Neue Spielregeln für den Datenschutz

Das bringt die EU-Datenschutz-Grundverordnung

Rat und Hilfe für Verbraucher in Europa

ECC-Net

Europäisches Verbraucherzentrum Österreich

Mag. Georg Mentschl
Leiter des Europäischen
Verbraucherzentrums Österreich

Liebe Leserin, lieber Leser!

Datenschutz ist in aller Munde. Und kaum jemand hat noch den Überblick, welches Unternehmen persönliche Daten gespeichert oder diese gar weitergegeben hat. Ob die Kundenkarte im Supermarkt, die Mitgliedschaft in einem Fitnesscenter oder die Teilnahme an einem Preisausschreiben – Daten werden überall gesammelt und weiterverarbeitet. Mit der neuen Datenschutzgrundverordnung (DSGVO) sind Unternehmen verpflichtet, Auskunft über die Verwendung bzw. Weitergabe von persönlichen Daten zu geben und diese sorgfältiger zu behandeln.

Die wichtigsten Regelungen der DSGVO – u.a., wie Sie die Löschung personenbezogener Daten beantragen können (samt einem Musterbrief dazu) und Tipps, wie man sich gegen die Datensammlerei wehren kann – haben wir auf den nächsten Seiten für Sie zusammengestellt. Piktogramme zu den einzelnen Themen weisen Ihnen den Weg durch die neuen Datenschutzregelungen, die Ihnen künftig mehr Rechte einräumen.

Wer gute Informationen hat, ist bekanntlich im Vorteil. Das sieht auch die Generaldirektion für Justiz der Europäischen Kommission so, die das Zustandekommen dieser Publikation finanziell unterstützt.

Weitere nützliche Informationen zu Konsumententhemen finden Sie auf www.europakonsument.at, der Website des Europäischen Verbraucherzentrums Österreich.

Die mit 25. Mai 2018 gültige EU-Verordnung zum Thema Datenschutz bringt strengere Regelungen in Bezug auf die Erhebung und Verarbeitung von personenbezogenen Daten.

Es war ein zähes Ringen: Jahrelang diskutierten Politiker, Lobbyverbände, IT-Konzerne und Verbraucherschützer über die Angelegenheit und stritten sich in langwierigen Debatten darüber. Sage und schreibe 4.000 Änderungsanträge, so viele wie noch nie in der Geschichte der EU, haben die Verhandlungen weiter in die Länge gezogen. Herausgekommen ist eine Verordnung (EU-Datenschutz-Grundverordnung, kurz DSGVO), die eine große Herausforderung für alle darstellt, aber neue Maßstäbe in Sachen Datenschutz setzt. Sie tritt am 25. Mai 2018 in Kraft.

Mit der neuen DSGVO gibt es erstmals ein einheitliches Datenschutzrecht in allen EU-Staaten. Die Verordnung soll einerseits die Verbraucher schützen und andererseits die Unternehmer-Interessen wahren. Sie geht uns alle an, sowohl privat als auch im Beruf, überall und jeden Tag. Denn ohne den Austausch und den Handel von Daten wäre das moderne Leben nicht denkbar.

Die neue Gesetzeslage räumt Ihnen als Konsument eine Reihe an Rechten ein, was den Umgang mit Ihren Daten betrifft: Sie müssen von nun an leichteren Zugang zu den über Sie gesammelten Daten bekommen, egal ob diese auf Servern in Österreich, in der EU oder irgendwo in Übersee liegen. Wenn Ihre Daten in ein Nicht-EU-Land gelangen, muss vorher Ihre Zustimmung eingeholt werden. Außerdem haben Sie Anspruch auf eine klare und leicht verständliche Information darüber, wer Ihre Daten zu welchem Zweck wo und in welcher Form verarbeitet. Sie können Daten „mitnehmen" und sich gegen die Verwendung unrichtiger oder unerwünschter Datensätze leichter zur Wehr setzen. Und Sie können verlangen, dass Daten gelöscht werden. Personenbezogene Daten, insbesondere solche von Kindern, sind ausdrücklich zu schützen. So sieht die neue DSGVO vor, dass die Nutzung von Internetdiensten wie Facebook, WhatsApp, Snapchat oder YouTube für unter 16-Jährige nur mit elterlicher Zustimmung erlaubt ist.

EU-Datenschutz-Grundverordnung

Unternehmen in der Pflicht

Zu den wichtigsten Neuerungen gehören:

Das Recht auf Information: Wer personenbezogene Daten speichert, hat die Pflicht, die Betroffenen darüber zu informieren – sowohl, wenn er diese selbst erhebt, als auch, wenn er sie von Dritten erhält. Er muss ihnen mitteilen, wer welche Daten, wo, wie, wann und wieso erhebt und wie lange sie gespeichert werden. Falls Daten von Dritten hinzukommen, müssen auch diese Quellen angegeben werden; ebenso, wenn Daten an Dritte weitergegeben werden.

Das Recht auf Auskunft: Jeder EU-Bürger hat Anspruch auf Auskunft darüber, was über ihn gespeichert wird. Binnen eines Monats nach der Antragstellung muss der Datensammler dem Interessierten Zugang dazu gewähren und eine kostenlose Kopie sämtlicher über ihn gesammelten Daten liefern. Die Antragstellung kann schriftlich oder sogar mündlich erfolgen. Wichtig dabei ist nur, dass ein Identitätsnachweis erbracht wird.

Das Recht auf Löschung: Über diesen auch „Recht auf Vergessenwerden" genannten Anspruch wurde schon 2014 im Zuge einer Klage gegen Google vom Europäischen Gerichtshof entschieden. Mit der neuen DSGVO ist er nun europaweit kodifiziert. Damit steht jedem Betroffenen das Recht zu, seine Daten löschen zu lassen. Generell sind Datensammler verpflichtet, selbige zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr notwendig sind – oder unverzüglich, wenn die betroffene Person ihre Einwilligung widerruft.

Das Recht auf Korrektur: Wenn die über Sie erhobenen Daten falsch sind, haben Sie das Recht, sie berichtigen oder ergänzen zu lassen.

Das Recht auf Widerspruch: Sie können der Verarbeitung Ihrer personenbezogenen Daten zu Vermarktungszwecken oder aus anderen Gründen, die sich aus Ihrer besonderen Situation ergeben, widersprechen.

Das Recht auf Einschränkung der Verarbeitung: Sie können von einem Datensammler verlangen, seine Tätigkeit einzuschränken – etwa, wenn Sie sich nicht sicher sind, ob die gesammelten Infos richtig sind. Oder wenn Sie vermuten, dass die Verarbeitung unrechtmäßig ist.

Das Recht auf Übertragung: Auf Ihre Veranlassung muss ein Unternehmen die über Sie gespeicherten Daten an ein anderes übermitteln. Das ist beim Wechsel eines Dienstleisters wie beispielsweise Telefonanbieter, Versicherung oder Onlineshop sehr sinnvoll.

Als **Mindestalter** für die Abgabe einer rechtwirksamen Einwilligung zur Verarbeitung personenbezogener Daten sieht die neue Verordnung 16 Jahre vor, wobei die einzelnen Mitgliedstaaten niedrigere Altersgrenzen festsetzen können. Österreich sieht in seinem Anpassungsgesetz das vollendete 14. Lebensjahr vor. Teenagern wird dadurch die Anmeldung bei Diensten wie WhatsApp oder Instagram theoretisch erschwert. Auch in Sachen **Datensicherheit** legt die neue DSGVO genaue Spielregeln fest. Verstöße wie etwa Hacks müssen innerhalb von 72 Stunden gemeldet werden, und zwar sowohl bei der Datenschutzbehörde als auch bei den Personen, deren Daten betroffen sind. Außerdem müssen die Unternehmen bzw. Organisationen dafür sorgen, dass die von ihnen gespeicherten Daten sicher verwahrt sind.

Bei Verstößen gegen die genannten Punkte drohen **Strafen**. Der Beschluss zur Umsetzung der DSGVO in Österreich sieht jedoch eine weit mildere Vorgehensweise vor als von der EU geplant: Demnach muss zunächst verwarnt werden, bevor eine Strafe erfolgt. Zudem müssen die Geldbußen verhältnismäßig sein. Schließlich sieht Österreich einige Ausnahmen vor: Für die Wissenschaft, Medien und Behörden gelten gelockerte Bestimmungen.

Ihr Recht auf Information und Zugang

Wissen, was Sache ist

In der EU dürfen nur mehr Daten gesammelt werden, die zur Erfüllung des Zwecks, für den sie bestimmt sind, notwendig sind. Um das zu überprüfen, gibt es das Recht auf Auskunft.

Generell müssen Unternehmen und Organisationen gemäß der neuen DSGVO bei ihrer Datensammelei nach dem **Minimalprinzip** und der **Zweckbindung** vorgehen, sprich: Nur jene Daten dürfen gespeichert werden, die für die Erfüllung des jeweiligen Zwecks tatsächlich erforderlich sind. In diesem Zusammenhang ist auch von der **Datensparsamkeit** die Rede.
Bei Anwendungen im Internet ist diesbezüglich auch die sogenannte **Privacy by Design** („Datenschutz durch Technikgestaltung") bzw. **Privacy by Default** („Datenschutz durch datenschutzfreundliche Voreinstellungen") geboten. Zum Beispiel müssten Browser demgemäß von vornherein auf die datenschutzfreundlichste Art und Weise programmiert und voreingestellt sein. Ein Beispiel für einen mit Daten sehr sorgsam umgehenden Browser ist Cliqz. Seine integrierte Suchmaschine für das deutschsprachige Web setzt eine andere Technik ein als Google und überzeugt mit treffsicheren und oft nützlicheren Ergebnissen als jene Browser, welche die Suche auf die jeweilige Person abstimmen. Bei der Verwendung von Firefox haben Sie die Möglichkeit, durch sogenannte Erweiterungen (Add-ons) Anpassungen zugunsten des Datenschutzes vorzunehmen.
Tipp: Bei Suchmaschinen gibt es mit Startpage und DuckDuckGo gute Alternativen zu Google.

Sobald Sie personenbezogene Daten preisgeben, haben Sie das Recht, bestimmte **Informationen** von jener Stelle zu erhalten, die sie sammelt. Diese Informationen müssen präzise, transparent und verständlich formuliert sein. Dazu gehören:

- der Name dieser Firma oder Organisation
- der Zweck, für den sie die Daten erhebt und verarbeitet
- die Kategorien der Daten, die verarbeitet werden
- die Rechtsgrundlage aufgrund derer das geschieht
- die Dauer der Speicherung
- ob die Infos an Dritte weitergegeben werden
- ob Daten in Länder außerhalb der EU fließen
- Ihre Datenschutzrechte
- Ihr Recht auf Beschwerde bei einer Datenschutzbehörde
- Ihr Recht, Ihre Einwilligung wieder zurückzuziehen
- ob eine automatisierte Entscheidungsfindung (einschließlich Profiling) besteht
- ob sich der Zweck der Datenverarbeitung möglicherweise ändern kann

Treffen Computersysteme mithilfe Ihrer Daten automatisierte Entscheidungen, die Sie betreffen, dann können Sie beantragen, dass sich künftig eine natürliche Person in den Entscheidungsprozess einschaltet. Beispiele dafür wären eine Online-Beantragung eines Kredites oder ein automatisiertes Verfahren zur Jobvergabe.

Von Ihrem Recht auf **Zugang** zu den über Sie vorliegenden personenbezogenen Daten können Sie jederzeit Gebrauch machen. Sie können jede Firma oder Organisation, mit der Sie einmal in Kontakt waren, anschreiben und fragen, welche Daten über Sie gespeichert worden sind und wie diese verwendet werden. Manche Firmen oder Behörden haben einen eigenen Datenschutzbeauftragten als Ansprechpartner, andere eine eigens eingerichtete Maske auf ihrer Website. Eine vorgeschriebene Form zur Vorgangsweise gibt es nicht. Entscheidend ist nur, dass Sie Ihre Identität nachweisen können.

Was muss offengelegt werden?

Ist der Antrag eingebracht, hat das Unternehmen maximal einen Monat Zeit, dem Anfragenden eine kostenlose Kopie sämtlicher über ihn gesammelten Daten zu liefern. Darin muss die Firma alle über die Person gespeicherten Daten angeben. Auf Verlangen muss sie auch bekannt geben, woher sie die Daten hat.
Tipp: Das Recht auf Zugang bestand schon vor Inkrafttreten der neuen DSGVO – allerdings gab es damals keine Fristen. Datenkraken wie Facebook haben das ausgenutzt und es den Antragstellern so schwer wie möglich gemacht. Meist haben sie zunächst nur kleine Datenschnipsel herausgerückt und gehofft, dass sich die Betroffenen damit zufriedengeben. Nur diejenigen, die nicht lockergelassen haben, haben nach Monaten oder gar Jahren mehr Daten erhalten. Bleiben Sie hartnäckig – nützt das nichts, dann melden Sie den Fall am besten der Datenschutzbehörde.

Das Recht auf Löschung

Die Freiheit, Spuren zu verwischen

Im Internet finden sich Informationen über Sie, die Sie lieber privat halten möchten? Sie wollen, dass ein Unternehmen all Ihre Daten von seinen Servern löscht? Sie bekommen persönlich adressierte Werbung, kennen das Unternehmen aber nicht? Es gibt Möglichkeiten, zu reagieren.

Zunächst einmal müssen Unternehmen der neuen Verordnung zufolge Daten prinzipiell löschen, sobald sie den Zweck, für den sie erhoben wurden, erfüllt haben. Zudem hat die betroffene Person jederzeit das Recht, ihre Einwilligung zur Datenverarbeitung zu widerrufen. Auch wenn nie eine Einwilligung zur Datenverarbeitung eingeholt wurde, was leider noch oft passiert, kann widerrufen werden.

Löschen überhaupt möglich?

Was genau die Verordnung unter „Löschung" versteht, ist nicht näher definiert. Datenträger wie CDs oder Akten sind physisch zu zerstören. Bei wiederbeschreibbaren Datenträgern wie Festplatten ist eine spezielle Software einzusetzen. In der Praxis dürften komplette Löschungen jedenfalls oft schwierig sein – zumal Daten meist noch in Backups gespeichert sind oder mit anderen Daten verknüpft werden und sich dabei wie ein Sandkorn in der digitalen Wüste „verflüchtigen".

Löschantrag bei Google

Mit im Durchschnitt 700 Anfragen pro Tag trudeln die meisten Löschanträge beim Suchmaschinenbetreiber Google ein. Wer dort Daten aus den Trefferlisten entfernt haben möchte, für den hat das Unternehmen eine eigene Maske mit dem Titel „Löschung aufgrund des europäischen Datenschutzes" eingerichtet, zu finden unter dem Suchbegriff „Legal Removal Requests". Freilich prüft Google die Anfragen, bevor es Infos aus seinen Listen entfernt. Das macht auch Sinn. Denn ansonsten würde die mit dem Internet gewonnene Informationsfreiheit wohl einer Welle der Zensur zum Opfer fallen. Löschanträge können prinzipiell an jedes Unternehmen gestellt werden, sie sind keinen strengen formalen Normen unterworfen. Nur die Erbringung eines Identitätsnachweises ist Pflicht, etwa mit einem beigelegten Scan des Ausweises. Ein Löschantrag könnte wie folgt aussehen:

Absender
(Vorname, Nachname,Straße, Hausnummer,Postleitzahl, Ort)

Adressat
(Firmenbezeichnung, Adresse, E-Mail, Datum)

Löschung meiner personenbezogenen Daten

Sehr geehrte Damen und Herren,
ich bitte Sie, gemäß Art. 17 der Datenschutzgrundverordnung (DSVGO) alle Daten, die Sie von mir gespeichert haben, unverzüglich zu löschen. Darüber hinaus möchte ich sichergestellt wissen, dass die Löschung auch von jenen Stellen durchgeführt wird, denen Sie meine Daten übermittelt haben.

Bitte bestätigen Sie mir kurz, dass die Datenlöschung umfänglich vollzogen wurde. Sollten Sie dieses Schreiben ignorieren, werde ich mich an die Datenschutzbehörde wenden. Außerdem behalte ich mir weitere rechtliche Schritte vor.

Mit freundlichen Grüßen

(Unterschrift)

Tipp: Sie schicken ein solches Schreiben aus Beweisgründen am besten per Einschreiben ab!

Maßnahmen gegen Spam

Vor unerwünschten Werbenachrichten per Post, Mail, SMS oder Anruf schützt sich der Nutzer in erster Linie mit seinem eigenen Hausverstand. Personenbezogene Daten sollten niemals leichtfertig und im Web nur auf seriösen Seiten herausgegeben werden. Einhalt geboten wird Spam auch mit einem kostenlosen Eintrag in die sogenannte ECG-Liste der Rundfunk und Telekom Regulierungs-GmbH (per Mail an: eintragen@ecg.rtr.at). Gegen per Post versandte Direktwerbung können Sie sich mit dem bekannten „Keine Werbung-Pickerl" am Postfach und mit einem Eintrag in die Robinsonliste vom Fachverband Werbung wehren (per Mail an: werbung@wko.at).
Tipp: Eine gute Adresse für alle datenschutzrechtlichen Anliegen ist neben der Datenschutzbehörde (und den Verbraucherschutzverbänden) die von Max Schrems ins Leben gerufene Non-Profit-Plattform noyb (noyb.eu). Ihr Kernziel ist es, die mit der neuen DSGVO gewonnenen Rechte durchzusetzen.

Widersprechen, korrigieren,

Die Dinge in die Hand nehmen

Neben dem Recht auf Löschung können Sie auch das Recht auf Widerspruch, Korrektur oder Einschränkung der Verarbeitung in Anspruch nehmen. Auch die Mitnahme von Daten bei einem Anbieterwechsel muss per Gesetz leicht möglich sein.

Ihre Daten können Sie nicht nur komplett löschen lassen. Sie können auch eine Korrektur von falschen oder unrichtigen auf Sie bezogenen Informationen veranlassen. Zudem können Sie einfordern, dass Datensammler ihre Tätigkeit einschränken. Dieses Recht ist für all jene Fälle gedacht, in denen ein Unternehmen einer Löschung nicht nachkommen kann – z.B., wenn es die Daten aus rechtlichen Gründen nicht löschen darf. Es muss dabei aber sicherstellen, dass die Daten nicht mehr weiterverwendet werden, auch von Dritten nicht, an die es sie möglicherweise weitergegeben hat. Das Recht auf Widerspruch gegen eine Verarbeitung personenbezogener Daten kann ebenfalls jederzeit in Anspruch genommen werden. Dadurch können beispielsweise lästige Direktwerbemaßnahmen verhindert werden.

Tipp: Wer aus datenschutzrechtlichen Gründen auf den Komfort der elektronischen Gesundheitsakte **ELGA** verzichten möchte, der muss Widerspruch beim Hauptverband der österreichischen Sozialversicherungsträger einlegen. Wer sich schon einmal gefragt hat, woher die **GIS** ihre Daten bekommt: Ihr ist gemäß dem Rundfunkgebührengesetz ein privilegierter Zugang zu den Daten der Meldebehörden eingeräumt. Mit einem Widerspruch ist in diesem Fall nichts zu erreichen.

Anbieterwechsel leicht gemacht

Ein Recht, das sich für die meisten als nützlich erweisen dürfte, ist jenes auf die Übertragbarkeit von Daten. Unternehmen sind verpflichtet, personenbezogene Daten auf Wunsch Ihnen oder anderen Verantwortlichen in strukturiertem, maschinenlesbarem Format zu übergeben. Dieses Recht auf Datenmitnahme soll Verbrauchern einen Anbieterwechsel erleichtern – etwa, wenn sie einen Umstieg bei sozialen Netzwerken, Film- oder Musikportalen, Mail-Providern, Cloud-Anbietern, Treue- oder Bonuskarten oder Apps vollziehen möchten.

Eine Mär ist indes, dass Unternehmen seit Inkrafttreten der neuen DSGVO mit Datenhandel kein Geld mehr verdienen dürfen. Längst lukrieren Datenkraken Milliarden von Euro damit und es ist ihnen auch weiterhin erlaubt, sofern sie sich an die geltenden Gesetze halten. Demgemäß dürfen sie Daten auch an Dritte weitergeben. Sie müssen die Betroffenen allerdings darüber in ihren Nutzungsbedingungen informieren.

Apropos Nutzungsbedingungen: Jeder kennt sie, keiner liest sie. Studien zufolge sehen sich die wenigsten die Allgemeinen Geschäftsbedingungen an, bevor sie einen Dienst oder eine Plattform in Anspruch nehmen. Dabei würde es sich lohnen, diese zumindest zu überfliegen, da sich Firmen in den AGB allerhand bewilligen lassen.

Tipp: Geben Sie im digitalen AGB-Text in der Suchfunktion (Strg + F) Schlüsselwörter wie „Daten", „Verarbeitung" oder „Weitergabe" ein und lesen Sie dann die entscheidenden Passagen.

Videoüberwachung: Kameras, Drohnen, Dashcams

Um selbst keinen datenschutzrechtlichen Verstoß zu begehen, gilt es, einige Dinge zu beachten, wenn Instrumente eingesetzt werden, die beobachtende Aufgaben übernehmen können. Wer eine **Videoüberwachungsanlage** im privaten Bereich installiert, muss dies mit einigen Ausnahmen der Datenschutzbehörde melden (beim DVR Datenverarbeitungsregister, siehe dsb.gv.at). Die Anlage muss außerdem mit einem Hinweisschild versehen werden. Öffentlicher Grund darf von Privaten gar nicht überwacht werden oder eben nur soweit es für den Zweck der Überwachung des genehmigten privaten Bereiches zwingend notwendig ist.

einschränken

Die im privaten Gebrauch immer beliebter werdenden **Drohnen** können sowohl unter das Luftfahrtgesetz als auch unter das Datenschutzrecht fallen – unter Letzteres jedoch nur, wenn sie mit einer Kamera ausgestattet sind und personenbezogene Daten aufnehmen. Dann besteht ebenfalls Meldepflicht beim DVR. Eine Drohne mit Kamera, die nicht aufzeichnen kann, muss nicht gemeldet werden. Der Einsatz von **Dashcams** (Kameras, die aus einem Auto heraus aufzeichnen) ist hierzulande nicht erlaubt.
Die DSGVO wird derzeit noch von vielen Unternehmen missachtet. So wurde etwa 2017 in über 1.000 Apps eine versteckte Anwendung gefunden, die Nutzer über das Mikrofon des Smartphones belauscht. Die Daten, die eine Software namens Alphonso erhob, wurden an die Werbeindustrie weiterverkauft. Geahndet werden diese Überschreitungen aber immer noch viel zu selten. Die Datenschutzbehörde ist in ihrer aktuellen Besetzung kaum in der Lage, all dem nachzukommen. Die eigens dafür gegründete Non-Profit-Organisation NOYB ist noch in der Etablierungsphase, und für Einzelne ist es teuer und kompliziert, gegen Rechtsverletzungen vorzugehen.

Viele nehmen so etwas einfach in Kauf. Ein kostenloser und komfortabler Service, wie ihn Google oder Facebook bieten, muss mit Daten bezahlt werden, so ein in dem Zusammenhang häufig vorgebrachtes Argument. Es ist auch nicht falsch.

Foto: Mediaparts/Shutterstock.com

Die ePrivacy-Verordnung

Die ePrivacy-Verordnung ist ein Spezialfall: Sie ist besonders bedeutend, weil sie die oft allgemeinen und abstrakten Vorgaben der DSGVO in vielen Fällen konkret macht. Ursprünglich sollte sie zeitgleich mit 25. Mai 2018 in Kraft treten. Doch nach derzeitigem Stand der Dinge ist frühestens 2019 mit einem Inkrafttreten zu rechnen – und noch unklar ist, in welcher Form.

In ihrem ursprünglichen Entwurf sieht die Verordnung eine wesentliche Einschränkung bei Protokollier-Tätigkeiten im Internet vor. User dürften dann nur noch mit ihrer ausdrücklichen Einwilligung mit Cookies und anderen Techniken on- und offline – etwa durch analog gewonnene Einkaufsdaten – verfolgt (im IT-Jargon: „getrackt") werden. Das würde einem Aus für maßgeschneiderte Werbung im Internet gleichkommen. Die Richtlinie sieht auch ein Recht auf Verschlüsselung vor. Kommunikationsanbieter müssen sich demnach verpflichten, ihre Software stets auf dem aktuellen Stand zu halten. Vorgesehen ist derzeit auch, dass Regierungen die Kommunikation nicht einsehen dürfen, was wiederum mit dem neuen „Sicherheitspaket" der österreichischen Bundesregierung nicht vereinbar wäre.

Dass die Daten den Konzernen Millionen an Einnahmen bringen, sollte dennoch zum Nachdenken anregen – oder zumindest bewusst machen, dass Daten einen Wert haben. Nicht umsonst bezeichnen IT-Experten Daten gerne als das neue Gold.
Unaufhaltsam ist jedenfalls der Trend hin zu noch mehr datengetriebenen Technologien. Die Ära des **Internet of Things**, dem Internet der Dinge, ist längst angebrochen. Fast schon Standard sind mittlerweile die smarten Fernseher. Wobei Untersuchungen gezeigt haben, dass Hacks in die Systeme dieser Geräte selbst für Amateure keine große Sache sind. Bedauerlicherweise kommt das Thema Datensicherheit bei vielen technischen Innovationen immer noch erst an hinterer Stelle. Potenzielle Einfallstore für Betrüger werden allzu oft erst geschützt, wenn die Geräte schon am Markt sind.

So auch beim aktuellen Verkaufsrenner, den smarten Lautsprechern von Amazon und Google. Sind Alexa & Co erst einmal gehackt, steht die Wanze mitten im Wohnzimmer. Die Behauptung der Anbieter, dass die Spracherkennung erst auf Zuruf funktioniere, darf angezweifelt werden.

Letztendlich liegt es auch an den Nutzern, wie datenschutzfreundlich künftige Technologien sein werden. Sie können Einfluss nehmen, indem sie nicht jede Neuerung gleich kritik- und bedenkenlos annehmen und sich bei Verstößen zur Wehr setzen.

Die wichtigsten Tipps im Umgang mit Ihren Daten

Schützen Sie Ihren Computer. Halten Sie Betriebssystem und Programme mit automatischen Updates aktuell, verwenden Sie Virenschutzsoftware und Firewall und verschlüsseln Sie Ihre WLAN-Verbindung.

Geben Sie grundsätzlich nicht zu viel von sich preis. Was Sie nicht von sich hergeben, kann auch nicht verbreitet werden. Seien Sie zurückhaltend bei Fotos, Videos und Texten in den sozialen Medien. Das Internet vergisst nichts. Einmal veröffentlichte Daten sind nur schwer oder gar nicht mehr zu entfernen.

Persönliche Daten geheim halten. Wohnadresse, Telefonnummer, Passwörter etc. gehen Fremde nichts an. Wo immer möglich, verwenden Sie einen anonymen Nickname anstelle Ihres richtigen Namens.

Sichere Passwörter verwenden. Sichere Passwörter bestehen aus einer Kombination aus mindestens acht Buchstaben, Zahlen und Sonderzeichen. Verwenden Sie unterschiedliche Passwörter für unterschiedliche Benutzerkonten. Diese sollten sich voneinander unterscheiden und keine Verbindung zu Ihrer Person zulassen.

Achten Sie auf Verschlüsselung der Daten. Eine sichere Verbindung mit einem Server an den Sie Daten übermitteln, erkennen Sie an dem Beginn der Adresszeile mit „https:"

Aufpassen bei E-Mails. E-Mails mit unbekanntem Absender, Links und Anhänge sind ein Risiko. Bei Verdacht sollten Sie Links nicht anklicken, Anhänge nicht öffnen und Ihren PC mit einer aktuellen Virensoftware scannen.

Vorsicht bei der Nutzung öffentlicher Computer. Lassen Sie sich bei der Eingabe von Daten nicht von Fremden über die Schulter schauen. Speichern Sie keine Login-Daten und melden Sie sich vom PC immer ab („Logout").

Es muss nicht immer Google sein. Die großen Suchmaschinen im Netz, insbesondere Google, fangen Daten Ihrer Suchanfragen ab. Wenn Sie die Datensammelei reduzieren wollen, sollten Sie die Suchmaschine für Ihre Recherchen im Internet regelmäßig wechseln.

Cookies löschen. Auf den meisten Webseiten hinterlassen Sie Spuren durch sogenannte „Cookies". Diese können Sie über die Browsereinstellungen löschen bzw. können Sie Cookies von Drittanbietern grundsätzlich blockieren.

Festplatten sicher löschen. Bevor Sie Ihren Rechner verkaufen oder entsorgen, sollten Sie Ihre Daten endgültig löschen, damit diese nicht wiederhergestellt werden können (z.B. mit einem Daten-Shredder). Auch vor dem Verkauf von Smartphones und Tablets sollten persönliche Daten unwiderruflich entfernt werden.

Rat & Hilfe kostenlos

Europäisches Verbraucherzentrum Österreich, Mariahilfer Straße 81, A-1060 Wien
www.europakonsument.at
www.facebook.com/europakonsument.at

EUROPA-HOTLINE 01 / 588 77 81
Mo bis Fr von 9 bis 12.30 Uhr
E-Mail: info@europakonsument.at

Rat und Hilfe für Verbraucher in Europa
ECC-Net
Finanziell unterstützt durch die Europäische Union

Eine Initiative der Europäischen Kommission und des VKI

Impressum

Herausgeber und Medieninhaber
Verein für Konsumenteninformation
Mariahilfer Straße 81, 1060 Wien
ZVR-Zahl 389759993
Verlags- und Herstellungsort Wien
Grafische Gestaltung VKI/Herstellung
Cover-Foto Sashkin / Shutterstock.com
Druck Leykam Druck GmbH & Co KG, 7201 Neudörfl

Diese Broschüre wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert. Der Inhalt reflektiert lediglich die Ansichten des Autors/der Autorin und liegt in seiner/ihrer alleinigen Verantwortung; er reflektiert nicht die Ansichten der Europäischen Kommission und/oder der Exekutivagentur für Verbraucher, Gesundheit, Landwirtschaft und Lebensmittel (Chafea, Luxemburg) oder irgendeiner anderen Einrichtung der Europäischen Union. Die Europäische Kommission und die Agentur übernehmen keinerlei Verantwortung für eine mögliche Verwendung von Informationen, die dieser Broschüre zu entnehmen sind. Weitere Informationen zum ECC-Net finden Sie im Internet unter: http://ec.europa.eu/consumers/ecc/index_de.htm