diese Daten dürfen Behörden frei untereinander tauschen, sofern sie das für ihre Aufgaben benötigen. Auch Unternehmen dürfen Daten austauschen, wenn dies für ihre Geschäfte erforderlich ist, zum Beispiel an Firmen, die professionell Daten verarbeiten.

### WELCHE DATEN SIND WIE GESCHÜTZT?

#### Besondere personenbezogene Daten sind stark geschützt:

- Ethnische Herkunft
- Politische und religiöse Überzeugung
- Gewerkschaftszugehörigkeit
- Daten, die die Gesundheit betreffen
- Sexualleben

#### Diese personenbezogenen Daten sind nicht besonders geschützt:

- Alle persönlichen und sachlichen Informationen zu einer Person, zum Beispiel Name, Adresse, Geburtstag, Einkommen, Haustiere und ähnliche Informationen.

### WANN MÜSSEN DATEN GELÖSCHT WERDEN?

- Wenn sie nachweislich falsch sind
- Wenn der Betroffene seine Einwilligung widerruft
- Wenn sie keiner Aufgabe oder keinem Geschäftszweck mehr dienen

### SONDERFÄLLE

#### Besondere personenbezogene Daten

- Dürfen ohne Einwilligung nur zur Gefahrenabwehr, Straftatenverfolgung, Landesverteidigung zum Schutz von Leben, für gesundheitliche oder juristische Zwecke, wichtige Forschungszwecke oder wenn internationale Abkommen es fordern, gespeichert und übermittelt werden
- Behörden dürfen sie zudem zur Erledigung ihrer Aufgaben speichern, etwa, um die Kirchensteuer zu berechnen

#### Auskunftsteien (z. B. Schufa)

- Dürfen Positivmeldungen etwa über ordentlich bezahlte Kredite jederzeit speichern
- Dürfen Negativmeldungen hingegen nur nach zweimaliger Mahnung und anschließendem Warnhinweis speichern
- Müssen erledigte Sachverhalte (z. B. bezahlte Schulden) nach maximal vier Jahren wieder löschen

#### Adresshändler

- Dürfen ohne Einwilligung Daten aus öffentlichen Quellen erheben und weitergeben
- Dürfen Personenlisten aus Name, Adresse, Alter und Beruf erstellen und weitergeben, also zum Beispiel eine Liste aller Zahnärzte zwischen 30 und 40 Jahren in Bayern







**Nur im Oktober 2012!**  
Bestellungen nach dem  
31.10.2012 können leider nicht  
mehr berücksichtigt werden.

# Mehr Geschwindigkeit Homepage Dynamic

## 1blu-Homepage „Dynamic“

- > 2 Inklusiv-Domains
- > 20.000 MB Webspace
- > Unbegrenzter Traffic
- > 20 MySQL-Datenbanken
- > 750 E-Mail-Adressen, 45 GB Speicher
- > Unbegrenzte FTP-Accounts
- > Joomla, Wordpress, Typo3  
uvm. vorinstalliert
- > PHP5, Perl, Python, SSI, SSH
- > 24/7-Technik-Hotline
- > Keine Einrichtungsgebühr

**3,69**  
€/Monat\*

**Preis gilt dauerhaft!**

Webhosting für Profis – Die 1blu-Homepage „Dynamic“ bietet Ihnen garantierte Bandbreite für starke Website-Performance, ein eigenes SSL-Zertifikat und unbegrenzten Traffic. Erhältlich ist das Produkt zum Dauerpreis von 3,69 €/Monat\* nur bis Ende Oktober 2012!

**+** Tolle Website-Performance durch  
10 Mbit/s Bandbreiten-Garantie!

**+** Eigenes SSL-Zertifikat inklusive!

\* Preis/Monat inkl. 19% MwSt. Angebot verfügbar ab Anfang Oktober 2012 (Näheres unter [www.1blu.de/dynamic](http://www.1blu.de/dynamic)). Es fällt keine Einrichtungsgebühr an. Vertragslaufzeit jeweils 6 Monate, jederzeit kündbar mit einem Monat Frist zum Vertragsende. Bei Software-Bestellung 7,90 € Versandkosten.

\*\* Preis/Monat inkl. 19% MwSt. Einrichtungsgebühr 1blu-Drive jeweils einmalig 9,90 € bei einer Vertragslaufzeit von 1 Monat, keine Einrichtungsgebühr bei einer Vertragslaufzeit von 12 Monaten. Verträge jeweils jederzeit kündbar mit einem Monat Frist zum Vertragsende.



## 1blu-Drive

- > Ihre Daten in der Cloud!
- > Komfortabler Online-Speicher
- > 25 GB nur **1,90 €/Monat\*\***  
[www.1blu.de/drive](http://www.1blu.de/drive)

nur unter **[www.1blu.de/dynamic](http://www.1blu.de/dynamic)**  
030 - 20 18 10 00

biologischen Daten“, betont Schufa-Sprecher Andreas Lehmann. Gemeint ist eine Praxis, die andere Wirtschaftsauskunfteien durchaus pflegen: Da wird Kreditwürdigkeit anhand des Wohnortes, Geschlechts oder Alters geschätzt. Wer im Nobelviertel lebt, bekommt demnach eher einen Kredit als ein Student in einem heruntergekommenen Stadtteil, in dem viele Schuldner wohnen. Solche Geo- und Biodaten sind wiederum auch für Adresshändler interessant. Diese bündeln Menschen zu homogenen Gruppen und verkaufen deren Namen und Adressen an Unternehmen, die wiederum Werbung verschicken – etwa an alle Zahnärzte Bayerns zwischen 30 und 40 Jahren.

Woher stammen diese Daten? Zunächst einmal aus allen öffentlichen Quellen, angefangen beim Telefonbuch. Theoretisch dürfte auch Ihr Facebook-Profil genutzt werden – eine Studie, inwieweit sich dortige Angaben überhaupt sinnvoll nutzen lassen, brach die Schufa aber nach großen Protesten im Frühjahr wieder ab. Dazu kommen eingekaufte Daten, etwa über Preisausschreiben und Gewinnspiele. Wer an solchen Stellen sparsam mit seinen Daten umgeht, der ist den Adresshändlern weitestgehend unbekannt. Auch das hat der Selbsttest gezeigt.

## Der Staat agiert oft am Rande der Legalität

Am erlaubten Datenhandel beteiligt sich auch der Staat: Der Verkauf von Namen, Adressen und Doktorgraden brachte Deutschlands 35 größten Kommunen 2011 rund 12 Millionen Euro ein. Doch die Behörden wissen noch weit mehr: Das Finanzamt kennt Ihr Einkommen, das Arbeitsamt Ihren Lebenslauf, die Krankenkasse kann aus Ihren Arztbesuchen Rückschlüsse auf Ihre Gesundheit ziehen, Polizei, Staatsanwaltschaft und Gerichte speichern Ihre Fehlritte. Diese Daten haben Sie meist zwangsweise abgegeben, sie dürfen zudem unter den Behörden frei getauscht werden, wenn das für ihre Aufgaben nötig ist. Dabei können Ihre Daten sogar über den Atlantik wandern. Die USA dürfen im Rahmen des SWIFT-Abkommens Ihre Kontobewegungen einsehen und müssen das nicht einmal vor Ihnen verantworten. Und die Heimatschutzbehörde Homeland Security sammelt bei der Urlaubseinreise in die USA Fotos und Fingerabdrücke. „Oftmals schwierig“, sei es da, sagt Juliane Heinrich, Pressesprecherin des Bundesdatenschutzbeauftragten, „auf einen angemessenen Ausgleich zwischen Sicherheitsinteressen und Datenschutz hinzuwirken.“ Im Selbsttest reagierte zumindest das Department of Homeland Security. Wer eine beglaubigte Ausweiskopie einsendet, bekommt Einblick in die gespeicherten Daten.

Auch hiesige Ermittlungsbehörden dürfen beim Datensammeln sehr weit gehen, vor allem, wenn ein konkreter Verdacht besteht. So fragte die Berliner Polizei in den vergangenen vier Jahren 1.408 Mal Funkzellen ab. In dem Fall müssen Provider der Behörde die Datensätze aller Handys geben, die zu einem bestimmten Zeitpunkt in einer bestimmten Mobilfunkzelle eingeloggt waren. 6,6 Millionen Datensätze wurden in Berlin erhoben, nur 5.383 davon für Ermittlungszwecke benötigt. Bisher müssen Unschuldige, deren Daten auf diese Weise erhoben wurden, nicht darüber benachrichtigt werden. Wie ein dystopisches Big Brother wirkt gar das Forschungsprojekt Indect der EU – hier würden über Kameras sogar Mimik und Verhalten aufgenommen und gespeichert, um daraus Rückschlüsse auf künftige Straftaten ziehen zu können. Dass das Projekt aber jemals in geltendes Recht umgesetzt wird, ist derzeit unwahrscheinlich. Mit dem deutschen Grundgesetz wäre es in seiner jetzigen Form jedenfalls nicht vereinbar. Bis Ende 2013 wird noch an Indect geforscht, federführend ist die Universität Krakau.

Machtlos sind Sie gegen die Datensammler allerdings nicht – egal ob es sich um Privatunternehmen oder Behörden handelt.



## DATENSAMMLER STOPPEN

Viele Daten werden ohne Ihr Wissen über Sie gesammelt. CHIP zeigt Ihnen, wie Sie das mit einfachen Mitteln verhindern können

### ... BEI GEWINNSPIELEN IM INTERNET

Preisausschreiben werden in den meisten Fällen dazu genutzt, Ihnen Ihre Daten zu entlocken, um diese an Werbefirmen weiterzuverkaufen. Die beste Methode, das zu verhindern: Nicht teilnehmen.



### ... BEI DER WEBSUCHE

Anonyme Suchmaschinen wie ixquick.de **1**, duckduckgo.com **2**, gibiru.com **3** oder metager2.de **4** speichern bei Suchanfragen keine persönlichen Informationen wie IP-Adressen.



### ... BEIM SURFEN



**HideMan** ist ein kommerzieller VPN-Client, der den Internetverkehr über einen Proxy-Server umleitet und so die Identität verschleiert. CHIP-Leser surfen damit exklusiv acht Stunden pro Woche gratis.



**PrivitizeVPN** von The Pirate Bay leitet die Verbindung über einen schwedischen Server um. Das Tool ist zwar gratis, dafür aber langsam und mit Werbung (Download unter [chip.de](http://chip.de)).



**TOR** (The Onion Router) verbindet zahlreiche Nutzer zu einem Anonymisierungsnetzwerk. Wer das Tool nutzt, wird beim Surfen über mehrere Knoten umgeleitet – die IP-Adresse bleibt so geheim.

### ... BEIM EINKAUFEN IM SUPERMARKT

Um beim analogen Shoppen anonym zu bleiben, sollte man auf jeden Fall auf Vorteilskarten wie Payback oder DeutschlandCard verzichten: Sie spionieren das Konsumverhalten ihrer Besitzer aus.





Fujitsu empfiehlt Windows® 7.



shaping tomorrow with you

# Das schlankeste 14-Zoll-Notebook der Welt

[lifebook.de.ts.fujitsu.com](http://lifebook.de.ts.fujitsu.com)



## Fujitsu LIFEBOOK U772 Ultrabook™ – Erleben Sie Design kombiniert mit professioneller Leistung

### LIFEBOOK

mit der 3. Generation der Intel® Core™ vPro™  
Prozessorfamilie – Bereichert Ihr Leben.

- Intel® Core™ i7 vPro™ Prozessor
- Windows® 7 Home Premium 64-Bit
- Empfohlenes Upgrade zu Windows® 7 Professional
- inkl. 256 GB SSD
- Ultimative Konnektivität mit integriertem WLAN, Bluetooth und 4G/LTE
- Standortunabhängiges, ergonomisches Arbeiten dank Antiglare-Display, HDMI-Schnittstelle, HD-Webcam und optionaler Docking Station



**Kaufen Sie einen Windows 7-PC und  
erhalten Sie Windows 8 Pro für nur 14,99 €.**

Dieses Angebot ist ab dem 2. Juni 2012 bis zum  
31. Januar 2013 gültig. Ausführliche Informationen  
finden Sie unter [windowsupgradeoffer.com](http://windowsupgradeoffer.com).

# 1.499,- €\*

Bestellcode: VFY:U7720M27S1DE

\* Unverbindliche Preisempfehlung inkl. MwSt. Preise, Liefermöglichkeiten, technische Änderungen und Irrtümer vorbehalten. Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller. Produktabbildungen ähnlich. Dieses Angebot ist gültig bis zum 31. Oktober 2012. Die in diesem Dokument wiedergegebenen Bezeichnungen können Marken sein, deren Benutzung durch Dritte für eigene Zwecke die Rechte der Inhaber verletzen kann.

Überall  
einfacher arbeiten



# WIE behalte ich die Kontrolle?

Ihre Daten gehören immer noch Ihnen. Sie können sie einsehen, korrigieren und auch löschen lassen

Sind Ihre Daten einmal im Umlauf, können Sie nichts mehr dagegen unternehmen – vergessen Sie diesen Spruch. Das Bundesdatenschutzgesetz gibt Ihnen weitgehende Kontrolle über Ihre Daten. Mehr als Sie vielleicht denken. Das beginnt mit einem simplen Auskunftsrecht. Einmal im Jahr muss Ihnen jedes Unternehmen und jede Behörde auf Anfrage mitteilen, welche Daten über Sie gespeichert sind, woher diese stammen und was mit diesen Daten geschieht. Wie Sie dieses Auskunftsrecht am besten geltend machen, verraten wir im Kasten rechts. Die Reaktionen der verschiedenen Stellen in unserem Selbsttest sind unterschiedlich. Positivstes Beispiel ist wohl Amazon. Der Online-Händler brauchte zwar einige Wochen für die Bearbeitung, schickte dann aber ein dickes Paket Akten, das unter anderem jeden einzelnen Bestellvorgang umfasste, inklusive Produkt, Preis und Bestellnummer. Den Mailverkehr mit dem Kundensupport schickt der Versandhändler auf Wunsch nach. Auch die Schufa sandte auf Anfrage eine komplette Auskunft über die Scorewerte und ihre Zusammensetzung – diesen Service bietet die Auskunft aus Kulanz sogar mehr als einmal pro Jahr an. Praktisch: Das Auskunftersuchen ist kostenlos und inhaltlich nahezu deckungsgleich mit der Schufa-Bonitätsauskunft, die sonst 18,50 Euro kostet. Google hat für den Datenschutz einen Online-Service: Über das Dashboard (unter [google.com/dashboard](http://google.com/dashboard)) lässt sich einsehen, welcher Google-Dienst welche Daten gespeichert hat. Schwieriger liegt der Fall bei Behörden: Hier ist es wichtig, den Fragesteller eindeutig zu identifizieren, weswegen beglaubigte Kopien des Personalausweises angefordert werden.

## Unternehmen rücken nicht alles raus

Doch auch damit kommen Sie nicht überall weiter. Ein Auskunftersuchen ist etwa bei manchen amerikanischen Behörden fruchtlos: Welche Kontobewegungen zum Beispiel über das internationale Bankenabkommen SWIFT mitgelesen wurden, werden Sie nie erfahren: Die zuständige Behörde verweigert die Auskunft. Das darf sie, weil sie in den USA sitzt und damit nicht dem Bundesdatenschutzgesetz unterliegt. Generell gilt, dass Ihre Daten im Ausland weniger geschützt sind als hierzulande – ein Punkt, den man etwa bei der Nutzung von Cloud-Diensten bedenken sollte. Gerade in den Vereinigten Staaten verlangen Geheimdienste regelmäßig Zugriff auf die privaten Accounts der Nutzer.

Fraglich ist auch, ob Sie wirklich immer alle Daten erhalten, die über Sie gespeichert sind. Google etwa weist in seinem ansonsten tadellosen Dashboard darauf hin, dass Server Logs, Cookies und die Interessen, nach denen einem Werbung zugeordnet wird, geheim bleiben. Facebook stellte mir zwar ein 82 MByte großes Archiv zum Download bereit, das enthielt aber nur, was in meinem Profil sichtbar war – und nicht etwa meine versandten Nachrichten. Bei Apple



## SO NUTZEN SIE IHR AUSKUNFTSRECHT

→ Einmal pro Jahr muss Ihnen jede Behörde und jedes Unternehmen Auskunft darüber geben, welche Daten über Sie gespeichert sind und an wen sie weitergegeben wurden.

→ Um dieses Recht einzufordern, schicken Sie am besten einen Brief an die betreffende Stelle. Zur eindeutigen Identifikation sollte eine Kopie Ihres Personalausweises beiliegen.

→ Stellen wie das Bundeskriminalamt, die sehr sensible Daten über Sie gespeichert haben könnten, fordern sogar eine amtlich oder polizeilich beglaubigte Kopie Ihres Personalausweises. Die erhalten Sie für fünf Euro in der nächstgelegenen Polizeiwache oder dem nächsten Bürgeramt.

→ Im Anschreiben ist unbedingt auf den Paragraphen 34 des Bundesdatenschutzgesetzes (BDSG) hinzuweisen, aufgrund dessen Sie die Auskunft verlangen. Eine Gebühr dafür darf Ihnen nicht berechnet werden, außer natürlich dem Porto für die ersuchte Antwort.

→ Manche Stellen, etwa die Schufa, erlauben darüber hinaus auch mehrere kostenlose Anfragen pro Jahr. Online-Unternehmen wie Facebook, Google und Amazon bieten die Datenauskunft auch online an. Bei Amazon reicht es zum Beispiel schon, den Kundensupport anzuschreiben.

→ Damit Sie kein Unternehmen vergessen und sich lästiges Briefeschreiben sparen, gibt es Online-Generatoren wie [selbstauskunft.net](http://selbstauskunft.net) und [datenschmutz.de](http://datenschmutz.de) ([datenschmutz.de/cgi-bin/auskunft](http://datenschmutz.de/cgi-bin/auskunft)), die auch die passenden Adressen eintragen.




fehlt eine Auskunft über die heruntergeladenen Apps. Behörden wie Polizei und Verfassungsschutz müssen Sie zudem nicht darüber informieren, ob und wann gegen Sie ermittelt wurde. Gibt es Anhaltspunkte, dass nicht alle gespeicherten Daten offengelegt wurden, können Sie mithilfe eines Anwalts eine eidesstattliche Versicherung erwirken. Damit versichert die betroffene Stelle, Ihnen alle Daten gegeben zu haben. Eine falsche Versicherung wäre strafbar. Datenjäger können also lästig werden. Verweigern darf sich dem aber zumindest keine deutsche Stelle. „Das ist eine Ordnungswidrigkeit, bei der Sie sich an den Landesdatenschutzbeauftragten wenden können“, sagt Rechtsanwalt Florian Decker. Der kann ein Bußgeld von bis zu 50.000 Euro verhängen.

## Falsche Daten müssen korrigiert werden

Ihre Rechte enden aber nicht mit der Auskunft. Stellen Sie zum Beispiel fest, dass die über Sie gespeicherten Daten nachweislich falsch sind, muss das Unternehmen oder die Behörde diese korrigieren – vom falsch geschriebenen Namen bis zum zu Unrecht aufgeführten Negativeintrag bei der Schufa. Gelöscht werden müssen alle Daten, die für Aufgaben nicht benötigt werden – also etwa Ihre Kontoverbindung, die Sie bei Amazon nicht mehr nutzen. Manche Daten sind dabei besonders schützenswert und dürfen ohne Ihre Einwilligung gar nicht erst erfragt werden. Dazu gehören die religiöse Überzeugung, sexuelle Orientierung oder die Gewerkschaftszugehörigkeit.

Daten dürfen zudem nicht endlos über Sie gespeichert werden, selbst wenn sie noch nötig sein könnten. Die Schufa und andere Wirtschaftsauskunfteien müssen etwa Negativeinträge nach maximal vier Jahren löschen, wenn sich der Sachverhalt erledigt hat, Sie also etwa die angemahnten Schulden bezahlt haben. Ein Ende aller Datenspeicherung bedeutet nicht einmal der Tod eines Menschen. Gerade Privatunternehmen erfahren nur selten vom Tod ihrer Kunden: Wer denkt schon beim Tod eines Angehörigen daran, dessen Google-Account abzumelden? So löschen Firmen die Daten ihrer gestorbenen Kunden erst, wenn Angehörige dies beantragen. Im Regelfall ist dafür ein Nachweis verantwortlich. Verpflichtet dazu sind sie kurioserweise nicht: „Die Daten Verstorbener unterliegen nicht dem Bundesdatenschutzgesetz“, so Juliane Heinrich. Behörden informieren sich gegenseitig vom Tod eines Bürgers – das heißt aber nicht, dass sofort alle Daten über diese Person gelöscht werden. Und das hat handfeste Gründe: „Gelöscht werden Daten bei uns erst dann, wenn daraus keine Ansprüche mehr entstehen können“, sagt Andreas Feuser, Pressereferent der Rentenversicherung. Gemeint ist etwa die Witwenrente, die sich aus Einzahlungen des Verstorbenen berechnet. Missgeschicke wie GEZ-Mahnungen an Tote lassen sich bei der Langzeitspeicherung offenbar nicht ausschließen.

## Datenschutz: Bürger fragen mehr nach

Wer nicht aufpasst, dessen Daten können also wortwörtlich unsterblich werden. Um dem entgegenzuwirken, möchte etwa EU-Kommissarin Viviane Reding ein „Recht auf Vergessen“ im Internet einführen. Derzeit reicht es zum Beispiel nicht, den Facebook-Account einfach abzumelden – er bleibt danach noch für mehrere Monate auf den Servern des Netzwerks bestehen. Sie könnten Ihren Entschluss ja noch bereuen und zurückkehren. Bisher hat der Staat keine Handhabe gegen solche Praktiken. Diese Ohnmacht gegenüber globalen Konzernen müsse beseitigt werden, sagt Juliane Heinrich. Sie setzt dabei vor allem auf die gestiegene Sensibilität der Bürger: Von 2008 bis 2010 stieg die Zahl der Datenschutzanfragen beim Bundesbeauftragten um rund 47 Prozent – und damit auch die Aussicht auf noch viele überfüllte Briefkästen.  CHRISTOPH SACKMANN, AUTOR@CHIP.DE



**Gefällt Ihnen dieser Artikel?**

Teilen Sie ihn mit Freunden! Anleitung auf Seite 10

# SO BEHALTEN SIE IHRE DATEN

## TRACKING VERHINDERN



**Ghostery** ist eines der beliebtesten Anti-Tracking-Tools. Die Erweiterung, die es für alle gängigen Browser gibt, blockt erfolgreich Werbe-, Analyse- und Tracking-Elemente, die sich auf vielen Seiten verbergen.



**Kill-ID** für Chrome entfernt die eindeutige Identifikationsnummer aus Googles Analyse-Browser. So verrät dieser zukünftig nichts mehr über das Surfverhalten des Nutzers an den Suchmaschinenbetreiber.



**NoScript** ist ein Add-on für Mozilla-basierte Browser, das – außer auf vertrauenswürdigen Webseiten – alle JavaScript-, Java- und Flash-Plug-ins blockt, um so vor möglichen Angriffen zu schützen.

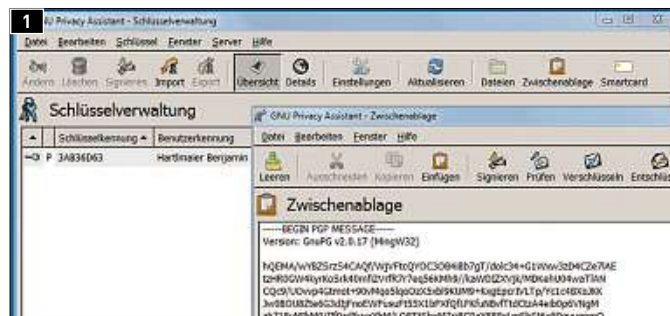


**Collusion** für Firefox ist ein experimentelles Add-on, das beim Surfen alle Spionage-Aktivitäten, die im Hintergrund ablaufen, grafisch darstellt.

**Achtung:** Geht nur mit deaktivierten Anti-Tracking-Tools!

## E-MAILS VERSCHLÜSSELN

Wer sicherstellen will, dass selbst Polizei oder Geheimdienste nicht mitlesen, kann mit PGP (Pretty Good Privacy) E-Mails sicher verschlüsseln. Empfehlenswert sind die auf dem offenen PGP-Standard GnuPG basierenden Programme Gpg4win **1** und Enigmail **2**, ein Add-on für Mozillas Mailclient Thunderbird.



## SENSIBLE DATEN SCHÜTZEN

**TrueCrypt** (Open-Source), verschlüsselt Verzeichnisse, externe Laufwerke oder ganze Festplatten (Download unter [chip.de](http://chip.de)).

**BoxCryptor** kodiert Ihre Daten vor dem Hochladen in die Cloud mit einer 256-Bit-Verschlüsselung. Zwei GByte sind gratis.

**PeaZip** öffnet seltene Archivdateien und packt Daten sicher in kodierte Archive mit Passwort und Keyfile (Download unter [chip.de](http://chip.de)).

## DEUTSCHE CLOUDANBIETER NUTZEN



**Die Deutsche Telekom** bietet unter dem Namen Telekom-Cloud einen Online-Speicher mit zahlreichen Funktionen an. Die Server stehen ausschließlich in Deutschland.



**Strato** verspricht für sein HiDrive TÜV-geprüfte Datensicherheit. Die Clouddaten liegen in Berlin und Karlsruhe und fallen somit unter das deutsche Datenschutzrecht.



**1&1** stellt Online-Speicher über seine beiden E-Mail-Dienste WEB.DE und GMX bereit. Die Server der beiden annähernd identischen Cloudangebote stehen in Deutschland.



Die meisten Tools finden Sie auf der Heft-DVD.  
CHIP-Code: SECURITY