

Meine Daten = Deine Daten? – Denkste!

„Datenklau“ ist derzeit eines der meist benutzten Wörter in den Medien. Viele Bürgerinnen und Bürger haben den Eindruck, ihre persönlichen Daten seien wie zum fast beliebigen Verhökern freigegeben und suchen Hilfe bei der Landesbeauftragten für den Datenschutz. Die aktuelle Debatte um legalen und illegalen Verkauf persönlicher Daten, um Missbrauch von Informationen aus Call Centern oder umstrittenen Telefongeschäften bis hin zur Plünderung privater Konten durch Kriminelle, die sich ungesetzlich erworbener Bankdaten bedienen – dies alles und mehr beunruhigt Verbraucherinnen und Verbraucher. Lesen Sie hier unsere Sammlung nützlicher Informationen und Tipps, wie Sie selbst ihre persönlichen Daten besser schützen – und sich gegen schmutzige Tricks der Datenhändler wehren können.

– Wer sagt mir eigentlich, welche Daten über mich in irgendwelchen Datenbanken liegen?

Tja, auf diese Frage gibt es eine gute und eine „schlechte“ Antwort. Die gute ist diese: Das geltende Datenschutzrecht garantiert grundsätzlich allen Bürgerinnen und Bürgern einen Anspruch auf Auskunft über gespeicherte Daten sowie auf Berichtigung, Sperrung oder Löschung ihrer Daten. Die „schlechte“ Nachricht: Welche Behörde, Institution oder Firma welche Daten über Einzelne gespeichert hat, muss leider aufwendig in jeweils einzelnen Schreiben abgefragt werden; immerhin aber gibt es dafür [hier](#) vorbereitete Musterbriefe mit ausführlichen Anleitungen.

– Dürfen Firmen oder Behörden einfach meine Daten speichern und weitergeben?

„Einfach“ dürfen die das nicht, die Datenverarbeitung (hierzu gehören u. a. die Datenspeicherung und Datenübermittlung) ist streng geregelt. Die einschlägigen Gesetze [des Bundes](#) und des [Landes Bremen](#) nennen aber viele Gründe, wann und warum Speicherung und Verarbeitung persönlicher Daten zulässig sein können. Oft müssen die Betroffenen über eine Speicherung ihrer Daten nicht gesondert unterrichtet werden, weil davon ausgegangen wird, dass sie es bereits wissen oder damit rechnen müssten. Das ist häufig ein Problem: Viele Verbraucherinnen und Verbraucher erteilen Firmen die Erlaubnis zur Speicherung oder Weitergabe ihrer Daten, ohne es wirklich zu wollen – etwa, indem sie „Kleingedrucktes“ in Verträgen nicht sorgfältig lesen und so mehr oder weniger versteckte Einwilligungen unterschreiben. Das Gesetz gestattet es beispielsweise, für Werbezwecke Datenpakete mit Name, Anschrift, Geburtsjahr und Zugehörigkeit zu einer Personengruppe weiterzugeben – wenn die Betroffenen dem nicht widersprechen. Datenschützer fordern seit langem, solche Geschäfte von der ausdrücklichen vorherigen Zustimmung der Betroffenen abhängig zu machen, bislang leider vergeblich. Zudem haben gerade die Datenschutzskandale im Sommer 2008 gezeigt, dass es darüber hinaus einen unüberschaubaren Markt illegalen Datenhandels gibt.

– Woher haben Einrichtungen, die ich manchmal selbst gar nicht kenne, meine Daten?

Zunächst einmal: Gegen illegale Praktiken beim Umgang mit persönlichen Daten gibt es keinen umfassenden Schutz. Aber es gibt eben auch viele legale Fallen, in die Verbraucherinnen und Verbraucher allzu leicht tappen können: Wer etwa an einem Preisausschreiben oder einer Verlosung teilnimmt, wer eine Rabatt- oder Kundenkarte

beantragt hat, wer allzu sorglos im Internet Geschäfte tätigt, an Umfragen oder Onlinespielen teilnimmt oder Auskünfte erteilt, der trägt sehr oft selbst dazu bei, dass einzelne Daten über ihn gesammelt werden oder auch öffentlich abrufbar sein können. Und Daten, die einmal bei entsprechenden Händlern oder im Internet kursieren, sind in der Regel für Betroffene nicht mehr zu kontrollieren.

– Warum können Datenschützer solche Praktiken nicht stoppen?

Illegale Praktiken des Datenhandels finden in einer riesigen Grauzone statt, in der zum Teil legal erhobene Daten mit anderen durch kriminelle Methoden zu einem äußerst gewinnträchtigen Handelsnetz verknüpft werden. So ist zwar unerwünschte Telefonwerbung ebenso ungesetzlich wie etwa der aktuell aufgeflogene Handel mit Kontodaten – aber Datenschützer plädieren seit langem für weiter reichenden Schutz Betroffener: ausdrückliche Zustimmung zur Datenweitergabe und anderes mehr. Völlig machtlos aber sind die Datenschützer ebenso wie der Gesetzgeber, wenn Verbraucherinnen und Verbrauchern selbst leichtfertig ihre Daten preisgeben: Wer sich in Formularen, Fragebögen, im Internet oder bei Onlinespielen „entblößt“, den kann keine Behörde vor Missbrauch seiner Daten bewahren. Im Übrigen können die nur mit gering personellen Mitteln ausgestatteten Datenschutzbeauftragten nicht einmal ansatzweise die Einhaltung der Datenschutzregelungen prüfen.

– Was kann ich denn tun, um meine Daten wenigstens künftig zu schützen?

Die Sorgfalt im Umgang mit den eigenen Daten wird wegen der Auswüchse des Datenhandels immer wichtiger. Das Dumme daran ist, dass solche Sorgfalt oft nicht nur Zeit kostet, sondern häufig auch mit Unbequemlichkeiten verbunden ist. Einfach mal

eben Adresse, Telefonnummer, E-Mail-Kontakt oder auch Kontodaten mitzuteilen oder einzugeben, erleichtert nicht nur viele Vorgänge, sondern macht sie manchmal sogar billiger. Klar: Denn solche Daten können auch für Einrichtungen, die legal handeln, bares Geld sein – und für illegal arbeitende erst recht. Verbraucherinnen und Verbraucher sollten mindestens mit ihren Konto- und Kreditkartendaten sowie mit Telefon- und Handynummern äußerst zurückhaltend umgehen. Es empfiehlt sich weitere Mail-Adressen für Bestell- oder Infozwecke einzurichten, um die persönliche Adresse besser zu schützen. Dies ist einfach und meist kostenlos. Auch der Umfang des Eintrags im Telefonbuch sollte überdacht werden. Ebenso sollte mit Angaben über Alter, Beruf, Hobbys oder Freunde zurückhaltend umgegangen werden. Zudem sollte immer darauf geachtet werden, dass nicht versehentlich einer Weitergabe der Daten an Dritte zugestimmt wird. Die Datenschützer des Bundes und des Landes Bremen halten eine Vielzahl von Tipps bereit und, was Bürgerinnen und Bürger tun können, wenn sie einen Missbrauch ihrer Daten vermuten ([Tipps vom BfDI](#) – [Tipps vom LfDI Bremen](#)).

– Dürfen Verträge oder Geschäfte gekoppelt werden an eine Preisgabe von Daten?

Immer häufiger finden sich nicht nur bei Internet-Geschäften, sondern auch in normalen Kauf- oder Dienstleistungsverträgen Klauseln, in denen vom Kunden Daten abgefragt werden und häufig auch deren Verarbeitung oder Weitergabe durch Kreuzchen oder Unterschrift zugestimmt werden soll. Oft wird sogar das Zustandekommen des Vertrages hiervon abhängig gemacht. Hier helfen nur erhöhte Wachsamkeit der Kundinnen oder Kunden, das genaue Studium der Verträge und das Gespräch mit dem Geschäftspartner, die Frage, warum denn diese oder jene Daten für den gewünschten Kauf nötig sein sollen. Ein Möbelhändler beispielsweise braucht keine Kundenangaben

über Geburtstag oder Beruf, um einen Schrank zu liefern! Im äußersten Falle sollten Verbraucherinnen und Verbraucher auch mal bereit sein, auf ein Geschäft zu verzichten, wenn der Datenhunger des Vertragspartners allzu unsinnig erscheint. Doch Vorsicht: Eine Einwilligung zur Datenweitergabe etwa an die SCHUFA zur Bonitäts-Überprüfung kann ein Geschäftspartner verlangen. Unmittelbar hat das nichts mit Werbung zu tun – häufig werden aber gerade in diesbezüglichen Klauseln pauschale Einwilligungserklärungen versteckt!

– Kann ich denn meine bereits verfügbaren Daten irgendwie pauschal blockieren?

Es gibt hier einen begrenzten Schutz – die so genannten Robinson-Listen. Unter der Internetadresse www.robinson-liste.de können Verbraucherinnen und Verbraucher sich informieren, wie sowohl ihre Postanschrift als auch ihre Faxnummern sowie Mail-Adressen und Telefon- oder Handynummern für Werbesendungen oder -anrufe gesperrt werden können. Das Verfahren ist dort anschaulich beschrieben – es ist kostenlos und die Sperre gilt unbegrenzt bis zum Widerruf durch den Betroffenen; lediglich bei Postanschriften ist alle fünf Jahre eine Aktualisierung nötig. Die Sache hat nur einen kleinen Haken: Datenhändler und Werbetreibende, die ihre Datenbanken mit diesen Robinson-Listen abgleichen, sind nicht zwingend verpflichtet, die Einträge zu berücksichtigen – zwar tun es die meisten, aber schwarze Schafe gibt es in jeder Branche; zudem gilt dieses Verfahren nur in Deutschland, das Geschäft mit dem Datenhandel aber ist international.

Wer vermeiden möchte, dass Dritte seine Telefonnummer oder Anschrift über das gedruckte oder elektronische Telefonbuch erfahren oder das die Auskunft diese

herausgibt, sollte hiergegen bei seinem Netzbetreiber Widerspruch einlegen. Dieses Recht kann jederzeit mit Wirkung für die Zukunft wahrgenommen werden.

Möglichkeiten für den Betroffenen, der Übermittlung seiner Daten an Privatpersonen oder nicht öffentliche Stellen zu widersprechen, ergeben sich auch aus den Bestimmungen des Einwohnermelderechts. Liegen Tatsachen vor, welche die Annahme rechtfertigen, dass dem Betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann, hat die Meldebehörde auf Antrag oder von Amts wegen eine Auskunftssperre im Melderegister einzutragen. Eine Melderegisterauskunft ist in diesen Fällen unzulässig, es sei denn, dass nach Anhörung des Betroffenen eine Gefahr für die genannten schutzwürdigen Belange ausgeschlossen werden kann. Die Auskunftssperre endet mit Ablauf des zweiten auf die Antragstellung folgenden Kalenderjahres; sie kann auf Antrag verlängert werden.

Besondere Widerspruchsrechte bestehen im Hinblick auf die Erteilung von Melderegisterauskünften an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlamentswahlen, zu Alters- oder Ehejubiläen und in Bremen auch an Adressbuchverlage. Der Betroffene kann der Übermittlung seiner Daten in diesen besonderen Fällen jederzeit und ohne Grund bei der Meldebehörde widersprechen. Auf die Möglichkeit des Widerspruchs ist der Betroffene entsprechend der gesetzlichen Vorgaben hinzuweisen.

– Ich erhalte oft Anrufe mit irgendwelchen Werbeangeboten. Muss ich das hinnehmen?

Nein. Die Rechtslage ist nach geltendem Wettbewerbsrecht sowie der Rechtsprechung des Bundesgerichtshofes (BGH, NJW 2000, 2677) eindeutig: Nur wenn Betroffene ausdrücklich eingewilligt haben, dürfen sie angerufen werden. Und diese Zustimmung muss vor dem Anruf erfolgt sein – es genügt nicht, wenn der Werbetreibende sie zu Beginn des Gesprächs abzufragen versucht! Das Problem ist eben nur, dass viele Menschen eine solche Einwilligung erklärt haben, ohne es eigentlich zu wollen: Sie brauchen nur entsprechende Hinweise in Verträgen oder Preisausschreiben übersehen zu haben.

– Wie verhalte ich mich bei solchen unerwünschten Werbe-Anrufen?

Kommentarlos den Hörer aufzulegen, hilft leider nur kurzfristig – häufig folgen dann in den nächsten Tagen oder Wochen weitere Belästigungen. Offensives Reagieren kann da nützlicher sein: Wer ein Telefon mit einer entsprechenden Anzeige hat, sollte auf jeden Fall die Nummer der Anrufer notieren. Zwar verstecken die meisten Werbeanrufer derzeit noch ihre Nummern, das will der Gesetzgeber aber in Kürze unterbinden. Bis dahin müssen Betroffene versuchen, den Anrufer in ein Gespräch zu verwickeln: Name der Person und ihrer Firma erfragen, Sitz und Zweck der Firma, Auftraggeber und Umfang des Werbeauftrags – je mehr Daten über den Anrufer festgestellt werden können, desto besser. Oft scheitern solche Versuche, weil die Anrufer ihrerseits das Gespräch beenden. In jedem Fall sollte der Angerufene darauf hinweisen, dass weitere Anrufe unerwünscht sind, und die Löschung aller seiner Daten

verlangen. Anschließend sollten alle Informationen, die über den Anruf erlangt werden konnten, protokolliert werden, um sie bei Bedarf – also bei Häufung oder Wiederholung – dem zuständigen Datenschützer oder der nächsten Verbraucherzentrale mitzuteilen.

– Ein Werbeanrufer hat mich überrumpelt und mir was aufgeschwatzt? Was nun?

Lotto-Anbieter, Telefon- und Internetanbieter oder Zeitschriftenverkäufer – um nur wenige Beispiele zu nennen – sehen sich in einem knüppelhaften Wettbewerb. Das führt oft dazu, dass ihre Call Center zu Überrumpelungsmethoden oder geschwätzigen Tricks greifen, um sich einen Vorteil zu sichern. Dieses Überraschungsmoment stellt eine große Gefahr bei Werbeanrufen dar: Dem Angerufenen bleibt wenig Bedenkzeit, das Angebot in Leistung oder Preis zu hinterfragen. Grundsätzlich gibt es da immer ein Widerrufsrecht: Der anschließend übermittelte Vertrag enthält in der Regel entsprechende Klauseln – und für die bislang geltenden Ausnahmen etwa bei Abonnement- oder Wettverträgen bereitet der Gesetzgeber gerade eine Verschärfung zum Schutz der Kunden vor. Allerdings sollte konsequent darauf verzichtet werden, am Telefon etwa Bank- oder Kontodaten mitzuteilen, denn sonst können windige Vertragspartner sich leicht mal Geld vom Kunden ergaunern, bevor der ein Widerrufsrecht überhaupt wahrgenommen hat!

– Oft werden Kontodaten verlangt, gibt es da keinen Schutz?

Grundsätzlich sollte sich jeder Kontoinhaber überlegen, ob die bequeme Option „Ermächtigung zum Lastschriftinzug“ immer auch die beste Lösung ist. Je weniger derartige Erklärungen unterschrieben werden, desto geringer die Chance eines Missbrauchs, im Zweifel ist für die Bürgerin oder den Bürger der Weg einer

Überweisung oder eines Dauerauftrags immer die sicherere Option. Im Übrigen sollten nur vertrauenswürdigen Unternehmen Kontodaten bekannt gegeben werden, und das gilt vor allem bei Internetgeschäften: Die Kontoinhaber sollten verschärft darauf achten, dass sie tatsächlich die richtige Webseite des gewünschten Unternehmens aufgerufen haben und dass eine verschlüsselte Übertragung eingeleitet worden ist. Die Webadresse im Browserfenster muss unbedingt mit den Buchstaben ‚https‘ beginnen - wenn dort nur ‚http‘ steht, sollte auf Datenübertragung unbedingt verzichtet werden.

– Wie verhalte ich mich, wenn unerwünschte Abbuchungen geschehen sind?

Wer unerwünschte Abbuchungen feststellt, muss zunächst mit seiner Bank reden, die dann diese Abbuchung rückgängig macht. Allerdings sind solche Rückbuchungswünsche nur innerhalb bestimmter Fristen möglich. Es ist daher dringend anzuraten, die eigenen Kontoauszüge regelmäßig und gewissenhaft zu überprüfen. Wenn sich erkennbar illegale Abbuchungen wiederholen, könnte es dem Kontoinhaber nicht erspart bleiben, von seiner Bank eine neue Kontonummer zu verlangen. Das ist äußerst lästig – aber im schwerwiegenden Fall nicht zu ändern.

– Kann ich eigentlich Datendiebe irgendwie zur Rechenschaft ziehen?

Grundsätzlich gilt bei mutmaßlichem Datendiebstahl oder rechtswidriger Datenverarbeitung zum Nachteil Betroffener (und nicht nur für Kontodaten!): Das ist strafbar und kann nach dem Bundesdatenschutzgesetz (§ 44 BDSG) mit bis zu zwei Jahren Haft- oder Geldstrafe geahndet werden. Allerdings muss der Betroffene binnen drei Monaten ab Bekannt werden Strafantrag bei Polizei oder Staatsanwaltschaft stellen. Nur wenn Bürgerinnen und Bürger von dieser Möglichkeit Gebrauch machen, kann dem

Datenmissbrauch konsequent Einhalt geboten werden – im Zweifelsfalle berät der Datenschützer, ob der jeweilige Missbrauchsverdacht gerechtfertigt scheint. Darüber hinaus ist das Ausspähen von Daten gemäß § 202a Strafgesetzbuch mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe belegt.