Meine Daten gehören mir!

Die besten Tipps gegen Datenspione

Mein Recht auf Datenschutz

Jeder EU-Bürger hat es: das Grundrecht auf Datenschutz. Es wird ständig weiterentwickelt und sichert mir derzeit zu, dass

- meine personenbezogenen Daten geheim gehalten werden;
- ich Auskunft über die über mich gespeicherten Daten erhalte;
- ich Informationen bekomme, zu welchem Zweck meine Daten verarbeitet werden;
- falsche Daten über mich richtiggestellt werden;
- unzulässig gespeicherte Daten gelöscht werden.

Was dürfen Unternehmen speichern?

Grundsätzlich dürfen Unternehmen und Behörden all jene Daten speichern, die sie brauchen, um ihre Geschäfte abwickeln zu können. Sie dürfen alle Infos sammeln, die Personen freiwillig angegeben oder selbst im Internet öffentlich gemacht haben. Auch der Handel mit und der Austausch von Daten ist erlaubt. Einige Informationen sind besonders geschützt. Dazu gehören die ethnische Herkunft, die persönliche und politische Einstellung, Gesundheitsdaten und das Sexualleben. Keinen besonderen Schutz genießen Daten wie der Name, die Adresse, der Geburtstag oder das Einkommen. Wobei: Nicht alle Internetunternehmen halten sich an die Grundsätze, die in Europa bzw. in Österreich gelten. Es liegt also auch in deiner Hand, wie viel Wissen Google & Co über dich sammeln. Indem du einige Regeln beachtest, kannst du die „Datensaug-Aktionen" zumindest einschränken.

Die 7 goldenen Datenschutz-Gebote

- Allgemeine Geschäftsbedingungen (AGB) lesen: Bevor du Apps herunterlädst oder bestimmte Angebote im Netz nützt, nimm dir ein bisschen Zeit, um dich mit den AGB und Datenschutzbestimmungen zu befassen. Überfliege sie zumindest und suche mit der Tastenkombination Strg + F nach Schlüsselwörtern wie „Datenschutz", „Dritte", „Euro" oder „Rechtsverletzung".
- Daten sind die Währung, mit der im Internet bezahlt wird. Und so wie du beim Geld darauf schaust, wo du es ausgibst, solltest du es in Sachen Datenpreisgabe halten: „So viel wie nötig, so wenig wie möglich", ist ein gutes Prinzip in dieser Angelegenheit.
- Lösche Cookies (auf der Festplatte gespeicherte Minidateien) regelmäßig oder stelle deinen Browser so ein, dass er zumindest Drittanbieter-Cookies komplett zurückweist.
- Verwende einen Trackingschutz, um zu verhindern, dass Datenkraken mitlesen, wie und wo du surfst (► Seite 5).
- Verschlüssle deine E-Mails, zum Beispiel mithilfe von PGP (Pretty Good Privacy). Eine Anleitung dazu gibt's unter http://www.selbstdatenschutz.info/e-mail_verschluesseln.
- Werde aktiv, wenn du wissen möchtest, was bestimmte Firmen über dich speichern (► Seiten 8/9 und 26/27).
- Wenn du im Internet Infos über dich entdeckst, von denen du nicht möchtest, dass sie öffentlich sind, dann wehr dich! Denn du hast ein Recht aufs Vergessenwerden – und damit das Recht auf Löschung bestimmter Daten. Wie du das bei den Suchergebnissen von Google beantragst, findest du auf ► Seite 5.

Google/Alphabet

Google ist die meistgenutzte Suchmaschine der Welt. Zudem dominiert der Mutterkonzern Alphabet unter anderem den Markt für mobile Betriebssysteme (Android), Browser (Chrome), E-Mail-Dienste (Gmail) und Onlinevideos (YouTube). Dazu kommt jedes Jahr eine Vielzahl an neuen Diensten und Tochterunternehmen.

Was Google von mir wissen will. Googles Machtfülle ist so groß, dass es in der Lage ist, mit Abstand die meisten Daten über eine Einzelperson zu sammeln. Du gibst ihm immer dann Infos, wenn du einen seiner Services in Anspruch nimmst. Sei es die Suchmaschine, sein Chrome-Browser oder Android, sei es, wenn du über Picasa Bilder mit anderen Menschen teilst oder Termine im Google Kalender einträgst. Wenn du bei Google Maps am Smartphone die Standorterfassung aktiviert hast, dann weiß das Unternehmen immer, wo du dich befindest. Über Gmail lesen die Algorithmen Telefonnummern, Post- und E-Mail-Adressen deiner Freunde und Bekannten mit. Gleichzeitig ist kein anderes Unternehmen so professionell darin, Infos auszuwerten und in das Angebot an maßgeschneiderter Werbung einfließen zu lassen.

Wie kann ich mich schützen? Da Google für die meisten von uns bereits zu so etwas wie einem ausgelagerten Denkapparat geworden ist, dem wir unsere intimsten Dinge anvertrauen, ist es schwer, der Firma wenig Daten preiszugeben. Allerdings sollte dir bewusst sein, dass Google deine Daten zu Geld macht. Außerdem lässt sich die Sammlung und Auswertung von Daten begrenzen, indem du die Browser-Einstellungen so änderst, dass Cookies regel-

mäßig gelöscht werden (wobei das das Surfen ein wenig erschwert). Weiters empfiehlt es sich, am PC einen Tracking-Schutz zu installieren. Denn Programme wie Ghostery oder Adblock verhindern, dass Dritte mitlesen, und sie blenden Werbung aus. Auch fürs Smartphone gibt es inzwischen Werbeblocker. Wer sich unabhängiger von Google machen möchte, der kann Dienste wie GMX oder Yahoo statt Gmail nutzen, Open Street Map statt Google Maps oder Firefox statt Chrome.

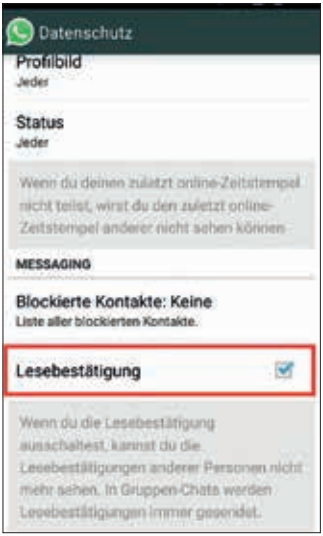
Extratipp. Im Google-Dashboard (engl. Armaturenbrett) unter www.google.com/dashboard kann ein jeder beim Konzern registrierte User (dazu reicht eine Gmail-Adresse, die Nutzung von Android oder anderen Google-Produkten) einen Teil der gespeicherten Daten sehen. Für die meisten ist der erste Blick in das Verwaltungssystem ein überraschendes Ereignis. Du bekommst eine Übersicht deiner Apps, deiner Google-Suche, der über YouTube angehörten Songs, und bei aktiviertem GPS siehst du, wann du dich in den letzten Monaten und Jahren wo aufgehalten hast. Ein weiterer wichtiger Punkt für alle, die Einträge über sich aus der Suchergebnisliste von Google streichen lassen möchten: Seit der EU-Gerichtshof im Mai 2014 das „Recht auf Vergessen" gestärkt hat, ist es möglich, den Konzern dazu zu verpflichten, Verweise auf Webseiten mit sensiblen Daten aus der Ergebnisliste zu streichen. Infos dazu unter: support.google.com/legal/contact/lr_eudpa?product=websearch.

WhatsApp

WhatsApp ist ein Chat-Dienst, über den Textnachrichten, Fotos, Videos, Sprachaufzeichnungen und Standortinformationen zwischen zwei Menschen oder in Gruppen ausgetauscht werden. Die Anwendung gehört zum Facebook-Konzern und wird von über 700 Millionen Menschen jeden Tag genutzt.

Was WhatsApp über mich wissen will. Sehr viel! Das wird schon bei der Anmeldung klar, bei der sich der Dienst Zugriff auf deine Identität, deine Kontakte, deinen Standort, deine SMS, Fotos, Medien und andere Dateien erlaubt. Außerdem auf deine Kamera, dein Mikrofon, deine WLAN-Verbindungsinfos, deine Geräte-ID sowie die Anrufinformationen.

Wie kann ich mich schützen? WhatsApp erklärt in seinen Allgemeinen Geschäftsbedingungen, keine Garantie dafür zu übernehmen, dass Inhalte vertraulich behandelt und sicher übertragen werden. Außerdem behält es sich vor, die Userdaten mit Dritten zu teilen „wenn es für die Nutzung, Pflege und Verbesserung des Services nötig ist". Das heißt: WhatsApp gibt zu, dass deine Daten nicht sicher sind. Im Gegenteil – es wurde schon in mehreren Friendly-hacking-Versuchen bewiesen, dass diese Datensauger-App unsicher ist. Daher wäre es freilich am konsequentesten, komplett auf den Dienst zu verzichten. Aber wie viele wollen das schon? Wenigstens hast du die Möglichkeit, deine Datenschutz-Einstellungen in einem sehr beschränkten Maß zu individualisieren. Wenn du zum Beispiel nicht möchtest, dass die ersten Zeilen einer Message auf dem Bildschirm angezeigt werden (falls das Handy an



einem Ort liegt, an dem ein zweiter den Text mitlesen kann). Dann solltest du unter den Einstellungen „Vorschau anzeigen" deaktivieren. Möchtest du verhindern , dass die Chatpartner sehen, ob du eine Nachricht schon gelesen hast, dann kannst du die Lesebestätigungs-Funktion unter „Einstellungen/Account/Datenschutz" ausschalten. Allerdings kannst du dann auch keine Bestätigungen von anderen sehen. Den „zuletzt online"-Status kannst du ebenfalls unter „Datenschutz" ausschalten, wodurch die anderen User nicht mehr sehen können, wann du WhatsApp zuletzt benutzt hast. Der Online-Status selbst lässt sich nicht verbergen. Beim Profilbild und dem Status kannst du wählen, ob diese Info für jeden, nur für deine Kontakte oder für niemandem ersichtlich ist – wobei du keinesfalls „jeder" einstellen solltest.

Extratipp. WhatsApp mag der populärste Chatdienst sein. Doch es gibt auch alternative Anbieter, zu deren Verwendung sich möglicherweise auch dein Freundeskreis überreden lässt. Der Dienst Line etwa verdient sein Geld nur mit dem Verkauf von Stickern. Für Gruppen-Chats eignen sich die Apps GroupMe oder KakaoChat. Letzterer ist in Sachen Datensicherheit sogar ISO-zertifiziert. Generell unter Datenschützern beliebt sind die beiden Schweizer Anwendungen Threema und MyEnigma. Beide setzen komplett auf verschlüsselte Kommunikation.

Facebook

Mit knapp 1,5 Milliarden Mitgliedern ist Facebook das zurzeit größte soziale Netzwerk der Welt. Die Seite verliert zwar im Vergleich zu anderen Plattformen besonders unter den Jugendlichen an Bedeutung. Trotzdem ist sie in Österreich nach Google immer noch die am zweithäufigsten besuchte Website.

Was Facebook über mich wissen will. Am liebsten alles! Facebook ist eine „Datenfressmaschine"! Mittlerweile wissen wir, dass der Konzern nicht nur das speichert, was wir auf Facebook und den ebenfalls dazugehörenden Kanälen WhatsApp und Instagram preisgeben. Er erhebt auch unser Surfverhalten auf anderen Seiten und kauft sich Daten von spezialisierten Sammelfirmen zu. Er wertet sie aus und erstellt ein detailliertes Persönlichkeitsprofil. Neben dem Namen, dem Geburtstag, Wohnort und der Zahl der Freunde enthält es Infos über persönliche Vorlieben, die politische und sexuelle Orientierung und sogar über unseren gesundheitlichen Zustand.

Wie kann ich mich schützen? Forscher haben herausgefunden, dass ein Computer, der 70 Likes analysiert, eine Person besser einschätzen kann als sein Freund. Nimmt er 300 Likes unter die Lupe, kennt er ihn bereits besser als sein Lebenspartner. Sprich – wenn du nicht möchtest, dass Facebook so gut über dich Bescheid weiß, dann solltest du jeden Like und jeden Kommentar abwägen, selbst in geheimen Facebook-Gruppen. Außerdem kannst du die Auswirkungen der Datensammelwut von Facebook einschränken, indem du in den Privatsphäre-Einstellungen den Regler auf eine minimale Auswertung der persönlichen Daten zu Werbezwecken setzt (unter „Einstellungen/Werbeanzeigen/Werbeanzeigen & Freunde" auf

„bearbeiten" klicken, das Feld „Kombiniere meine sozialen Handlungen mit Werbeanzeigen für" auf „Niemand" setzen und die Änderungen speichern). Weiters sollte unter der Rubrik „Einstellungen" die Sichtbarkeit der eigenen Beiträge keinesfalls auf „alle" gestellt sein. Bei den Apps (ein Unterpunkt von „Einstellungen") solltest du die Funktion „Facebook Plattform" abstellen, indem du den entsprechenden Button wählst. Dadurch wird verhindert, dass sich Facebook bei anderen Diensten wie zum Beispiel Spotify automatisch einloggt. Wenn du bestimmte Likes rückgängig machen möchtest, kannst du das im Aktivitätenprotokoll tun. Und bei den Sucheinstellungen kannst du dich entscheiden, von wem du gefunden werden möchtest. Hier solltest du über den „Bearbeiten"-Link die Option „Freunde" auswählen.

Extratipp. Wenn du genau wissen möchtest, was Facebook über dich weiß, kannst du vom EU-Recht auf Einsichtnahme der gespeicherten Daten Gebrauch machen. Eines vorweg: Dazu brauchst du viel Ausdauer und Geduld. Zuerst muss du ein Formular zur Herausgabe der Daten abschicken (unter www.facebook.com/help/contact/166828260073047). Dann erhältst du eine Antwort-Mail, die auf ein Download-Tool verweist, auf dem Facebook einen nur mit einem Bruchteil der Daten abspeisen möchte. In Folge musst du dich bei der irischen Datenschutzbehörde beschweren, von der du in der Regel aber ignoriert wirst. Also heißt es lästig sein und dich gegebenenfalls bei der EU-Behörde beschweren. Alle Anleitungen dazu gibt's auf www.europe-v-facebook.org.

YouTube

Für viele Jugendliche ist es bereits die wichtigste Seite im Netz: Das Videoportal YouTube, auf dem du als Nutzer kostenlos Videos ansehen, liken und disliken sowie kommentieren kannst. Außerdem kannst du auch selbst Filme hochladen.

Was YouTube von mir wissen will. Die Plattform gehört Google/Alphabet – darum fließen alle Daten auf die Server des Konzerns und fungieren dort als „kleiner" Baustein im gesamten Wissen, dass der Internetriese über jeden einzelnen Internetnutzer angesammelt hat. Ein jeder, der über ein Google-Konto verfügt, ist damit automatisch auch auf YouTube registriert. Das heißt: Viele haben ein YouTube-Konto, wissen es aber nicht. YouTube selbst sammelt alle Infos über das Seherverhalten seiner Seitenbesucher; darüber, welche Musik und welche Filme der Einzelne mag; je nach den angeschauten Inhalten und der Nutzungsintensität weiß YouTube über deine Vorlieben und Hobbys Bescheid – ob du gerne Tiere magst (Katzenvideos…), Kochsendungen, gefährliche Stunts und so weiter.

Wie kann ich mich schützen? YouTube – und damit Google – die eigenen Daten vorzuenthalten, ist nicht möglich, wenn du die Videoplattform nutzt. Wohl aber kannst du für Privatheit gegenüber den anderen YouTube-Usern sorgen, zum Beispiel, indem du den Zugang zu deinen Playlists einschränkst. Das kannst du am PC unter „Video Manager/Playlists/Bearbeiten/Playlist-Einstellungen" tun, indem du dort die Option „Privat" wählst. Dann können nur du selbst und von dir ausgewählte (registrierte) Nutzer die Playlist anhören. Dasselbe gilt für deine eigenen Videos – auch die können

auf „Öffentlich" oder „Privat" gestellt sein. Daneben existiert mit „nicht gelistet" noch ein „Zwischending". Auf diese Art eingestellte Videos können nur von Usern angesehen werden, die den direkten Link dazu haben. Über die YouTube-Suche dagegen ist das Video nicht auffindbar. Eine weitere Wahlmöglichkeit in Sachen Datenschutz besteht hinsichtlich der Videostatistiken. Die können sich Nutzer wahlweise direkt unter dem Video ansehen – oder auch nicht, wenn du als Bereitsteller des Videos das nicht möchtest. Dann kannst du es verhindern, indem du unter „Einstellungen/Datenschutz" das Häkchen unter „Statistiken und Daten für meine Videos standardmäßig öffentlich anzeigen" entfernst.

Extratipp. Kurios aber wahr: Rechtlich gesehen ist die Nutzung von YouTube erst ab dem „rechtlich erforderlichen Alter für den Abschluss eines Vertrages" erlaubt, wie die Plattform in ihren Geschäftsbedingungen schreibt. Das beträgt in Österreich, abhängig vom Rechtsgebiet, 14 bzw. 18 Jahre. Alle, die Videos auf YouTube stellen,sollten sich davor in Sachen Urheberrechte (Rechte zum Schutz geistigen Eigentums) schlau machen. Du solltest nur Material hochladen, für das du die Rechte besitzt; deswegen sind zum Beispiel TV-Mitschnitte oder irgendwo downgeloadete Filme ein No-Go. Von Bedeutung ist auch, welche Musik im Hintergrund eines selbst gedrehten Films läuft und welche Personen mitspielen (Persönlichkeitsrechte).

Instagram

Instagram ist eine App, mit der Fotos und Videos inklusive kurzer Texte verbreitet werden können. Die Bilder und Kurzfilme können mit verschiedenen Filtern versehen werden. Werden die Inhalte mit sogenannten Hashtags (#) versehen, so werden sie mit Bildern mit ähnlichen Inhalten verknüpft.

Was Instagram von mir wissen will. Die App benötigt Zugriff auf die Kamera und die Fotos auf dem Smartphone – und bei Videoaufnahmen Zugriff auf das Mikrofon. Außerdem lässt sich Instagram in seiner Datenschutzerklärung erlauben, sämtliche Nutzerinhalte, Standortinformationen, die Geräte-ID und Daten aus Cookies an seinen Mutterkonzern Facebook weiterzugeben.

Wie kann ich mich schützen? Gegen die Datensammlerei von Instagram bzw. Facebook kannst du nicht viel tun. Du kannst dir aber mehr Privatsphäre innerhalb der Instagram-Community verschaffen. Denn: Bei der Installation der App sind das Nutzerprofil und sämtliche Bilder automatisch für alle zugänglich. Es gibt jedoch die Möglichkeit, selbst einzustellen, wer die Inhalte sehen darf und wer nicht. Dafür musst du auf dem Eingangsbild der geöffneten App unten rechts auf das Symbol der Visitenkarte klicken, dann auf die Funktion „Bearbeite dein Profil" neben dem Profilbild. Daraufhin scrollst du nach unten und aktivierst die Funktion „Beiträge sind privat". Von nun an ist dein Profil für die Öffentlichkeit gesperrt und neue Follower müssen immer erst von dir akzeptiert werden, bevor sie Inhalte sehen können. Die Follower, die du vor der Aktivierung der Privacy-Funktion hattest, bleiben erhalten. Weiters besteht die

Möglichkeit, einzelne Bilder im eigenen Profil zu verbergen, und zwar, indem du das Profil wie davor beschrieben aufrufst, dann „Fotos von dir" und daraufhin das gewünschte Bild auswählst und die Einstellung „in meinem Profil verbergen" aktivierst. Auch das Taggen (das Markieren) von Bildern durch andere Nutzer ist bei Instagram von vornherein erlaubt. Wenn du selbst die Kontrolle darüber behalten möchtest, auf welchem Bild du „getagged" wirst, solltest du in deinem Profil die Rubrik „Fotos von dir" aufrufen, rechts oben „Einstellungen" auswählen und „manuell" hinzufügen. Von nun an kannst du jedes Tagging zuerst bestätigen oder ablehnen. Ungewollte Tags lassen sich im Nachhinein entfernen, indem du unter „Profil"/„Fotos von dir" das betreffende Foto auswählst, das Tag antippst und die Option „Mich aus dem Foto entfernen" wählst.

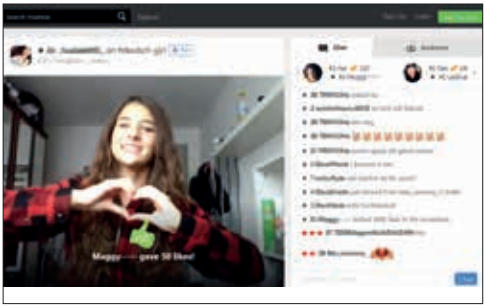
Extratipp. Von Haus aus privater ist die Funktion „Instagram Direct", die ebenfalls von der App angeboten wird. Damit können Bilder und Videos mit Messages an einzelne Personen verschickt werden und erscheinen auch nicht automatisch auf dem jeweiligen Profil. Auch Gruppen bis zu 15 Personen können unter Direct gebildet werden. Die Inhalte unter Direct können weder „getagged" noch auf Instagram selbst, Facebook, Twitter & Co geteilt werden. Den „Direct-Modus" findest du auf der Startseite rechts oben unter dem Schubladen-Symbol.

YouNow

Auf Now können sich Nutzer filmen und die Aufnahmen live im Internet veröffentlichen (broadcasten) und umgekehrt anderen Nutzern beim Streamen zusehen. Über ein Chatfenster lässt sich das Gesehene kommentieren und mit den „Darstellern" kommunizieren.

Was YouNow von mir wissen will. Die Registrierung kann nur über Facebook, Twitter oder Google+ erfolgen. Im Zuge des Prozesses erhält YouNow von der jeweiligen Plattform Infos über deinen Namen, die von dir dort bekannt gegebenen Tätigkeiten, deinen Wohnort, deine Interessen, Vorlieben, Fotos und Videos, deine E-Mail-Adresse und Telefonnummer, deine Freunde in den sozialen Medien „und mehr", wie YouNow in seiner Datenschutzerklärung schreibt.

Wie kann ich mich schützen? Abseits davon, welche Daten YouNow erfasst, birgt es ein Gefahrenpotenzial, sich online vor einer großen Menge unbekannter Menschen darzustellen. Noch dazu, wo man schnell einmal mehr private Einblicke gibt, als man eigentlich möchte – und man sich oft nicht dessen bewusst ist, dass eine Tat oder ein Satz bei einer Liveübertragung nicht im Nachhinein herausgeschnitten werden kann. Außerdem wird häufig gegen Persönlichkeits- und Urheberrechte verstoßen, etwa wenn andere Personen mitgefilmt werden oder Musik- oder Videomitschnitte im Stream vorkommen. Wenn du dich für eine Anmeldung auf YouNow entscheidest, solltest du dich deinen Zusehern keinesfalls mit deinem Klarnamen, sondern unter einem Nickname vorstellen. Festgelegt wird er, indem du am Eingangsbild auf dem PC nach dem



Einloggen oben auf das Profilbild klickst, unter „Settings/Information/Nickname" ein Häkchen setzt und einen Spitznamen eingibst (unter Android und iOS muss unter dem Zahnrad-Symbol unter „Edit Profile/Nickname & Url" der Regler „Replace your Real Name" aktiviert werden). Ebenso wenig sollte der Wohnort preisgeben werden. Dafür musst du am PC unter „Profilbild/Settings/Privacy" ein Häkchen bei „Hide my city" setzen. Lästige User im Chat können blockiert werden, indem du auf das Profil der jeweiligen Person klickst, dann auf das Fähnchen und dann auf „Block". Sollten sich User unangebracht verhalten, empfiehlt sich eine Meldung der Person beim Moderator (Klick auf „Kontaktiere einen Moderator", Formular ausfüllen und abschicken). Ein Nutzer kann aber auch über sein Profil gemeldet werden, und zwar wieder mit einem Klick auf das Fähnchen und der Wahlmöglichkeit „Report User". Dabei sollte ein Begründung wie etwa „Offensive Conduct", „Nudity" oder „User under 13" angegeben werden.

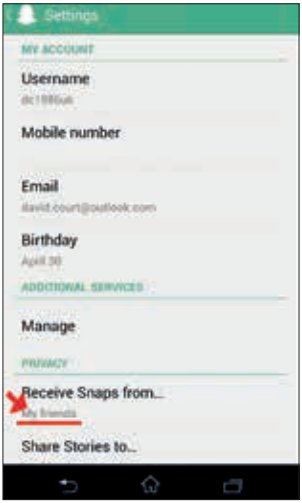
Extratipp. Frage dich, ob du es nötig hast, dich auf der Seite zu präsentieren! Wenn doch nicht, dann ist das Konto schnell gelöscht – und zwar, indem du auf dein Profilbild klickst und im Dropdown-Menü den Punkt „Settings" wählst. Dann klickst du auf „Connected Accounts" und rechts neben dem sozialen Netzwerk (z.B. Facebook) auf „Disconnect". Endgültig gelöscht wird das Konto unter „Privacy/Terminate my Account" und „Yes, Terminate".

Snapchat

Über den Messaging-Dienst Snapchat lassen sich Bilder und Videos verschicken, die nur für eine kurze Zeit sichtbar sind. Nach ein bis zehn Sekunden „verschwinden" die Inhalte vom Gerät (werden aber nicht komplett gelöscht). Die App wird häufig zum sogenannten Sexting, das heißt zum Versenden freizügiger Bilder, verwendet.

Was Snapchat von mir wissen will. Eine Menge! Snapchat lässt sich bei der Installation Zugriff auf deine Identität (Name, E-Mail-Adresse, Telefonnummer, Alter) erlauben, dazu auf deine Kontakte, den Standort, SMS, Fotos, Medien & Dateien, die Kamera, das Mikrofon sowie auf die Geräte-ID und die Anrufinformationen. Darüber hinaus sammelt die App Daten über dich aus anderen Quellen, zum Beispiel über den Provider oder das verwendete Betriebssystem.

Wie kann ich mich schützen? Mittlerweile ist bekannt, dass über Snapchat verschickte Bilder und Videos nicht endgültig gelöscht werden und auch nicht wirklich „flüchtig" sind. Sie sind in bestimmten Files „versteckt" und können entweder wieder gefunden werden oder sie werden mithilfe von Apps wie „Pic Saver" bei Erhalt automatisch fotografiert bzw. downgeloadet und gespeichert. Außerdem haben Snapchat-User (vorerst nur die in den USA) seit Kurzem auch die Möglichkeit, sich für Geld Bilder und Videos wieder zurückzuholen. Ebenso wenig schützt Snapchat die Nutzerdaten, wie nach einem Hack in den USA bekannt wurde, bei dem über Nacht 4,6 Millionen Userprofile online gestellt wurden. Daher solltest du gut überlegen, welche Inhalte du über die App verschickst. In den Privatsphäre-Einstellungen kannst du entscheiden, ob du



Nachrichten nur von Freunden oder auch von Fremden erhalten möchtest und ob du Inhalte nur mit Freunden oder mit jedem teilen möchtest. Beide Funktionen sollten auf „Freunde" gestellt sein (auf dem Zahnrad-Symbol oben rechts unter „Wer kann ..." sowohl bei „Mir Snaps schicken" als auch bei „Meine Geschichte ansehen"). Um einen Kontakt zu blockieren, musst du auf die jeweilige Person in der Freundeliste tippen, dann auf das Zahnrad-Symbol und den Button „Blockieren" aktivieren. Gänzlich löschen lässt sich ein Kontakt, indem du auf demselben Wege unter dem Zahnrad-Symbol den Button „Löschen" aktivierst.

Extratipp. Ein Foto, das ursprünglich als Liebesbeweis für den Partner gedacht war, kann schnell zum Problem werden – etwa, wenn aus dem Freund ein „Ex" wird, der auf Rache sinnt und das Bild in seinem Bekanntenkreis weiterschickt oder online stellt. Nicht selten werden Sexting-Inhalte auch zur Erpressung benutzt. Daher ist es ratsam, den/die Empfänger/in solcher Bilder sehr sorgfältig auszuwählen. Es sollte jemand sein, den du gut kennst und zu dem du Vertrauen aufgebaut hast. Was das Bilderschießen selbst betrifft, ist es besser, sich so abzulichten, dass man nicht eindeutig identifizierbar ist – etwa, indem das Gesicht nicht zu erkennen ist. Werden regelmäßig solche Fotos verschickt, dann schadet es nicht, sie auch immer wieder gemeinsam mit dem/der Freund/in vom Smartphone zu löschen.

Runtastic

Die Runtastic-App protokolliert, wie oft und wie schnell man bestimmte Strecken läuft. Darüber hinaus bietet Runtastic eine Menge Zusatz-Apps und Hardware, die bei der Selbstvermessung hilft und Aktivitäten wie Radfahren, Sit-ups oder die Herzfrequenz und die Schlafqualität aufzeichnet.

Was Runtastic über mich wissen will. Je nachdem, welche Apps und Zusätze du verwendest, reichen die Protokollierungen von deiner Identität (Profildaten, Standort, Bilder, Videos, Audiodateien) über deine Bewegungsgewohnheiten bis hin zu höchst privaten Angelegenheiten wie Vitalfunktionen (Herzschlag), die Schlafqualität und die psychische Verfassung.

Wie kann ich mich schützen? Zwar versichert der Runtastic-Firmenchef, dass persönliche Informationen nicht an Dritte weitergegeben werden. Aber dass das auch in Zukunft so bleiben wird, das möchte er nicht versprechen. Deshalb, und weil es sich um äußerst sensible Daten handelt, und weil die Aktivitäten diversen Tests zufolge ohnehin nicht präzise aufgezeichnet werden können, empfiehlt es sich, komplett auf den Fitnesstracker zu verzichten. Die Löschung der Gratisversion der App funktioniert, indem du dich auf runtastic.com einloggst, im Menü „Einstellungen" wählst, auf „Login-Daten" klickst, rechts unten auf „Meinen Account löschen" gehst und „OK" tippst. Wenn du nicht auf die App verzichten möchtest, kannst du mit bestimmten Einstellungen für ein wenig mehr Privatheit sorgen. So solltest du das „Live-Tracking"-Feature deaktivieren, denn es ermöglicht Dritten, die Laufroute und andere Infos

einzusehen. Was genau andere User sehen können, das lässt sich unter den Privatsphäre-Einstellungen festlegen – wobei es gilt, bei der Datenpreisgabe so sparsam wie möglich vorzugehen. Außerdem solltest du deine Infos nicht auf Facebook oder Twitter teilen. Falls Social-Media-Plattformen bereits mitlesen, lässt sich das über „Menü/Einstellungen/Persönliche Info/Profil bearbeiten/Soziale Verbindung/Verbindung trennen" deaktivieren.

Extratipp. Das Erheben der eigenen Fitness, das die sogenannte Quantified-Self-Bewegung betreibt, ist ein großes und vor allem brisantes Zukunftsthema. Versicherungen interessieren sich bereits für solche Daten, weil sie Polizzen anbieten möchten, die vom Verhalten eines Menschen und seinem Fitness- und Gesundheitszustand abhängig sind. Sollten sich solche Modelle durchsetzen, dann würde nicht nur das solchen Versicherungen innewohnende Solidaritätsprinzip ausgehöhlt, sprich, dass die Gemeinschaft dafür aufkommt, wenn der Einzelne medizinische Hilfe braucht. Vielmehr noch würden die Kunden am Ende draufzahlen. Denn irgendwann hat wohl ein jeder mit gesundheitlichen Problemen zu kämpfen und muss gerade dann mit höheren Tarifen rechnen. Außerdem entstehen noch weitere Risiken. Bei einem Identitätsdiebstahl etwa können mithilfe der Daten Ausweise gefälscht werden. Zudem wird es Stalkern leicht gemacht, zum Beispiel, wenn sie Laufrouten live im Internet verfolgen können.

Spotify

Spotify ist ein Musikstreaming-Dienst, bei dem man Musik von großen Plattenlabels wie Sony, Emi und Universal, aber auch von vielen kleinen Labels legal und kostenlos hören kann. Für zehn Euro im Monat gibt es den Service in höherer Klangqualität und ohne Werbung.

Was Spotify über mich wissen will. Seit Sommer 2015 wird eine Unmenge an Daten gesammelt. Im August hat der Dienst seine Datenschutzbestimmungen geändert und lässt sich seitdem Zugriff auf folgende persönliche Daten erlauben: Neben Username, Passwort und Mailadresse sind es das Geburtsdatum, das Geschlecht und die komplette Anschrift. Ist die App mit Facebook verknüpft, dann holt sie sich die Profildaten, die Namen und Profilbilder deiner Freunde und Gruppen sowie deine Likes und Posts auf Facebook. Spotify protokolliert, wie die User untereinander interagieren und was ins Mikrofon gesprochen wird; außerdem die am Handy gespeicherten Kontakte, Bilder und Videos. Auch dein Standort wird miterfasst, sofern das GPS aktiviert ist.

Wie kann ich mich schützen? Die Nutzung des Dienstes selbst kann recht öffentlich, aber auch ein wenig „privater" vonstattengehen. Wenn du nicht möchtest, dass andere wissen, welche Musik du hörst, dann solltest du dich bei der Installation der App mit der E-Mail-Adresse und nicht mit dem Facebook-Account anmelden. Wer sich schon bei der Installation gegen Facebook entscheidet, muss während des Prozesses nur den Button „Musik, die ich höre, auf Facebook teilen" in der untere linken Ecke am Bildschirm auf Schwarz stellen (alternative Wahlmöglichkeit ist Grün). Wenn du die

Verknüpfung mit dem sozialen Netzwerk nachträglich entfernen möchtest, musst du folgendermaßen vorgehen: die App öffnen, im Menü „Bearbeiten" die „Einstellungen" aufrufen und die Option „Meine Aktivitäten und Musik, die ich höre, auf Facebook teilen" deaktivieren. Dann poppt ein Fenster auf, in dem nochmals „Posten auf Facebook deaktivieren" markiert werden muss. Wenn du außerdem nicht möchtest, dass deine Wiedergabelisten auf Spotify aufscheinen, kannst du es unterbinden, indem du unter „Interaktion" den Button „Meine Aktivität und Musik, die ich höre, mit Followern auf Spotify teilen" deaktivierst.

Extratipp. Unter „Interaktion" können weitere Einstellungen, die die Wiedergabeliste betreffen, vorgenommen werden. Einen größtmöglichen Schutz der Privatsphäre hast du, wenn du die Buttons bei „Neue Playlists automatisch veröffentlichen", „Mich als Top-Hörer für Künstler veröffentlichen" und „Meine aktuellen Top-Künstler anzeigen" auf Schwarz stellst und stattdessen die Option „Private Session" aktivierst. Wenn du hingegen nur bestimmte Playlisten für dich behalten willst, kannst du das auch einzeln tun, indem du mit der rechten Maustaste auf die jeweilige Wiedergabeliste klickst und dann „Geheim halten" aktivierst. Um dich schließlich noch vor allzu lästiger Werbung zu schützen, solltest du in deinen Profil-Einstellungen auf das Häkchen unter „Meine Personendaten können zu Marketingzwecken weitergegeben werden" verzichten.

Amazon

Amazon ist mit über 260 Millionen Kunden der größte Online-Versandhändler der Welt. Neben einem schier unendlich großen Warenangebot bietet das Unternehmen unter anderem eigene Hardware wie E-Book-Reader, Tablets und Streaming bzw. Downloadmöglichkeiten von Video- und Musikinhalten.

Was Amazon über mich wissen will. Die für einen Händler nötigen Informationen wie Name, Adresse, E-Mail-Adresse sowie Zahlungsarten sind längst nicht genug. Der Händler speichert die gesamte Einkaufs- und Suchhistorie seiner Kunden. Je nach Nutzerverhalten geht die Datensammelwut des Konzerns so weit, dass er detailliert über dein Leseverhalten Bescheid weiß (Kindle), welche Filme du ansiehst und welche Musik du hörst (Einkäufe, Streaming, Downloads). In den USA können Kunden bereits einen Lautsprecher namens Alexa kaufen, der über Spracherkennung auf Zuruf eine Einkaufsliste erstellen kann. Geplant ist, dass auch der Kauf selbst rein mündlich getätigt werden kann. Ist Alexa einmal aufgestellt, ist sie „always on" und kann theoretisch alles mithören, was in den eigenen vier Wänden besprochen wird. Die Fülle an Kundendaten, die von Amazon gehortet werden, ist vergleichbar mit jener von Google oder Apple.

Wie kann ich mich schützen? Die Sammelleidenschaft des Unternehmens lässt sich nicht so leicht einschränken. Wenn du auf Amazon einkaufen möchtest, musst du diese Preisgabe von Informationen in Kauf nehmen. Und wenn du ein Buch in vollkommener

Privatsphäre kaufen möchtest, dann bist du in einer Bücherei besser aufgehoben. Aber: Ein Ausspionieren deines Einkaufsverhaltens im Netz sowie lästige, auf dein Suchverhalten maßgeschneiderte Werbeanzeigen kannst du mit der Installation von bestimmten PC-Programmen (Adblocker, Trackingschutz) eindämmen. Ghostery beispielsweise ist eine Anwendung, die Programme ausfindig macht, die im Hintergrund private Daten von deinem Gerät an andere Seitenbetreiber übermitteln. Diese Programme werden dann auf Wunsch blockiert. Speziell gegen Werbung arbeiten kostenlos im Netz downloadbare Programme wie Adblock (für Chrome und Safari) oder Adblock Plus für Firefox.

Extratipp. Die Kundenbewertungen auf Amazon sind mit Vorsicht zu genießen. Denn ein bestimmter Club an Testern (Amazon Vine) bekommt regelmäßig Gratisprodukte zugeschickt. Um auch länger in diesem Club bleiben zu dürfen, bewerten die Mitglieder diese Waren meist äußerst positiv; mitunter auch solche, die sich keine Lobeshymnen verdienen. Weiters sollte der Nutzer genau auf die Preise der angebotenen Produkte achten. Denn die können sich, insbesondere bei elektronischen Produkten, alle paar Stunden ändern. Die Ursache dafür ist eine vom Unternehmen angewendete sogenannte Intelligent Pricing Software. Die errechnet aus verschiedenen Faktoren, wann der Durchschnittskunde bereit ist, wie viel für ein Produkt auszugeben, und passt die Preise laufend an.

Tinder

Unter Jugendlichen hat sich Tinder mittlerweile zur meistgenutzten Datingplattform entwickelt. Über GPS wird einem Mitglied angezeigt, welche anderen flirtwilligen User in der Nähe sind. Der Nutzer entscheidet nach dem „Hot or Not"-Prinzip, mit einem Wisch nach links oder rechts, ob er den anderen gut findet oder nicht. Wenn sich beide „liken", dann eröffnet sich eine Chatmöglichkeit.

Was Tinder von mir wissen will. Mehrheitseigentümer von Tinder ist die New Yorker Internetfirma IAC, der noch einige weitere Datenportale wie Match.com, Meetic oder OkCupid gehören. In den Allgemeinen Geschäftsbedingungen sichert Tinder sich und seinen Mutter- und Tochterunternehmen das weltweite, unbefristete, unwiderrufliche Lizenzrecht am gesamten Content der Tinder-Nutzer. Dazu gehören Name, Geschlecht, Wohnort und Fotos – Infos, die allesamt auf den amerikanischen Servern einer Datenkrake landen. Außerdem werden durch die Verbindung des Facebook-Profils alle deine Facebook-Daten an Tinder übertragen. Dazu kommt, dass ein junger Kalifornier bewiesen hat, dass Tinder relativ leicht zu hacken ist/war. Er machte sich einen Spaß daraus, ahnungslose Männer miteinander chatten zu lassen, die glaubten, sie unterhielten sich mit Frauen.

Wie kann ich mich schützen? Auf der sicheren Seite bist du, wenn du die App komplett vom Smartphone löschst. Das funktioniert folgendermaßen: Tinder starten und oben links auf das „Einstellungen"-Symbol klicken. „App-Einstellungen" auswählen und nach unten scrollen. Anschließend auf „Konto löschen" klicken und

die Abfrage mit „Konto löschen" bestätigen. Nach einigen Sekunden bist du ausgeloggt und das Konto ist gelöscht. Aber Vorsicht: Zwar ist jetzt die Verbindung von Facebook zu Tinder gelöscht. Trotzdem befindet sich die Anwendung weiterhin in den Facebook-Einstellungen und muss auch in den Facebook-Apps gelöscht werden. Wenn du auf Tinder bleiben möchtest, aber nicht willst, dass deine Facebook-Freunde es sehen, kannst du bei den Facebook-Einstellungen unter „Sichtbarkeit der Apps" die Option „Nur ich" auswählen.

Extratipp. Bei der Nutzung von Tinder nimmst du das Risiko in Kauf, dass andere erfahren, wo du dich gerade befindest, und möglicherweise auch, wo du wohnst. Da es sich beim Gegenüber in der Regel um einen Unbekannten handelt, solltest du eine gewisse Vorsicht walten lassen. Will ich, dass derjenige weiß, in welcher Gegend ich mich aufhalte? Diese Frage sollte sich jeder Tinder-User stellen, bevor er sich auf einen Wisch in die „Like"-Richtung oder einen Chat einlässt. Weiters solltest du dir Zeit lassen, bis es zum ersten Treffen kommt. Und es will gut überlegt sein, an welchem Ort das passieren soll. Keinesfalls sollte es das eigene Zuhause sein und auch nicht das des Flirtpartners. Am besten eignet sich ein neutraler Ort, von dem man leicht wieder verschwinden kann, falls das Gegenüber ein „Flop" ist. Das Lieblingskaffeehaus sollte es ebensowenig sein. Denn wer will dem „Leider-nicht-Partner" später noch öfter über den Weg laufen?

Zalando

Zuerst hat das Start-up aus Berlin nur Schuhe verkauft. Heute ist Zalando mit weit über 150.000 Artikeln im Angebot eines der größten Modeversand-Unternehmen ganz Europas. So groß geworden ist es, weil es die Ware kostenlos verschickt und wieder zurücknimmt.

Was Zalando über mich wissen will. Erfreulich wenig! Ein Test, in dem vom EU-weit geltenden Recht auf unentgeltliche Auskunft über die gespeicherten Kundendaten Gebrauch gemacht wurde, ergab Folgendes: Der Händler speichert nur das Nötigste wie Bestellnummer, Zeitpunkt des Einkaufs, Name, Mail-, Rechnungs- und Versandadresse und die Höhe des Bestellwertes sowie die Zahlart. Darf man dem Schreiben von Zalando Glauben schenken, werden keine Tiefendaten wie Alter, Familienstand, Hobbys und Vorlieben gespeichert. Informationen über die Bonität eines Kunden holt sich Zalando von einer Kreditauskunftei, hierzulande von der Firma CRIF.

Wie kann ich mich schützen? Generell hält sich Zalando an die im Vergleich zu den USA viel strengeren Datenschutzgrundsätze in Europa. Der Einkauf auf dieser Plattform birgt also kein großes Risiko. Wohl aber gibt es einige Tricks und Kniffe, die möglichem Datenmissbrauch entgegenwirken und grundsätzlich beim Gebrauch des Internets ratsam sind. Zum Beispiel solltest du deinen Internetbrowser so konfigurieren, dass Cookies nach dem Schließen des Browsers gelöscht und Drittanbieter-Cookies überhaupt blockiert werden. Außerdem sollten keine Passwörter im Browser gespeichert werden. Es ist zwar mühsamer, aber sicherer, wenn du bei Anmeldungen im Netz immer aufs Neue nach Username und Passwort

gefragt wirst. Und: Die Passwörter sollten nicht für alle Websites dieselben sein. Was die Registrierung auf verschiedenen Seiten wie Zalando betrifft, sollte man als User immer nur das Allernötigste angeben.

Extratipp. Stichwort Social Plug-ins – und zwar nicht nur bei Zalando, sondern bei allen Webseiten im Netz: Die Buttons von Facebook, Twitter & Co werden auf Seiten aller Art eingebaut, sei es auf Verkaufsseiten, auf Blogs oder Fanseiten eines Fußballvereins. Mithilfe dieser Plug-ins kannst du eine Seite schnell und einfach „liken", indem du auf das blaue Kästchen mit dem Daumen-hoch-Zeichen klickst. Facebook läuft derweil im Hintergrund mit und bekommt die Info, dass du auf eben dieser Seite surfst – sogar, wenn du zu der Zeit nicht im Netzwerk angemeldet bist. Das erlaubt den Social-Media-Riesen, noch umfassendere Surfprofile ihrer Nutzer zu erstellen. Zalando agiert bei den Social Plug-ins vorbildhaft, weil es die sogenannte 2-Klick-Lösung anwendet. Dabei sind die von Facebook und Twitter eingebetteten Buttons zunächst deaktiviert. Als Nutzer musst du erst mit einem Klick zustimmen, dass du die Kommunikation mit den Netzwerken zulässt. Mit einem zweiten Klick schließlich wird dieses Teilen mit den Social-Media-Seiten erst aktiviert. Doch noch längst nicht alle Seiten wenden die 2-Klick-Lösung an. Du musst deshalb zuerst überlegen, bevor du außerhalb von Facebook auf „Teilen" klickst.

Mjam

Mjam ist ein in Wien gegründeter Lieferdienstvermittler für Speisen und Getränke. Bestellt wird das Essen über die Homepage oder die App. Zur Auswahl stehen mittlerweile über 600 Restaurants in Österreichs größeren Städten.

Was Mjam über mich wissen will. Eigentlich nur die Daten, die es benötigt, um dir das Essen zustellen zu können: den Namen, die Telefonnummer, die E-Mail-Adresse, die Lieferadresse sowie, je nach Zahlungsmodalität, die Kreditkartennummer, das PayPal-Konto oder die Nummer einer Bankkarte. Doch wie sich im Jahr 2015 gezeigt hat, geht das Unternehmen nicht sorgsam genug mit diesen Daten um. Nachdem es bei Mjam ein Datenleck gegeben hat, sind zahlreiche Kunden aus Wien monatelang von Telefonkeilern (Scammern) belästigt worden. Wobei das Unternehmen erst nach einigen Wochen etwas gegen den Datenklau unternommen hat. Seine ahnungslosen Kunden hat es lange nicht aufgeklärt.

Wie kann ich mich schützen? Mit Mjam verhält es sich wie mit vielen anderen Internet-Services: Willst du die Dienstleistung in Anspruch nehmen, bleibt dir nichts anderes übrig, als die Daten preiszugeben. Du kannst jedoch stets darauf achten, es im geringstmöglichen Ausmaß zu tun. Grundsätzlich solltest du die Telefonnummer bei Internet-Diensten nur dann angeben, wenn es wirklich nötig ist, und im Zweifelsfall ganz auf die Anwendung verzichten. Vor dem Herunterladen von Apps wie der von Mjam solltest du gut überlegen, ob du sie auch tatsächlich brauchst. Außerdem bist du gut beraten, bei der Installation darauf zu achten, worauf die App

Zugriff haben möchte. Nach der Registrierung auf Mjam solltest du rasch das Passwort wechseln und das in regelmäßigen Abständen wiederholen.

Extratipp. Der Fall Mjam hat gezeigt, wie schnell es gehen kann, dass auf einer angeblich sicheren Seite preisgegebene persönliche Daten in falsche Hände geraten. Wobei ein von einem Datenleck betroffener User es nicht zwangläufig mitbekommen muss. Dass du Opfer eines „Leaks" geworden bist, erkennst du aber beispielsweise daran, dass du häufig von unterdrückten oder unbekannten Telefonnummern angerufen wirst und die Person am anderen Ende der Leitung dir etwas verkaufen möchte oder Geld verlangt, das du ihr angeblich schuldest. Wenn du öfter von lästigen Telefonkeilern bedrängt wirst, solltest du anonyme Anrufe und diejenigen Telefonnummern, unter denen die Scammer aufscheinen, sperren. Von selbst versteht sich, dass du diesen Anrufern keine weiteren privaten Daten von dir preisgeben, alle Anfragen ablehnen und auflegen solltest. Da diese Keiler in vielen Fällen nicht lockerlassen, empfiehlt sich nachzufragen, welche Firma hinter dem Anruf steckt, sich den Namen des Unternehmens und des Anrufers geben zu lassen und Letzterem mitzuteilen, dass man der Sache rechtlich nachgehen werde. Weiters besteht die Möglichkeit, solche Anrufe beim Netzbetreiber zu melden und/oder Anzeige bei der Fernmeldebehörde zu erstatten. Infos dazu unter www.bmvit.gv.at/telekommunikation/organisation/nachgeordnet/fmb/index.html.

PayPal

PayPal (engl. für „Bezahlfreund") ist ein Bezahldienst für das Internet. Das E-Payment-Programm funktioniert auf Basis von E-Mail-Adressen, die Zahlungsinformationen austauschen, daher genügen eine E-Mail-Adresse und ein Passwort, um einen Bezahlvorgang mit nur zwei Klicks abzuschließen. Rund eine Million Österreicher nutzen den Dienst.

Was PayPal über mich wissen will. Viel mehr als dir lieb ist, zumal es sich bei derartigen Bezahlinfos um sehr sensible Daten handelt. Mit Anfang Juli 2015 präsentierte PayPal seine neuen Datenschutzbestimmungen, die es in sich haben. Darin erklärt das Unternehmen, dass es sich die Rechte auf alle vom User bereitgestellten Inhalte „weltweit, unbefristet, unwiderruflich, gebührenfrei und unterlizensierbar, in allen bekannten Medien, jetzt und in Zukunft [...]" sichern lässt. Eine Passage, die vor allem dann relevant ist, wenn man Handel betreibt und Zahlungen über PayPal abwickelt. Außerdem ist der Gesetzestext so unverständlich und vage formuliert, dass selbst Anwälte ihre Mühe haben, ihn zu verstehen (allein das ist schon gesetzeswidrig). Bei der Weitergabe der Daten an Dritte ist PayPal alles andere als zimperlich. In der Liste werden knapp 400 Unternehmen genannt, an die der Bezahldienst Infos weitergibt. Darunter eine Menge Marketingunternehmen wie Facebook und Twitter und sogenannte Kreditauskunfteien, die auf Daten darüber spezialisiert sind, wie ein Verbraucher finanziell dasteht. Außerdem landen die Infos auch bei Datenkraken, die Persönlichkeitsprofile von Bürgern verkaufen, wie zum Beispiel der Konzern Acxiom.

Wie kann ich mich schützen? Bei Nutzung von PayPal musst du dir darüber im Klaren sein, dass die Anwendung jede Menge sensible Informationen nicht nur sammelt, sondern auch auf eine sehr freizügige Art und Weise weitergibt. Es gibt auch keine Möglichkeiten, die Datenschutz-Einstellungen auf PayPal in irgendeiner Weise anzupassen. Nachdem das Unternehmen 2015 seine Datenschutzgrundsätze geändert hat, haben zahlreiche Kunden ihr Konto gekündigt. Dazu raten auch auf E-Payment spezialisierte Juristen. Außerdem gibt es einige, wenngleich nicht so verbreitete, Alternativen wie Apple Pay, Android Pay oder ClickandBuy. Doch auch diese Anwendungen gewähren keinen ausreichenden Datenschutz. Am besten für den Kunden ist immer noch die Bezahlung per Rechnung. So kannst du die Ware auch prüfen, bevor du sie bezahlst.

Extratipp. Wer PayPal verwendet und einmal Probleme bei einer Zahlung hatte, dem kann es wegen der Datenweitergabe an Kreditauskunfteien passieren, dass er von bestimmten Händlern Ware nur mehr auf Vorkasse erhält. Besondere Vorsicht ist auch geboten was Spoof und Pishing (betrügerische Versuche per E-Mail, um an sensible Daten zu gelangen) betrifft. Wenn du eine E-Mail von PayPal erhältst und nicht sicher bist, ob sie auch von der Firma ist, solltest du sie direkt an spoof@paypal.com weiterleiten. Auffällig sind etwa Anreden wie „Sehr geehrter PayPal-Kunde". Denn das Unternehmen spricht seine User immer mit Vor- und Nachname an.

Die EU-Datenschutzreform

Derzeit gelten in den 28 EU-Staaten 28 unterschiedliche Datenschutzgesetze, doch das soll sich ändern. Trotzdem wird eine für alle Staaten geltende, einheitliche Datenschutzverordnung frühestens 2018 in Kraft treten. Mit der Reform werden die Rechte der Verbraucher gestärkt. Zum Beispiel durch

- das Löschenlassen personenbezogener Daten und Bilder
- Beschwerdemöglichkeiten im eigenen Land bei Problemen mit internationalen Firmen
- weitreichende Informationen über die Nutzung erhobener Daten
- empfindliche Strafzahlungen für Konzerne bei Verstößen

Links zum Thema Datenschutz

Österreichische Datenschutzbehörde: dsb.gv.at
Österreichischer Datenschutzrat: bundeskanzleramt.at/site/6417/default.aspx
Datenschutz in der EU: ec.europa.eu/justice/data-protection/index_de.htm
Initiative für sicheren Umgang mit dem Internet: saferinternet.at
Verein für Internet-Benutzer Österreichs: vibe.at
Plattform für digitale Rechte: netzpolitik.org
Europe vs. Facebook: europe-v-facebook.org/DE/de.html
Big Brother Awards: bigbrotherawards.at

Impressum

Herausgeber und Medieninhaber VKI, Mariahilfer Straße 81, 1060 Wien, ZVR-Zahl 389759993
Verlags- und Herstellungsort Wien | Printed in Austria | Foto Digital Storm/Shutterstock.com
Druck Holzhausen Druck GmbH, 2120 Wolkersdorf

Diese Broschüre entstand im Rahmen der „Action 670702 – ECC-NET AT FPA", für welche das Europäische Verbraucherzentrum Österreich Förderungen aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014-2020) erhält. Der Inhalt dieser Broschüre wurde vom Europäischen Verbraucherzentrum Österreich erstellt und liegt allein in dessen Verantwortungsbereich. Sie reflektiert weder die Ansichten der Europäischen Kommission noch der Agentur für Verbraucher, Gesundheit und Lebensmittel (Chafea) oder irgendeiner anderen Einrichtung der Europäischen Union. Die Europäische Kommission und die Agentur für Verbraucher, Gesundheit und Lebensmittel (Chafea) übernehmen keinerlei Verantwortung für eine mögliche Verwendung von Informationen, die dieser Broschüre zu entnehmen sind. Obwohl diese Broschüre mit größter Sorgfalt verfasst worden ist, kann der Verfasser dieser Broschüre für mögliche Irrtümer oder Unvollständigkeiten nicht haftbar gemacht werden.

Co-funded by the European Union

Rat und Hilfe für Verbraucher in Europa
ECC-Net
Europäisches Verbraucherzentrum Österreich