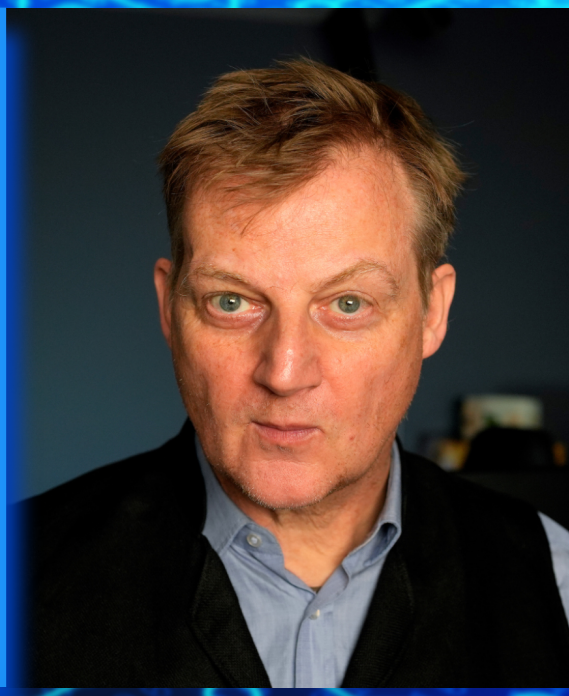
So geht's leichter...



So gebt Ihr weniger Daten preis

- Das Konzept Datensparsamkeit
- Weniger Daten in Social Media
- Datensammler abschalten
- Datensparsam im Internet
- Gespeicherte Daten löschen lassen

Jörg Schieb

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion schieb.de
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de

So geht's leichter
So gebt Ihr weniger Daten preis

Inhalt

So geht's leichter
So gebt Ihr weniger Daten preis

So geht’s leichter
So gebt Ihr weniger Daten preis

Datensparsamkeit: Weniger ist mehr

In einer Welt, in der das Teilen und Sammeln von Informationen so einfach geworden ist (zumindest für große Konzerne), dass wir es kaum noch bemerken, ist das Konzept der sogenannten Datensparsamkeit wichtiger denn je. Motto: Je weniger Daten wir über uns selbst preisgeben, umso besser.

Doch was bedeutet Datensparsamkeit eigentlich und warum sollten wir uns darum kümmern? Lassen Sie uns diese Reise beginnen, um zu verstehen, wie wir durch bewusstes Teilen unserer Daten nicht nur unsere eigene Privatsphäre, sondern auch die unserer Mitmenschen schützen können.

Was ist Datensparsamkeit?

Einfach ausgedrückt, bedeutet Datensparsamkeit, so wenig persönliche Informationen wie möglich preiszugeben. Es ist die Kunst des bewussten Umgangs mit unseren Daten im digitalen Zeitalter.

Stellen Sie sich das wie eine Diät für Ihre Daten vor: Sie geben nur das Nötigste von sich preis und halten alles Übrige zurück. Dies kann bedeuten, nicht jedes Detail Ihres Lebens in sozialen Medien zu teilen, vorsichtig zu sein, welche Apps Sie nutzen und welche Berechtigungen Sie ihnen erteilen, oder auch einfach mal nein zu sagen, wenn eine Website nach Ihrer E-Mail-Adresse fragt.

Warum ist Datensparsamkeit wichtig?

In der heutigen vernetzten Welt sind Daten das neue Gold. Unternehmen, Werbetreibende und sogar Regierungen haben ein großes Interesse daran, so viel wie möglich über uns zu erfahren. Mit diesen Informationen können sie unser Verhalten vorhersagen, uns

So geht’s leichter
So gebt Ihr weniger Daten preis

gezielt Werbung schicken oder politische Kampagnen gestalten. Aber diese Sammelwut hat auch eine Kehrseite: Je mehr Daten über uns gesammelt werden, desto anfälliger sind wir für Missbrauch, Betrug und Überwachung.

Vorteile der Datensparsamkeit im Alltag

1. **Schutz der Privatsphäre:** Indem Sie weniger Daten teilen, schützen Sie Ihre Privatsphäre. Sie entscheiden, wer was über Sie weiß, und behalten die Kontrolle über Ihre persönlichen Informationen.
2. **Reduzierung des Risikos von Datenmissbrauch:** Weniger geteilte Daten bedeuten ein geringeres Risiko, dass Ihre Informationen in falsche Hände geraten. Dies kann von Identitätsdiebstahl bis hin zu gezielten Phishing-Angriffen reichen.
3. **Verbesserung der digitalen Hygiene:** Datensparsamkeit zwingt uns, unsere digitalen Gewohnheiten zu überdenken und zu verbessern. Dies kann von der Überprüfung der App-Berechtigungen bis hin zur Verwendung sicherer Passwörter reichen.
4. **Weniger digitale Ablenkung:** Weniger Zeit in sozialen Medien zu verbringen oder gezielte Werbung zu vermeiden, kann zu weniger Ablenkung und einem stressfreieren Alltag führen.
5. **Einfluss auf Unternehmen und Politik:** Je mehr Menschen Datensparsamkeit praktizieren, desto mehr werden Unternehmen und Regierungen gezwungen, ihre Datensammlungspraktiken zu überdenken und möglicherweise zu ändern.

So geht’s leichter
So gebt Ihr weniger Daten preis

Wie können Sie Datensparsamkeit im Alltag umsetzen?

1. **Bewusster Umgang mit sozialen Medien:** Überlegen Sie zweimal, bevor Sie persönliche Informationen oder Fotos teilen. Nicht jedes Detail Ihres Lebens muss online sein.
2. **Überprüfung der App-Berechtigungen:** Sehen Sie sich an, welche Berechtigungen Ihre Apps haben, und überlegen Sie, ob diese wirklich notwendig sind.
3. **Verwendung von Datenschutztools:** Nutzen Sie Tools wie VPNs, ad blockers und anonyme Suchmaschinen, um Ihre Spuren im Internet zu verwischen.
4. **Vorsicht bei Online-Formularen:** Geben Sie nicht bei jeder Gelegenheit Ihre E-Mail-Adresse oder Telefonnummer an. Fragen Sie sich, ob diese Informationen wirklich notwendig sind.
5. **Regelmäßige Überprüfung Ihrer Daten:** Überprüfen Sie regelmäßig, welche Informationen über Sie im Internet verfügbar sind, und löschen Sie, was nicht öffentlich sein muss.

Datensparsamkeit ist kein Trend, sondern eine Notwendigkeit in unserer zunehmend digitalisierten Welt. Durch bewusstes Handeln können wir nicht nur unsere eigene Privatsphäre schützen, sondern auch ein Zeichen setzen gegen die unkontrollierte Sammelwut von Daten. Denken Sie daran: In der Welt der Daten ist weniger oft mehr.

Indem wir alle einen kleinen Beitrag leisten, können wir eine große Wirkung erzielen. Beginnen wir also heute, unsere digitale Diät zu planen und umzusetzen. Es ist ein Schritt in Richtung eines sicheren, privaten und gesünderen digitalen Lebens

So geht’s leichter
So gebt Ihr weniger Daten preis

Wissen ist Macht. Wenn andere zu viel wissen – vor allem über uns! –, dann macht das was!

Daten haben einen Wert, und der ist nicht gering. Zum einen auf Grund der Bedrohungen, die sich daraus ergeben: Zielgerichtete Angriffe, Ausspähen, ja sogar der Diebstahl einer kompletten Identität werden umso einfacher, je mehr Daten von euch öffentlich verfügbar sind.

Zum anderen auch monetär: Eure Daten erzielen für die, die sie sammeln, echtes Geld. Damit Unternehmen damit zielgerichtet Werbung an Euch ausrollen können und mehr Umsatz machen, für den Aufbau von Datenbanken, die genaue Einblicke in das Leben von Menschen bestimmter Altersklassen, Ausbildungen, sozialer Umgebungen und mehr geben bis hin zu Cyberkriminellen, die für eure entwendeten Passwörter und Zahlungsdaten richtig Geld bieten.

So geht's leichter
So gebt Ihr weniger Daten preis

Konten einrichten und nutzen: Sparsam!

Der Begriff der Datensparsamkeit ist nicht unbekannt, aber im Allgemeinen reaktiv gedacht: Vorhandene Daten zu löschen, um möglichst wenig über euch öffentlich zu machen, ist eine sehr gute Idee. Dazu findet ihr später noch die wichtigsten Tipps.

Was allerdings oft untergeht: Ihr gebt schon beim Anlegen eines Kontos viel mehr Informationen ein, als tatsächlich nötig sind. Der Datenschutz schreibt eigentlich „Datensparsamkeit" vor, also das Erfassen von nur so vielen Daten, wie wirklich benötigt werden. Den Anbietern aber ist das meist recht egal: Je mehr Daten die haben, desto genauer können sie euch mit Werbung versorgen. Und auch später solltet ihr genau darauf achten, welche Daten Apps und Konten teilen:

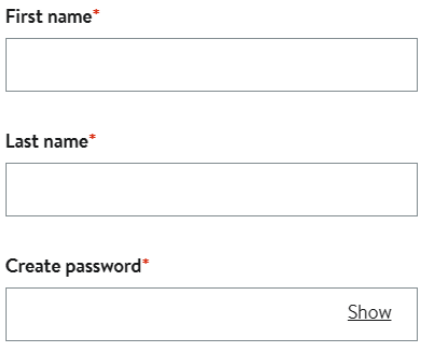
Der Trick mit dem Stern: Pflichtangaben

Die Unterscheidung zwischen nötigen und unnötigen Angaben ist für den Anwender nicht leicht: Diese definiert der Anbieter. Der Standard ist aber, dass bestimmte Felder beim Anlegen eines Kontos verpflichtend sind. Daran könnt ihr nichts ändern, auch wenn diese nicht unbedingt logisch für euch sein müssen.

So geht’s leichter
So gebt Ihr weniger Daten preis

Daten sparen beim Anlegen des Kontos

- In den ersten Schritt werden Basisinformationen abgefragt wie der Name und Vorname, Email-Adresse und auch das Geburtsdatum. Letzteres wird sicherlich nicht immer wirklich nötig sein, die Anbieter verargumentieren meist, dass sie ja sicherstellen müsst, dass ihr volljährig seid.
- In dieser Phase versteckt sich gerne auch die Werbeeinwilligung: Wenn ihr einen Haken bei „Ich möchte Werbung bekommen“ (oder einer ähnlichen Formulierung) setzt, dann erteilt ihr die Freigabe, euch mit Werbung zuzuspammen. Wenn ihr das wollt: Es steht euch frei. In der Regel aber lasst den Haken, das stellt auch sicher, dass einiges an Informationen über eure Vorliegen und euer Verhalten im Internet bei euch bleiben.



- Nachdem ihr die Basisinformationen eingegeben habt, wollen die Anbieter größtenteils noch möglichst viele weitere Informationen von euch haben. Hier unterscheidet genau, welche ihr weitergeben wollt.
- Im Standard sind die verpflichtenden Informationen (bei einem Versandhändler beispielsweise die Lieferadresse. Diese sind in den meisten Fällen mit einem roten Stern gekennzeichnet.
- Diese verpflichtenden Informationen müssen gefüllt sein, sonst kommt ihr im Registrierungsprozess nicht weiter.

So geht's leichter
So gebt Ihr weniger Daten preis

- Alle anderen Felder lasst einfach frei, es sei denn, ihr wollt explizit, dass der Anbieter sie kennt. Damit könnt ihr viele Daten einsparen.

Und später?

Einen Versuch ist es wert: Manche Anbieter überprüfen das Vorliegen der Pflichtangaben beim Anlegen des Kontos. Und manche dieser Pflichtangaben sind auch nur dafür wichtig. Ein Beispiel? Wenn ein Händler euch eine SMS schickt, um eure Handynummer zu verifizieren, er sie aber nicht weiter benötigt.

- Geht die Benutzerkonten der Dienste, die ihr angelegt habt, regelmäßig durch und löscht Informationen, die nicht nötig sind.
- Bei Pflichtfeldern kann es sinnvoll sein, irgendwelche Informationen anzugeben. Beispielsweise Einmal-E-Mail-Adressen oder ungültige Handynummern.
- Seid euch aber darüber bewusst, dass dann manchmal bestimmte Funktionen nicht mehr verfügbar sind. Unter anderem die Passwort-Wiederherstellung.
- Noch wichtiger: Geht regelmäßig die angelegten Konten durch und löscht die, die ihr nicht mehr braucht. Eure Daten sind dann im Zweifel zwar immer noch beim Anbieter gespeichert, eine Anmeldung (beispielsweise mit Euren gehackten Zugangsdaten) ist dann aber nicht mehr möglich.

Familieneinstellung vornehmen

Windows ist das Standard-Betriebssystem, das auf den meisten im Handel vertriebenen PCs vorinstalliert ist. Auch für Kinder und Jugendliche bleibt also keine Alternative. Deren Daten sind aber

So geht's leichter
So gebt Ihr weniger Daten preis

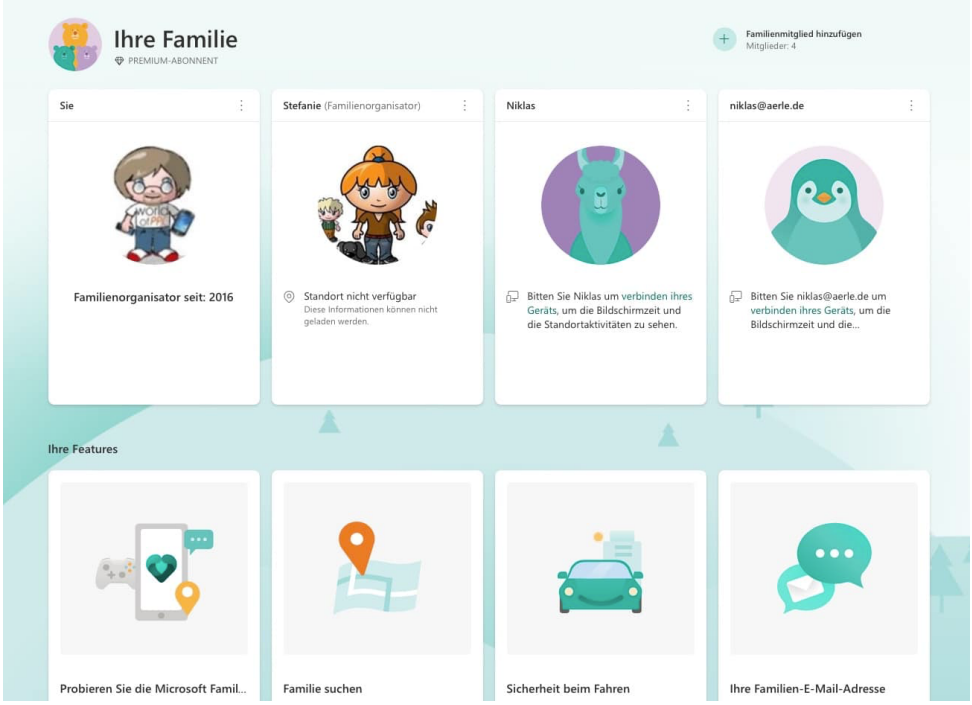
gegebenenfalls noch ein wenig kritischer als die der erwachsenen Anwender. Wem dies Sorge bereitet, der sollte sich die Familieneinstellungen anschauen.

Die Familie - auch unter Windows

Familie ist allgemein ein wichtiges Gut. Das kennt ihr aus dem normalen Leben, und warum sollte es am PC anders sein? Oft ist es so, dass ihr in der Familie eine Person habt, die IT-affiner ist als die anderen. Die euch regelmäßig damit nervt, dass ihr ja Dinge anders machen könntet, Sicherheitsrisiken eingeht und vieles mehr. Ärgert euch nicht, sondern macht einfach den einfach zum Familienmanager. Das macht vor allem Sinn, wenn ihr einen Jugendlichen oder ein Kind an einen PC lassen wollt.

Die Voraussetzung: Alle zugehörigen Microsoft-Konten müssen bereits angelegt sein, dann erst können sie in das Familienkonstrukt aufgenommen werden.

So geht’s leichter
So gebt Ihr weniger Daten preis



Festlegen der Rechte der Kinder/Jugendlichen

Der Ausgangspunkt für alle Familieneinstellungen ist das Family-Portal, das ihr unter diesem Link erreicht. Meldet euch mit dem Microsoft Account des Familienverwalters an, dieser bekommt dann automatisch die Administratorenrolle zugewiesen.

- Klickt auf das Plus neben **Familienmitglied hinzufügen**, um ein bestehendes Konto hinzuzufügen.

- Gebt die E-Mail-Adresse des hinzuzufügenden Kontos ein, dann wählt aus, ob dieses Konto

So geht's leichter
So gebt Ihr weniger Daten preis

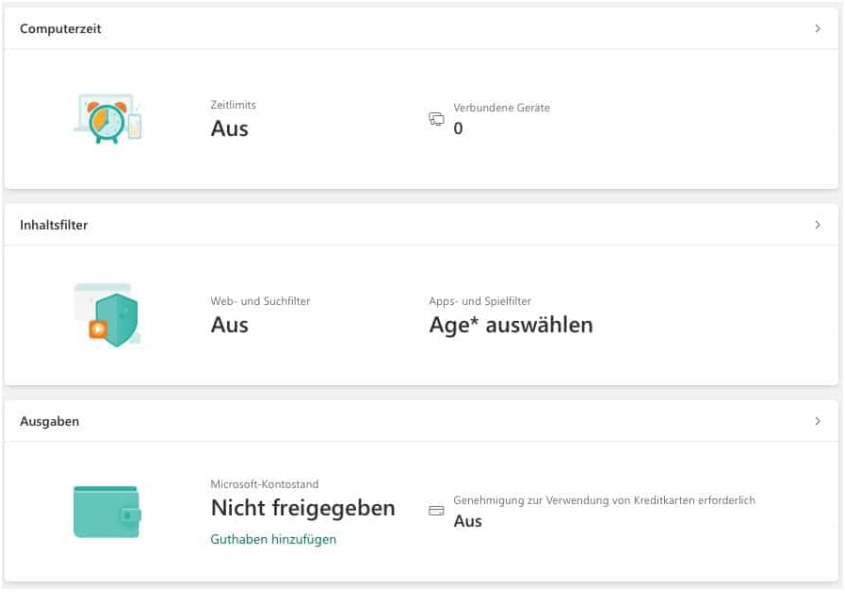
ein (verwaltetes) Mitglied sein soll oder ein weiterer Administrator.

- Folgt den Anweisungen auf dem Bildschirm.

Um nun die Berechtigungen und Kontrollmöglichkeiten einzurichten, klickt auf die drei Punkte oben rechts in der Kachel des zu verwaltenden Kontos, dann

- Klickt auf Zustimmung verwalten. Diese Option ist eigentlich nur für das Entfernen der Zustimmung des Elternteils zu dem Kinderkonto an sich, darunter verbergen sich aber auch die anderen Optionen.
- Klickt auf **Jugendschutz anzeigen**. Wichtig ist hier, dass mindestens ein Gerät (PC oder Notebook) mit dem Microsoft-Account angemeldet ist).
- Unter **Computerzeit** könnt ihr einstellen, wie lange der PC am Tag benutzt werden darf.
- Unter **Inhaltsfilter** könnt ihr festlegen, welche Inhalte aus welchen Kategorien verwendet werden dürfen. Das funktioniert mit Microsoft Edge, der ja der Standardbrowser in Windows ist.
- Unter **Ausgaben** gebt ihr ein Limit fest für die monatlichen Ausgaben im Windows Store und anderen Microsoft zugeordneten kostenpflichtigen Quellen an.

So geht’s leichter
So gebt Ihr weniger Daten preis



Teams: Nur gewünschte Informationen teilen

Wenn ihr mit Microsoft Teams arbeitet, dann teilt ihr nicht nur die Daten aus der Besprechung mit anderen Anwendern, sondern auch die eine oder andere Zusatzinformation. Das könnt und solltet ihr nur wissentlich tun!

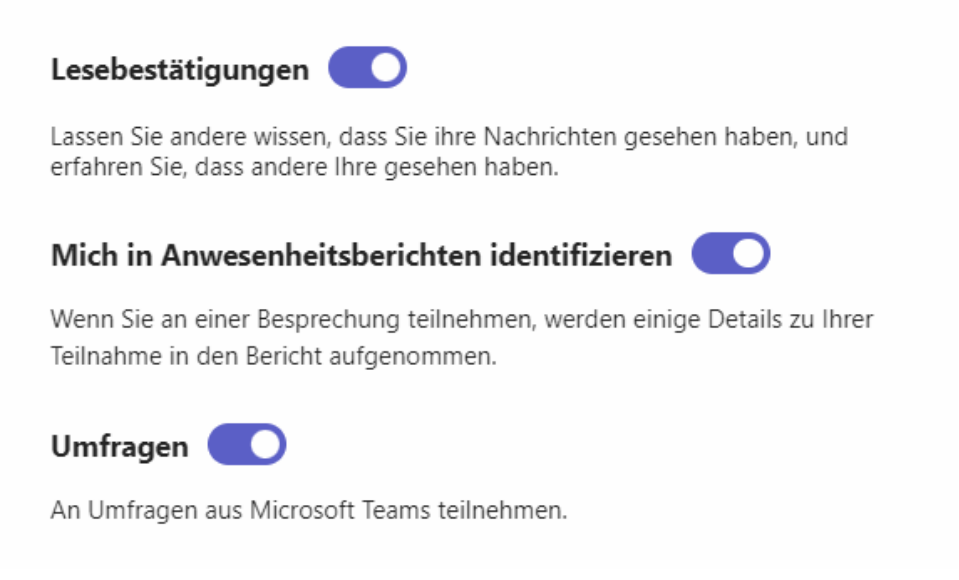
Vertraulich sollte vertraulich bleiben

Teams wird immer mehr zur Alternative zum persönlichen Gespräch und löst dieses in vielen Fällen gar ganz ab. Die Tatsache, dass ihr eigentlich alleine seid, und die anderen Teilnehmer nur virtuell dabei sind, führt schnell zu Unvorsichtigkeit: Ihr teilt Informationen, die nicht für alle Anwendenden gedacht sind, weil ihr im Zweifel gar nicht merkt, wer alles an dem Termin teilnimmt.

- Versichert euch über die Liste der Teilnehmer, welche Benutzergruppen im Termin sind und was diese wissen dürfen.

So geht's leichter
So gebt Ihr weniger Daten preis

- Achtet beim Teilen von Dokumenten darauf, dass es deutlich mehr auffällt, wenn eine Person eine Leinwand in einem Besprechungsraum abfotografiert, als wenn sie in ihrem eigenen Büro ein Bildschirmfoto von vertraulichen Unterlagen macht!



Welche Informationen teilt ihr unwissentlich?

Teams geht bei manchen Informationen einfach davon aus, dass ihr diese teilen wollt, auch wenn das nicht der Fall ist. Zwei Dinge solltet ihr hier kontrollieren und die Einstellungen vornehmen, die eurem Verständnis von Datenschutz entsprechen:

- Dazu wechselt in die Teams-Einstellungen, indem ihr auf die drei Punkte neben eurem Kontaktbild oben rechts und dann auf **Einstellungen** tippt.
- Klickt in der rechten Leiste auf **Datenschutz**.

Im Normalfall zeigt Teams den anderen Teilnehmern eines Chats an, wenn ihr eine Nachricht gelesen habt. Der Kreis mit dem Haken neben der Nachricht (der erst nur die erfolgreiche Zustellung anzeigt, wird

So geht's leichter
So gebt Ihr weniger Daten preis

dann ausgefüllt). Das führt oft dazu, dass ihr Beschwerden bekommt, warum ihr nicht auf die Nachricht antwortet, obwohl ihr sie gelesen habt. Egal, ob ihr sie nur versehentlich gesehen habt oder überhaupt keine Zeit zur Antwort hattet. Wenn ihr das vermeiden wollt, denn deaktiviert **Lesebestätigungen**.

Zu den Verwaltungsinformationen, die Teams zu einer Besprechung führt, gehören auch Daten zu eurer Teilnahme: Wer ihr seid, wie lange ihr teilgenommen habt und einige Informationen mehr werden automatisch gespeichert. Das ist nicht immer in eurem Sinn, ihr müsst es aber auch nicht hinnehmen: Deaktiviert in den Datenschutzeinstellungen einfach die Option **Mich in Anwesenheitsberichten identifizieren**, um das zu verhindern.

Die richtigen Daten im Kalender teilen

Wenn ihr in einem Team gemeinsam arbeitet, dann kommt es oft auch darauf an, gemeinsam Termine abzustimmen. In Outlook könnt ihr Kalender freigeben. Da können kleine Fehler aber große Auswirkungen haben! Beispielsweise, wenn der nicht besonders nette Kollege sieht, dass ihr ein Bewerbungsgespräch habt!

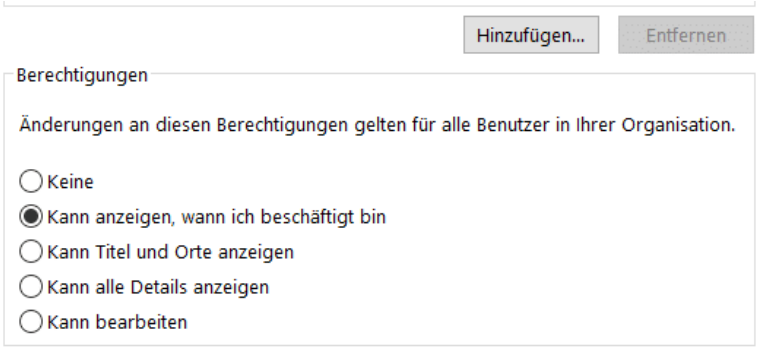
Freigabe von Kalendern

Um einen Kalender in Outlook freizugeben, geht wie folgt vor:

- Klickt in Outlook auf das Symbol des **Kalenders** unten in der Symbolleiste.
- Links in der Spalte seht Ihr dann euren Kalender.
- Klickt mit der rechten Maustaste darauf, dann auf **Freigabeberechtigungen**.

So geht's leichter
So gebt Ihr weniger Daten preis

- Outlook zeigt euch die aktuellen Berechtigungen für andere Benutzer in einer Liste an.
- Klickt auf **Hinzufügen**, um eine neue Freigabe hinzuzufügen.



Wichtig sind hier die Berechtigungsstufen, die ihr für den hinzugefügten Benutzer festlegen müsst:

- **Keine:** Der Benutzer sieht nur eine graue Linie als euren Kalender, aber nicht mal die Frei-/Belegt-Zeiten.
- **Kann anzeigen, wann ich beschäftigt bin**: Der Benutzer sieht die Balken von Terminen und die Art des Termins (Belegt, unter Vorbehalt, außer Haus), aber keine Titel.
- **Kann Titel und Orte anzeigen**: Die Option gibt euch Zugriff auf die Details der Termine im Kalender, aber nicht auf Teilnehmer, Anhänge oder andere Inhalte. Das wird die am meisten verwendete Freigabeform sein.
- **Kann alle Details anzeigen**: Jedes einzelne Detail des Kalenders liegt den Benutzern offen, die diese Berechtigung haben, inkl. aller anhängenden Dokumente. Hier solltet ihr genau abwägen, ob das nicht zu weitgehend ist. Beispielsweise, wenn vertrauliche Dokumente in den Terminen hängen.

So geht's leichter
So gebt Ihr weniger Daten preis

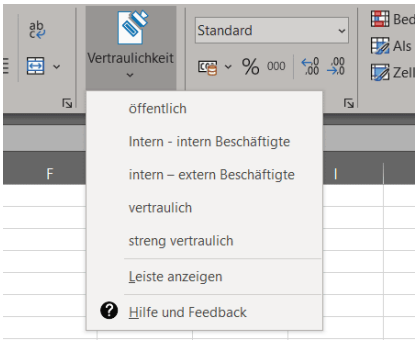
All diese Freigaben sind rein lesende Freigaben, der Benutzer, der sie erhält, kann an eurem Kalender nichts ändern. Das geht erst, wenn ihr **Kann bearbeiten** anwählt.

Wenn es sich bei dem einzurichtenden Vertreter handelt (und keine Benutzergruppe), dann könnt ihr eine zusätzliche Option anwählen: **Stellvertreter**. Dieser hat dann nicht nur alle Rechte auf die Elemente des Kalenders, sondern kann zusätzlich auch noch in eurem Namen Termine versenden.

Azure Information Protection

Wem dürft Ihr ein Dokument zeigen? Oft steht das irgendwo im Dokument mit Vermerken wie "Vertraulich" oder "Öffentlich". Microsoft gibt mit der Azure Information Protection (AIP) eine Möglichkeit, das direkt im Dokument als Attribut zu verankern.

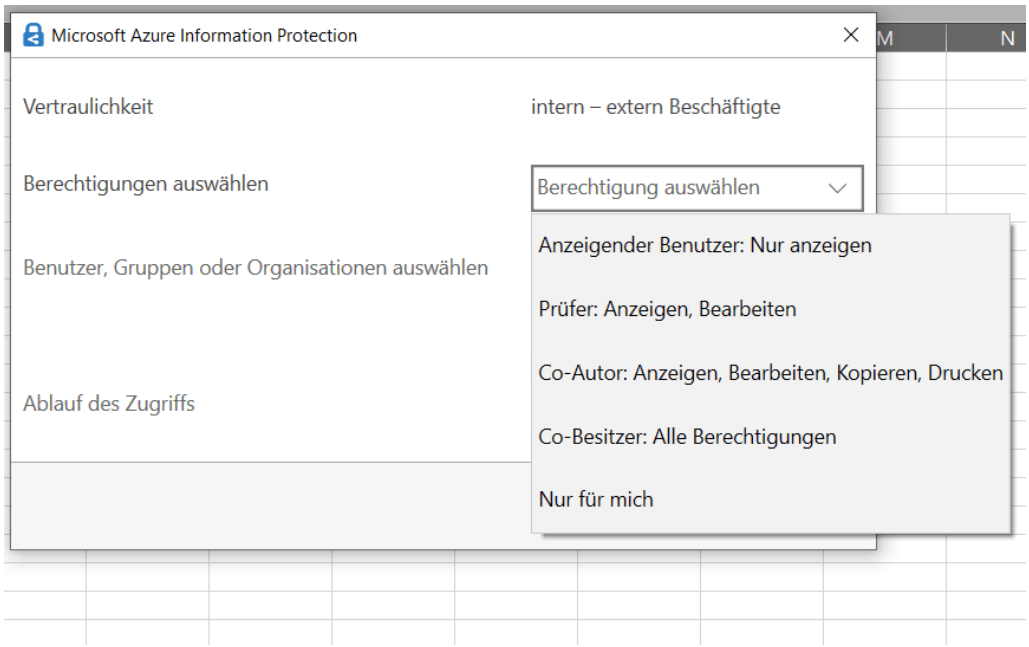
Im privaten Umfeld werdet Ihr das Problem selten vorfinden, wenn aber nur der Hauch von Vertraulichkeit in euren Dokumenten vorhanden ist, dann ist das euer täglich Brot: Im Verein, in der Firma, mit dem Steuerberater oder Anwalt. Da gibt es dann verschiedene Vertraulichkeitsstufen:



öffentlich: Jeder darf das Dokument lesen
intern: Nur interne Benutzer (intern im Sinne einer Firma, Kanzlei etc.)
vertraulich: Nur bestimmte, festlegbare Personen dürfen das Dokument lesen.
streng vertraulich: Nur bestimmte, vorher festgelegte Personen dürfen das Dokument lesen.

So geht's leichter
So gebt Ihr weniger Daten preis

In der Azure Information Protection (die unter Microsoft 365/Azure vom Administrator installiert und aktiviert werden muss) könnt Ihr diese Klassifizierung direkt über das Symbol Vertraulichkeit in der Symbolleiste der E-Mail vornehmen.



Hier ist der **intern-Status** noch einmal unterteilt in intern beschäftige und extern Beschäftigte. Das berücksichtigt, dass beispielsweise in einem Projekt sowohl der Firma zugehörige als auch von externen Firmen eingekaufte Benutzer als intern gelten können.

Wenn Ihr die Funktion häufiger nutzt, dann klickt einmal im Menü auf **Leiste anzeigen**, dann wird aus dem Symbol in der Symbolleiste eine immer dargestellte Leiste mit den Informationsklassifizierungen.

So geht's leichter
So gebt Ihr weniger Daten preis

Kommunikation und Social Networks

Datenschutz wird oft reduziert auf die rein technischen Aspekte: Passwörter, Firewalls, Antiviren-Programme und vieles mehr sind ohne Frage wichtig und dürfen nicht vernachlässigt werden, aber mindestens genauso wichtig sind die weichen Faktoren. Beispielsweise das Mitteilungsbedürfnis der Anwender. Dazu müsst ihr nur einmal mit offenen Augen und Ohren mit dem Zug fahren: Da stehen Notebooks mit Umsatzstatistiken auf dem Bildschirm offen herum, Berater telefonieren lauthals mit Kollegen und reden über ihre Kunden und vieles mehr.

Elektronische Kommunikation ist uns so in Fleisch und Blut übergegangen, dass wir wenig darüber nachdenken. Wie schnell ist eine E-Mail verschickt und versehentlich der falsche Adressat oder das falsche Dokument angehängt?

Oder nehmt die sozialen Netzwerke: Was ihr darin veröffentlicht, können viel mehr Menschen lesen, als wenn ihr eine E-Mail schreibt. Informationen, die auf diesem Weg einmal in der Welt sind, sind kaum ungeschehen zu machen.

Technisch lassen sich die weichen Faktoren kaum kontrollieren. Ihr können aber Vorkehrungen treffen, die es unwahrscheinlicher machen, dass Eure Informationen an die falschen Empfänger kommen und damit ebenfalls Daten einsparen!

Pannen bei E-Mails vermeiden

E-Mails trotz des Vormarsches der Messenger-Dienste immer noch ein wichtiges Kommunikationsmedium. Besonders kritisch, weil ihr oft nicht nur kurze Texte austauscht, sondern auch Dokumente mit teils

So geht's leichter
So gebt Ihr weniger Daten preis

vertraulichem Inhalt anhängen. Trefft Vorkehrungen, damit dabei möglichst wenig schiefgehen kann!

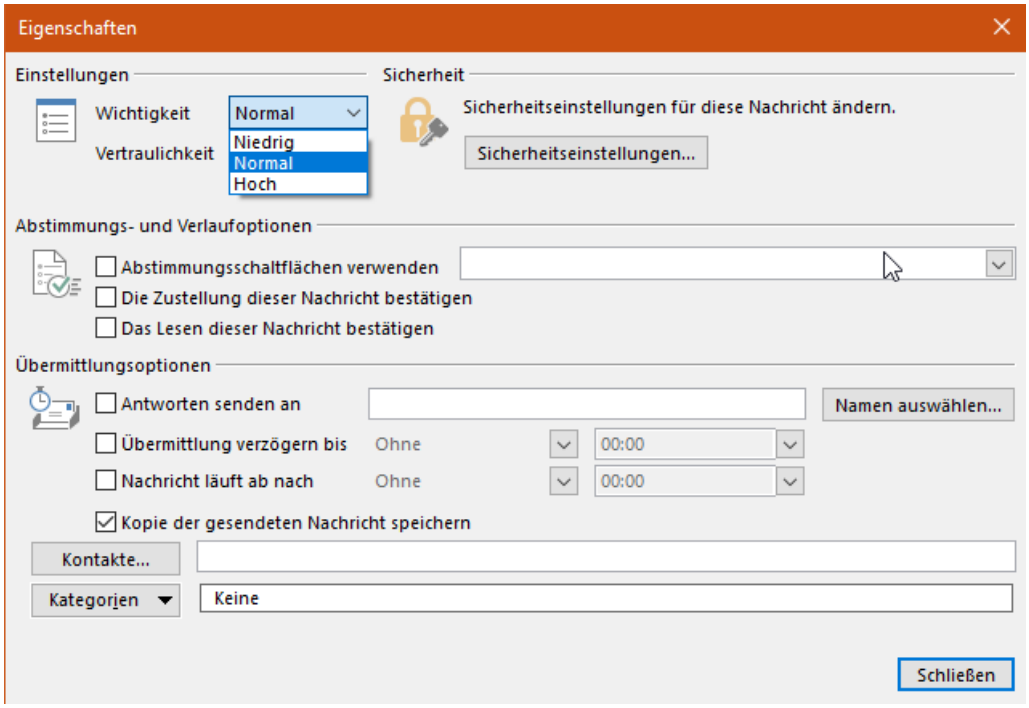
Wichtigkeit, Vertraulichkeit Verschlüsselung von E-Mails

Eine E-Mail besteht nicht nur aus den Verwaltungsinformationen. Natürlich sind Empfänger, Betreff und der Mailkörper wichtig, weil sie die Informationen transportieren. Zusätzlich könnt ihr aber noch einige Einstellungen vornehmen, die nahezu unsichtbar mit versendet werden und dem Empfänger weitere Informationen liefern.

- Zum Inhalt der Mail gibt es drei große Bereiche, die ihr beeinflussen können. Nicht jede E-Mail ist gleich wichtig, und so könnt ihr eine zusätzliche Kennzeichnung mitgeben, die dem Empfänger Aufschluss darüber gibt.

- Unter **Markierungen** in der Symbolleiste einer neuen E-Mail könnt ihr unter **Wichtigkeit** zwischen **Normal**, **Niedrig** und **Hoch** auswählen. Normal ist die Standardeinstellung. Wenn ihr dem Empfänger sagen wollt, dass die Bearbeitung nicht eilig ist, ist niedrig die richtige Wahl. Auf der anderen Seite hoch, wenn es pressiert!

So geht's leichter
So gebt Ihr weniger Daten preis



- Parallel dazu könnt ihr unter **Vertraulich** festlegen, dass die E-Mail vertraulich behandelt werden soll. Damit untersagt ihr beispielsweise eine Weiterleitung an Andere.
- Die dritte Möglichkeit ist die Verschlüsselung von E-Mails. Im Standard versendet Outlook E-Mails im Klartext. Das klingt schlimmer, als es ist, denn der Transfer zwischen den E-Mail-Servern ist im Normalfall schon verschlüsselt.
- Unter **Sicherheitseinstellungen** könnt ihr die E-Mail an sich aber noch einmal verschlüsseln. Dazu muss aber ein Zertifikat installiert sein. Das macht am besten der Administrator, der das E-Mail-System aufgesetzt hat.

Vorsicht bei Massenmailings

Mailingliste, Newsletter, Exceltabellen mit Mitgliederdaten: Tolle Möglichkeiten, vielen Menschen auf einen Streich Informationen

So geht's leichter
So gebt Ihr weniger Daten preis

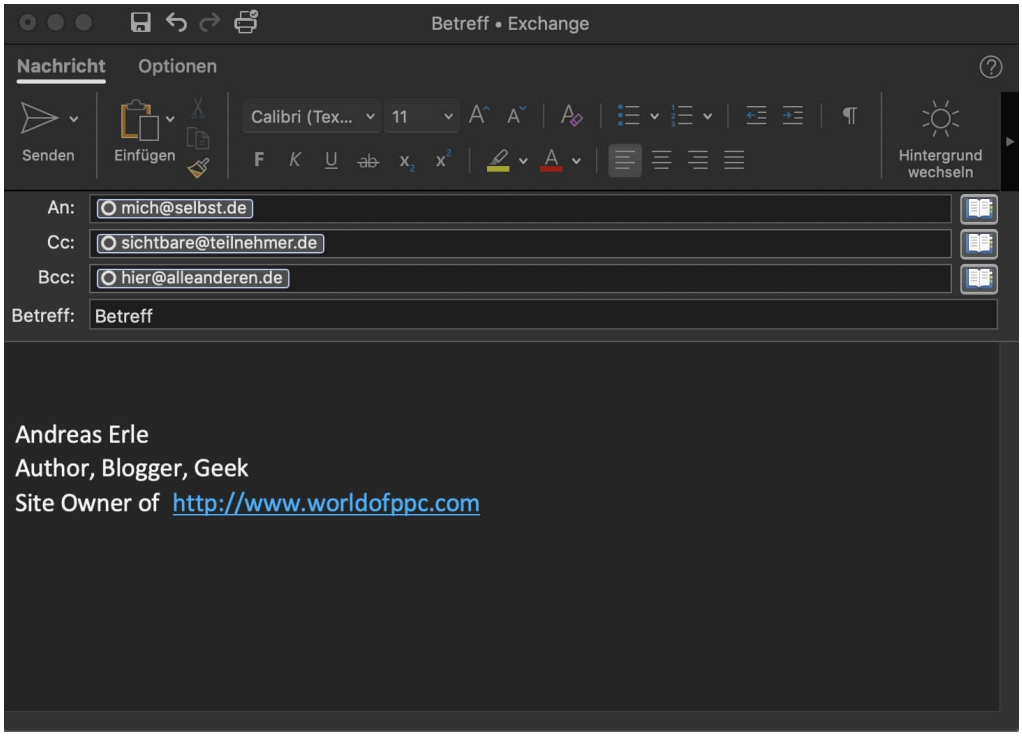
zukommen zu lassen. Was technisch so einfach scheint, ist nicht ganz so unproblematisch, wie der erste Blick vermuten lässt.

Die Zeiten von ungetrübter Massenmailfreude sind spätestens seit der Datenschutz-Grundverordnung (DSGVO) vorbei. Zumindest im nicht-privaten Bereich benötigt ihr eine rechtliche Grundlage, denn die E-Mail-Adressen sind ja auch personenbezogene Daten.

Gehen wir davon aus, dass ihr eine Grundlage für die Versendung von E-Mails an viele Adressaten gleichzeitig habt, dann solltet ihr vor allem auf zwei Dinge achten:

- **E-Mail-Empfänger bei Massen-E-Mails gehören ins BCC**: Normalerweise schreibt die Empfänger einer E-Mail in die **AN**-Zeile.
- Bei einer Massen-E-Mail solltet ihr das nicht tun, denn dann sieht jeder Empfänger jeden anderen. Das ist nicht angenehm, wenn die Empfänger sich nicht alle kennen. Datenschutzrechtlich ist es ebenfalls kritisch.
- Stattdessen schickt die Mail an euch selbst und nehmt die eigentlichen Empfänger in die **BCC**-Zeile. Dann sieht jeder Empfänger nur seine Adresse und die Ihre.

So geht’s leichter
So gebt Ihr weniger Daten preis



- **Zu viele E-Mails parallel können als SPAM angesehen werden**: Je mehr Empfänger Ihre E-Mail hat, desto mehr einzelne E-Mails werden verschickt.
- Der ein oder andere E-Mail-Server vermutet einen SPAM-Angriff und verzögert oder sperrt die Zustellung eurer E-Mail. Dann bekommt ihr in euren Posteingang eine Nachricht. Wenn das passiert, versucht beim nächsten Mal die E-Mails in kleineren Paketen zu schicken.

Verzögern des Mail-Versandes bei Outlook

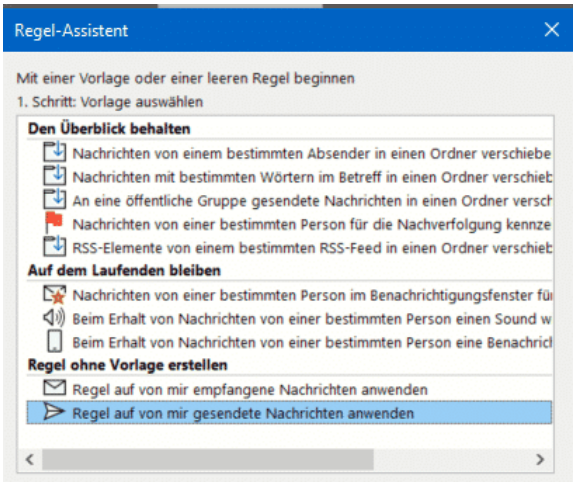
Kennt ihr die Situation? Eine Mail geht an einen riesigen Verteiler, ihr wollen dem Absender antworten und stattdessen klickt ihr auf "Allen Antworten" und die Antwort erreicht nicht einen, sondern viel zu viele Adressaten. Oder ihr stellt direkt nach Versand fest, dass der Anhang viel zu viele Daten enthält oder der Falsche für die Adressaten ist. Viel zu

So geht’s leichter
So gebt Ihr weniger Daten preis

viele Menschen, die Informationen von euch erhalten, die sie nichts angehen.

Das Zurückziehen der Nachricht hilft da leider nur sehr eingeschränkt. Oft merkt ihr den Fehler sehr schnell, da kann es helfen, wenn die Mails nicht direkt, sondern mit einer leichten Verzögerung hinausgehen.

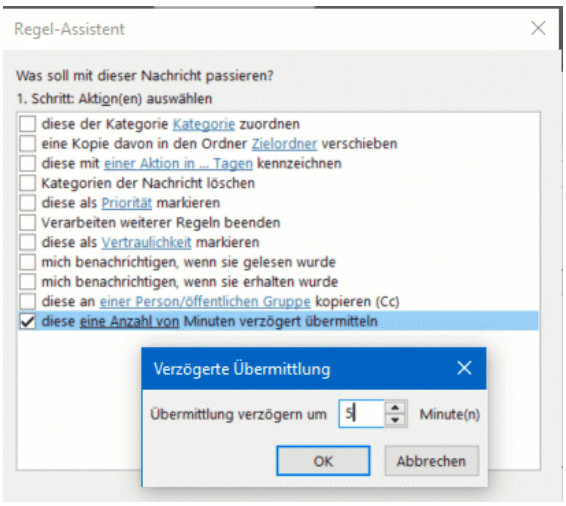
- Die Idee dabei ist simpel: Ihr sagt Outlook einfach, dass alle E-Mails, die ihr sendet, nicht direkt rausgehen sollen, sondern mit einer Verzögerung von beispielsweise 5 Minuten. Dazu bietet Outlook die Funktion der Regeln an.



- Klickt in Outlook auf **Datei** > **Regeln und Benachrichtigungen verwalten** > **Neue Regel**.
- Klickt ganz unten in der Liste auf **Regel auf von mir gesendete Nachrichten anwenden**.
- Im nächsten Bildschirm setzt keinen Haken bei den angezeigten Bedingungen. Outlook hinterfragt dann, ob diese Regel tatsächlich auf alle Nachrichten angewendet werden soll, das bestätigte dann.
- Outlook fragt jetzt nach Ausnahmen, auch hier wählt keine der Optionen an. Klickt euch sich nun bis zum Ende durch den Einrichtungsvorgang, dann bestätigt die Aktivierung der Regel.

So geht's leichter
So gebt Ihr weniger Daten preis

- Aktiviert jetzt ganz unten **diese eine Anzahl von Minuten verzögert übermitteln**.
- Klickt auf **eine Anzahl von** im Text der Aktion und gebt dann die Zahl der Minuten an, die die Übermittlung verzögert werden soll.



Ab diesem Zeitpunkt warten alle Nachrichten für 5 Minuten, nachdem ihr auf Senden geklickt habt, im Postausgang und werden erst dann versendet. Dies gilt nur den Rechner/das Outlook, in dem die Regel definiert wurde. Innerhalb dieses Zeitraums könnt ihr die E-Mail noch problemlos löschen und damit den Versand verhindern.

Privatsphäre und Anmeldungen

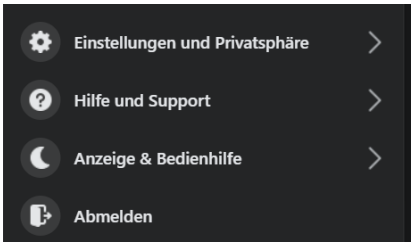
Soziale Netzwerke lassen sich aus unserem Leben kaum noch wegdenken. Facebook, Instagram, Twitter und viele mehr üben einen eigenartigen Einfluss auf uns aus: Wer hätte ohne sie den Drang verspürt, mit der Welt zu teilen, was er wann isst oder wo er gerade in welcher Stimmung etwas macht? Diese Gedanken werden uns nahezu abgenommen, weil diese Mitteilsamkeit heute zum guten Ton gehört.

Dass damit ein Risiko verbunden ist, liegt auf der Hand: Das Internet vergisst nichts, zumindest nicht übergreifend und schnell. Aus diesem Grund solltet ihr ein wenig Zeit in die Privatsphäreneinstellungen

So geht's leichter
So gebt Ihr weniger Daten preis

investieren. Die schützt nicht nur eure Privatsphäre, sondern auch die der Menschen, die ihr in euren Beiträgen markieren!

Privatsphäreneinstellungen bei Facebook



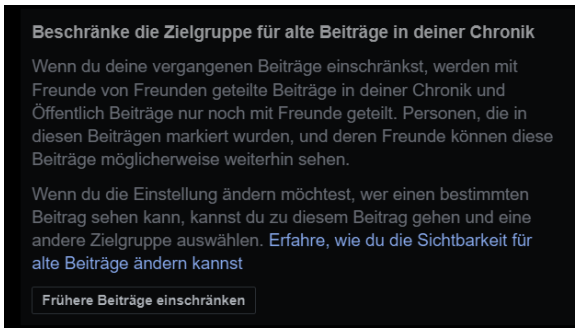
Facebook hat eine eigene Rubrik in den Einstellungen für die Privatsphäreneinstellungen.

- Klickt auf der Facebook-Webseite auf das Dreieck nach unten neben dem Profilbild, dann auf **Einstellungen und Privatsphäre**.
- Sollte der Pfad ein wenig anders aussehen: Facebook entwickelt sich kontinuierlich weiter, dabei werden auch die Menüs immer mal wieder angepasst!
- Klickt dann auf **Einstellungen** > **Privatsphäre**. Facebook zeigt euch nun eine umfangreiche Übersicht Ihrer Möglichkeiten, die Privatsphäre zu beeinflussen.

- Kontrolliert hier, dass ihr eure privaten Beiträge nicht öffentlich teilen. Das mag bei einem öffentlichen Anliegen Sinn machen, auf eure privaten Beiträge aber sollten aber nur bestimmte Personen Zugriff haben. Das könnt ihr unter **Wer kann deine zukünftigen Beiträge sehen?** festlegen.

So geht's leichter
So gebt Ihr weniger Daten preis

- Hier könnt ihre gesamte Freundesliste, eure Freundesliste außer bestimmten Personen oder gar nur bestimmte Freunde freischalten.
- Natürlich könnt ihr diese Einstellung für jeden Post auch verändern. Achtet dann nur darauf, dass Facebook nicht „zufällig" beim nächsten Post die falsche Einstellung verwendet!
- Oft ist man am Anfang noch entspannter, was die Privatsphäre angeht, der Reiz des Neuen überwiegt noch. Das macht aber nichts, denn ihr könnt die Zielgruppe für Beiträge, die für die Öffentlichkeit oder Freunde von Freunden sichtbar waren, mit einem Klick auf die Freunde einschränken. Klickt dazu auf **Frühere Beiträge einschränken** und folgt den Anweisungen.



- Vorsicht: Rückgängig machen könnt ihr dies nur, wenn ihr jeden einzelnen Beitrag wieder anpasst und freigebt!
- Wenn ihr in Beiträgen markiert seid, das aber nicht wollt, dann könnt ihr dies über das **Aktivitätenprotokoll** beeinflussen. Löscht einfach die Markierungen, die ihr nicht wollt oder gebt sie frei.

Facebook: Was sieht wer?

Kennt ihr das? "Eigentlich" achtet ihr peinlich genau darauf, dass ihr auf Facebook Beiträge nur an Freunde schickt. Und dann sagt euch jemand, mit dem ihr nicht befreundet seid: "Habe ich auf Facebook gelesen". Panik? Unnötig!

So geht's leichter
So gebt Ihr weniger Daten preis

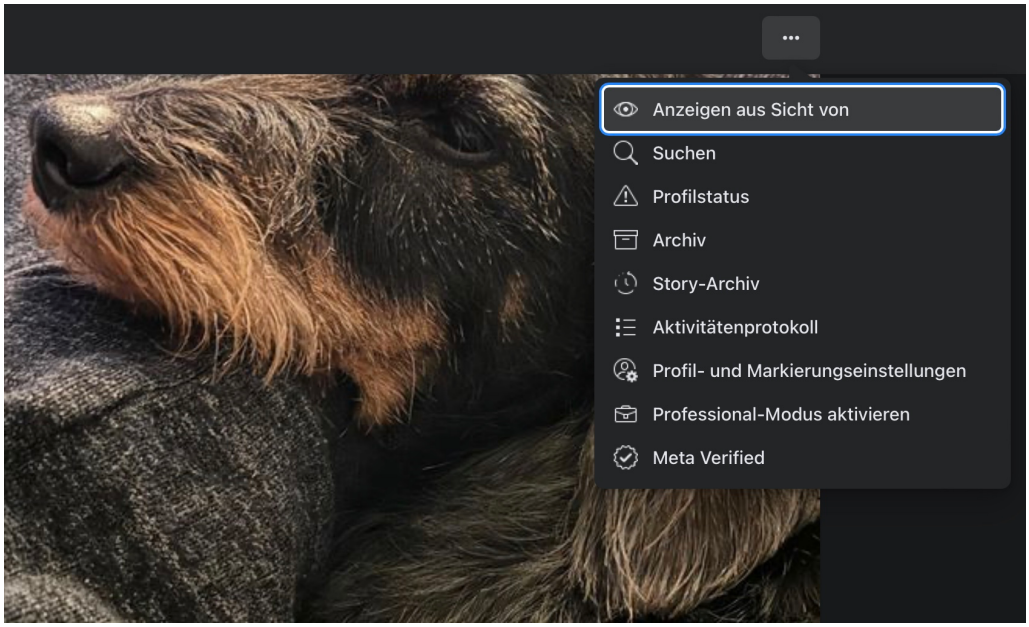
Öffentlich vs. Freunde

Facebook kennt im Großen und Ganzen drei Kategorien von Personen. Anhand dieser Kategorien wird eingeschränkt, welche Beiträge für Kontakte darin angezeigt werden:

- **Freunde**: Die Personen, mit denen ihr direkt befreundet seid. Die solltet ihr kennen, es macht aber durchaus Sinn, eure Freundesliste regelmäßig zu kontrollieren. Man weiß ja nie, wer sich da hineinschleicht oder vielleicht gar nicht mehr zum Kreis der echten Freunde und Bekannten zählt).
- **Freunde von Freunden**: Diese sind eine Zwischenkategorie. Einen direkten Zugriff auf eure Timeline könnte ihr ihnen nicht geben, in den Privatsphäre-Einstellungen von Facebook könnt ihr ihnen aber erlauben, Beiträge zu sehen, in denen Personen markiert sind, mit denen ihr und sie gleichzeitig befreundet seid.
- **Die Öffentlichkeit**: Das sind eben alle anderen Personen, die sich auf Facebook bewegen.

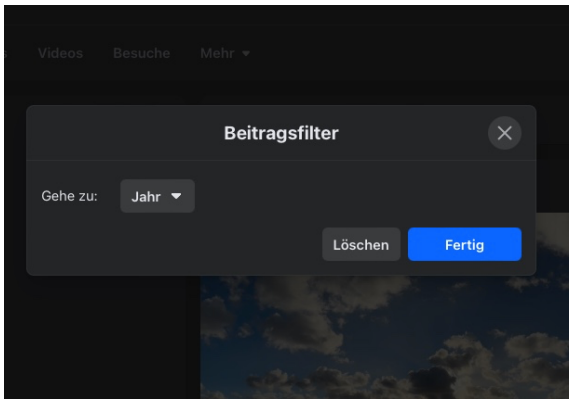
Kontrolliert regelmäßig, dass eure Privatsphäre-Einstellungen nicht auf öffentlich stehen, wenn ihr nicht tatsächlich wollt, dass jeder Fremde eure Beiträge sehen kann!

So geht’s leichter
So gebt Ihr weniger Daten preis



Öffentlich gepostet? Aber was?

Nicht selten passiert es, dass ihr einen einzigen Beitrag öffentlich posten wollt. Wenn ihr dazu die Privatsphäre-Einstellungen ändert, dann bedarf es nur einer kurzen Ablenkung, das Zurückstellen auf "Freunde" zu vergessen. Es macht Sinn, regelmäßig zu kontrollieren, welche Beiträge die Öffentlichkeit sehen kann. Das ist aber nicht so einfach zu finden:



- Öffnet die Facebook-Seite.
- Klickt auf euer **Kontobild** oben rechts auf dem Bildschirm, dann auf euren **Namen**.
- Neben den Tabs unter dem Profilbild und den Kontaktempfehlungen klickt rechts auf die **drei Punkte**, in dem Menü auf **Anzeigen aus Sicht** von.

So geht's leichter
So gebt Ihr weniger Daten preis

- Facebook zeigt euch jetzt alle Beiträge an, die öffentlich sichtbar sind.
- Wenn es zu viele sind, dann klickt auf **Filter** und wählt das Jahr aus, das euch interessiert.

Einschränken eines Beitrags

Wenn ihr nun einen Beitrag gefunden habt, den ihr nicht mehr öffentlich sehen wollt, dann geht so vor:

- Klickt in dem Beitrag auf das Datum.
- Bestätigt die Meldung, dass ihr die öffentliche Ansicht verlassen wollt.
- Klickt auf die drei Punkte im Beitrag, dann auf **Beitrag bearbeiten**.
- Unter eurem Namen im Beitrag klickt dann auf **Öffentlich** und wählt aus, wer den Beitrag sehen können soll.

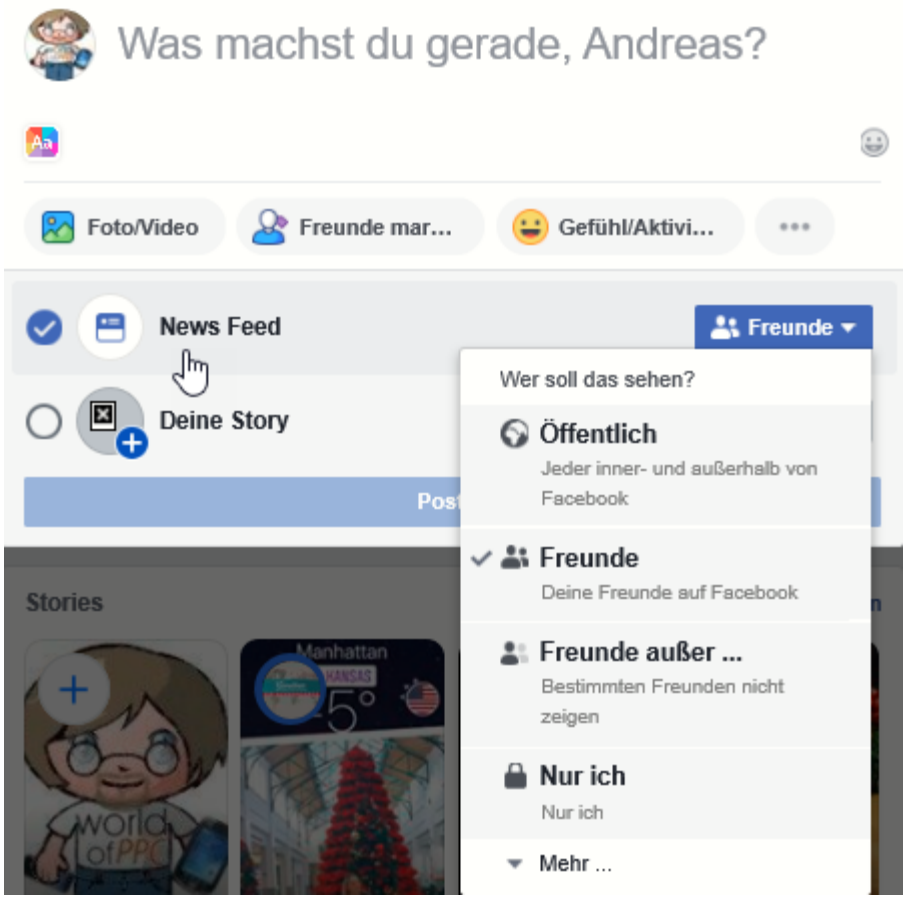
Bestimmte Personen von einem Facebook-Post ausschließen

Facebook ist vor allem deshalb toll, weil es den eigenen Aussagen eine ungeahnte Reichweite gibt. So könnt ihr mit einer Nachfrage mehr Leute erreichen, als ihr im direkten Zugriff habt. Dumm nur, wenn einer der virtuellen Freunde gerade eben nicht den Post nach einem Geschenk für ihn lesen soll. Kein Problem: Über Facebook könnt ihr einzelne Freunde aus Posts ausschließen. Oder eure Mutter! Wir zeigen euch, wie.

- Facebook erlaubt sehr feine Einstellungen der Privatsphäre, und dazu gehört auch das Einschränken von Beitragen für bestimmte Freunde.

So geht’s leichter
So gebt Ihr weniger Daten preis

- Klickt dazu in das Eingabefeld **Was machst Du gerade**. Fangt jetzt noch nicht an, den Beitrag zu tippen. Stattdessen klickt auf das Feld **Freunde**. Klickt es an, dann wählt **Freunde außer**...



- Ihr seht nun eine Liste eurer Freunde. Für jeden Freund in der Liste könnt ihr durch ein Anklicken des Stoppschild-Symbols auswählen, dass der Beitrag ihm oder ihr nicht angezeigt werden soll.

- Ihr könnt jederzeit diese Blockade wieder aufheben und den Post durch Deaktivieren der Einstellung wieder anzeigen lassen.

So geht's leichter
So gebt Ihr weniger Daten preis

- Klickt auf **Änderungen speichern**, um dem Beitrag seine Sichtbarkeit zuzuweisen. Viel Erfolg bei eurer geheimen Geschenkabfrage!

Instagram: Enge Freunde festlegen

Der Begriff der "Freunde" ist bei Facebook und Instagram immer relativ: Auch wenn diese sich so nennen, oft sind es nur entfernte Bekannte - wenn überhaupt. Bei Instagram mag es egal oder sogar gewünscht sein, wenn viele Leute eure Bilder sehen. Aber ihr könnt das durch eine neue Funktion noch ein wenig mehr einschränken!

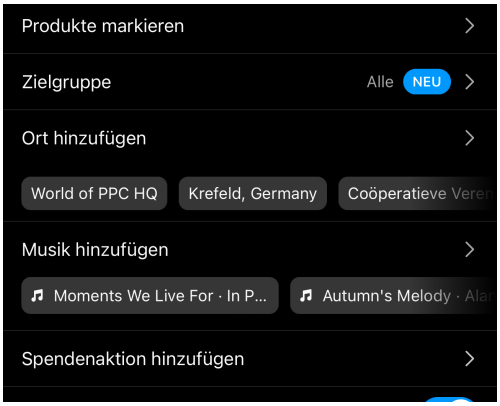
Freunde? Enge Freunde?

Gerade Instagram (aber auch Facebook) suggeriert, dass Menschen, mit denen wir virtuellen Kontakt haben und für die wir uns entschieden haben, Informationen zu teilen, "Freunde" sind. In der Realität gibt es unterschiedliche Gründe, eine solche "Freundschaft" einzugehen. Natürlich die Menschen, die uns tatsächlich nah sind und den Begriff verdienen. Dann aber auch Menschen, denen wir etwas beweisen oder verkaufen wollen und solche, die uns quasi überfallen haben und denen wir nicht entkommen konnten.

Die Differenzierung in den Beiträgen nach der ersten Gruppe und dem Rest war bisher nicht möglich. Allerdings hat Instagram das Problem erkannt und eine neue Funktion "Enge Freunde" eingeführt. Die seht ihr, wenn ihr eure App aktualisiert und einen neuen Beitrag verfasst:

So geht’s leichter
So gebt Ihr weniger Daten preis

Ob die "engen Freunde" nur wirklich nah sind oder ob ihr die Funktion nur nutzt, um allgemeine und private Beiträge zu trennen, ist am Ende vollkommen egal. Der Weg dahin ist derselbe:



- Öffnet eure Instagram-App und legt einen neuen Beitrag an.
- In den neueren Versionen der App findet ihr einen zusätzlichen Punkt Zielgruppe. Tippt diesen an.
- Ihr könnt auswählen zwischen Allen Kontakten und Engen Freunden.
- Um die Liste der engen Freunde zu verändern, tippt auf die Option.
- Instagram zeigt euch nun alle Kontakte an. Markiert die, die ihr als enge Freunde definieren wollt, entfernt die Markierung bei all denen, die das nicht sind.

- Wenn ihr einen Beitrag nur für die engen Freunde sichtbar haben möchtet, dann setzt den Punkt rechts von der Option. Diese Einstellung muss für jeden Beitrag vorgenommen werden.

So geht's leichter
So gebt Ihr weniger Daten preis

Instagram: Likes auch nachträglich wieder löschen

Likes sind die Währung bei Instagram: Je mehr ein Beitrag hat, desto wertvoller ist er. Allerdings verknüpft euch ein Like auch mit dem Beitrag, weil er von anderen Besuchern gesehen werden kann. Wenig bekannt: Ihr könnt Likes auch nachträglich wieder löschen!

Liken eines Beitrags

Der Vorgang an sich ist recht intuitiv: Wenn Ihr auf Instagram einen Beitrag seht, der Euch gefällt, dann könnt Ihr den durch einen Like von der Sichtbarkeit nach oben befördern.

Das hat nicht nur einen sichtbaren, sondern auch einen monetären Wert. Je mehr Likes ein Beitrag zieht und je mehr Beiträge mit vielen

So geht's leichter
So gebt Ihr weniger Daten preis

Likes ein Instagram-Konto hat, desto interessanter wird dieses Konto für Werbekunden. Influencer leben von dieser Werbung.

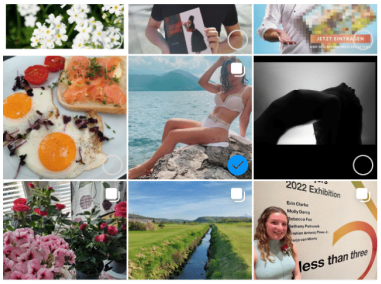
Entfernen von Likes in beliebigen Beiträgen

Likes sind im Beitrag sichtbar. Wenn ein Instagram-Follower von euch einen Beitrag aufruft, den Ihr geliked habt, dann wird ihm gegebenenfalls euer Name angezeigt. Das kann unangenehm sein, wenn es sich um einen Beitrag handelt, den Ihr eigentlich nicht liken wolltet oder hinter dem Ihr nicht mehr steht. Nur: Der kann weit in der Vergangenheit liegen und nicht mehr so einfach aufzufinden sein. Hierbei hilft Euch aber die Instagram-App:

- Loggt euch in euer Konto in der App ein und klickt auf das Symbol mit dem Kopf, das zu Eurem Konto führt.
- Klickt dann auf die drei Striche oben rechts (oder unten links, je nach Betriebssystem und App-Version).
- Klickt im Menü auf **Meine Aktivität (Interaktionen)** und dann auf **Gefällt mir**.
- Die App zeigt euch eine Liste der Bilder, die ihr geliked habt. Rollt so lange durch diese Liste, bis ihr das Bild findet, dem ihr das Like entziehen wollt.

So geht’s leichter
So gebt Ihr weniger Daten preis

- Haltet den Finger lange darauf, bis die Bilder alle mit einem Kreis unten rechts versehen sind. Dann verseht das Bild mit einem Haken, indem Ihr es antippt. Das könnt Ihr auch mit mehreren Bildern gleichzeitig machen.

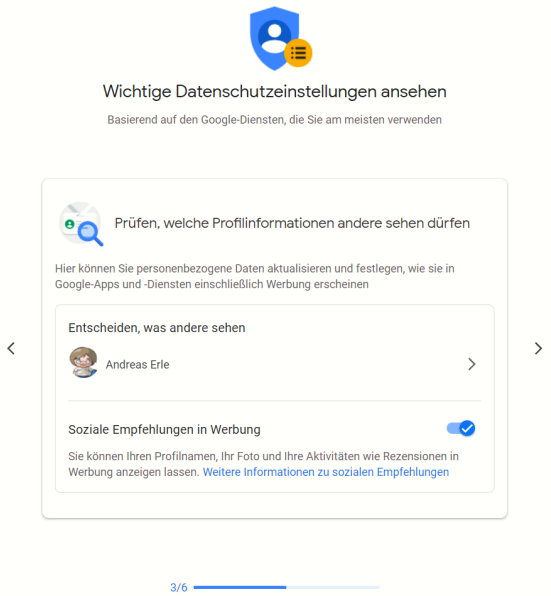


Gefällt mir nicht mehr (1)

- Tippt ganz unten auf **Gefällt mir nicht mehr**. Das entfernt euer Like von allen markierten Bildern.

Google und die Privatsphäre

Lacht nicht: Auch wenn Google ohne Frage gefühlt der größte Konsument und Verwerter eurer Daten ist, Privatsphäre ist alleine schon aufgrund der Datenschutzgesetzgebung ein Muss. In der Folge bietet auch Google eine Vielzahl an Hilfestellungen rund um Ihre Privatsphäre an.



- Diese sind gebündelt im Privatsphäre-Check, einer Unterseite eurer Kontoeinstellungen. Es empfiehlt sich, diese Seite regelmäßig aufzurufen und die Einstellungen zu kontrollieren und gegebenenfalls zu korrigieren.

- Google ändert regelmäßig den Leistungsumfang seiner Dienste. Damit werden auch Ihre Daten schnell anders verwendet oder neue Daten erhoben.

So geht's leichter
So gebt Ihr weniger Daten preis

- Wenn ihr euch nicht auf die Empfehlungen von Google verlassen wollt, dann könnt ihr alle Einstellungen auch manuell vornehmen.
- Dazu meldet euch an eurem Google-Konto an und klickt dann auf **Übersicht** > **Datenschutz und Personalisierung**. Hier könnt ihr beispielsweise festlegen, wer eure persönlichen Daten sehen darf, welche Daten zu eurem Verhalten gespeichert werden und vieles mehr. Wie immer: Datenschutz kostet Zeit und Aufwand, rechnet sich am Ende aber!
- Wenn ihr übrigens ein Android-Telefon nutzt, dann könnt ihr all diese Einstellungen auch direkt in den Datenschutz-Einstellungen des Gerätes vornehmen.

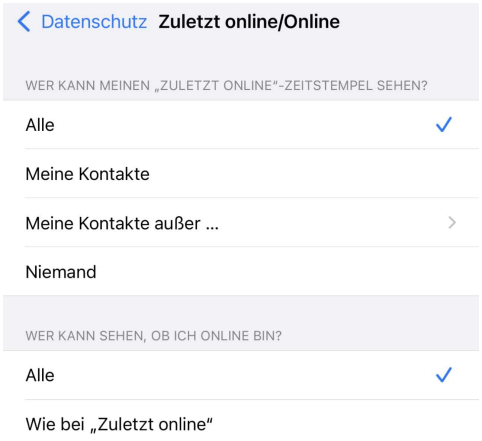
Weniger teilen bei WhatsApp

WhatsApp kann nicht nur zur Kommunikation eingesetzt werden, sondern bei falscher Konfiguration auch zum Ausspionieren von fremden Benutzern. Schützt euch davor!

WhatsApp soll die Kommunikation vereinfachen. Dazu gehört auch, dass unbekannte Personen miteinander Kontakt aufnehmen können. Die Basis dafür ist die Möglichkeit, nicht nur mit Kontakten, die WhatsApp haben, zu kommunizieren, sondern auch direkt über Rufnummern. Wer also eure Handynummer kennt, mit der Ihr bei WhatsApp registriert seid, der kann auch einige Informationen von euch sehen, auch wenn die Person nicht in euren Kontakten ist.

So geht’s leichter
So gebt Ihr weniger Daten preis

Besonders die Angabe, wann Ihr online wart, ist hier kritisch: Es gibt Spionage-Apps, die aus dieser Information dann ein Aktivitätsprotokoll von euch erstellen. Das muss nicht sein. WhatsApp hat mittlerweile eine eigene Option in den Datenschutzeinstellungen integriert:



- Klickt auf die drei Punkte oben rechts im WhatsApp-Fenster (bei Android) beziehungsweise das Zahnrad unten rechts (bei iOS).
- Tippt auf **Datenschutz** > **Zuletzt online/Online**.
- Unter **Wer kann meinen "Zuletzt Online"-Zeitstempel sehen** wählt **Meine Kontakte**, wenn Ihr den allen Kontakten zugänglich machen wollt oder **Meine Kontakte außer...**, wenn Ihr davon Kontakte ausnehmen wollt.
- Die im Standard gewählte Einstellung **Alle** sorgt dafür, dass auch Fremde Euren Status sehen können.

Damit habt Ihr erst einmal den Zugriff auf die Information, wann Ihr zuletzt online wart, eingeschränkt. Wichtig ist aber zur Vermeidung eines Onlineprofils, dass Ihr den aktuellen Online-Status einschränkt.

- Klickt auf die drei Punkte oben rechts im WhatsApp-Fenster (bei Android) beziehungsweise das Zahnrad unten rechts (bei iOS).
- Tippt auf **Datenschutz** > **Zuletzt online/Online**.
- Die im Standard gewählte Einstellung **Alle** sorgt dafür, dass auch Fremde Euren Status sehen können.

So geht's leichter
So gebt Ihr weniger Daten preis

- Unter **Wer kann sehen, ob ich online bin?** wählt **Wie bei zuletzt online**, dann ist dieselbe Einschränkung aktiv wie beim Zeitstempel der letzten Online-Aktivität.

Datensparsam im Internet

Das Surfen im Internet erinnert manchmal an einen undichten Duschkopf: Vorn kommt das Wasser raus, was ihr zum Duschen braucht, aber hinten sprüht es aus einem kleinen Loch im Schlauch unbemerkt an die Wand. Während ihr im Internet surft, hinterlasst ihr über eure IP-Adresse, Cookies und Browserkennungen eine Menge Daten, die Aufschluss über Vorlieben und Gewohnheiten geben.

Neben den Cookie-Einstellungen und dem Privaten Modus der verschiedenen Webbrowser könnt ihr auf Wunsch noch ein wenig mehr machen!

Surfen in einer Sandbox

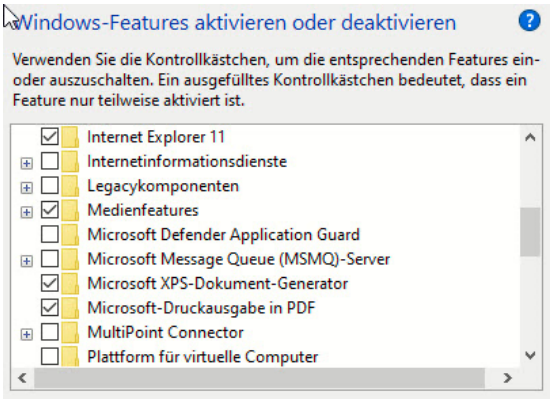
Das Internet ist eine Sammelstelle für Informationen, ein Schmelztiegel des Wissens. Allerdings gleichzeitig auch ein Ort, an dem sich auch viele üble Gesellen herumtreiben, die euch möglichst viele Informationen und Ressourcen abnehmen wollen. Schadsoftware, Phishing-Angriffe, kurz: Gefahr für Ihren PC. Microsoft versucht hier entgegenzuwirken, unter anderem durch den Microsoft Defender Application Guard (MDAG). Wir zeigen euch, wie ihr den nutzen könnt.

Einfach gesagt ist der MDAG eine kleine virtuelle Maschine, die zu eurem Rechner keinerlei Verbindung hat. Der Vorteil: Was immer ihr euch an Schadsoftware einfangen, kann nur in dieser virtuellen

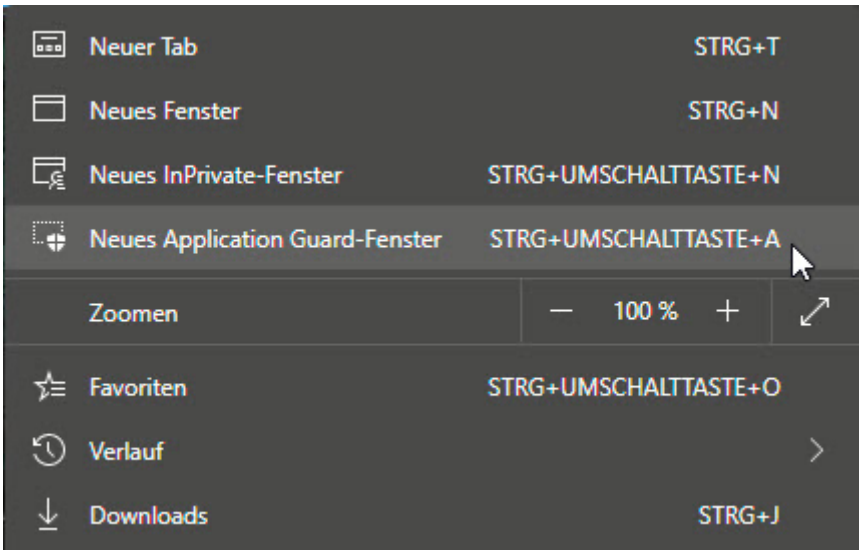
So geht's leichter
So gebt Ihr weniger Daten preis

Maschine Schaden anrichten. Die wird aber beim Beenden der Internetsitzung gleich komplett weggeworfen. Die Schadsoftware ist damit dann auch entfernt. Was kompliziert klingt, ist in der Anwendung mit wenig Aufwand umgesetzt. Der Vorteil: Eure ganzen echten Daten lasst Ihr auf dem Rechner, und in der virtuellen Maschine sind nur die Daten, die ihr wirklich braucht!

- Sucht in Windows nach **Windows Features aktivieren oder deaktivieren**. Dort hakt **Microsoft Defender Application Guard** an und klickt dann auf **OK**.

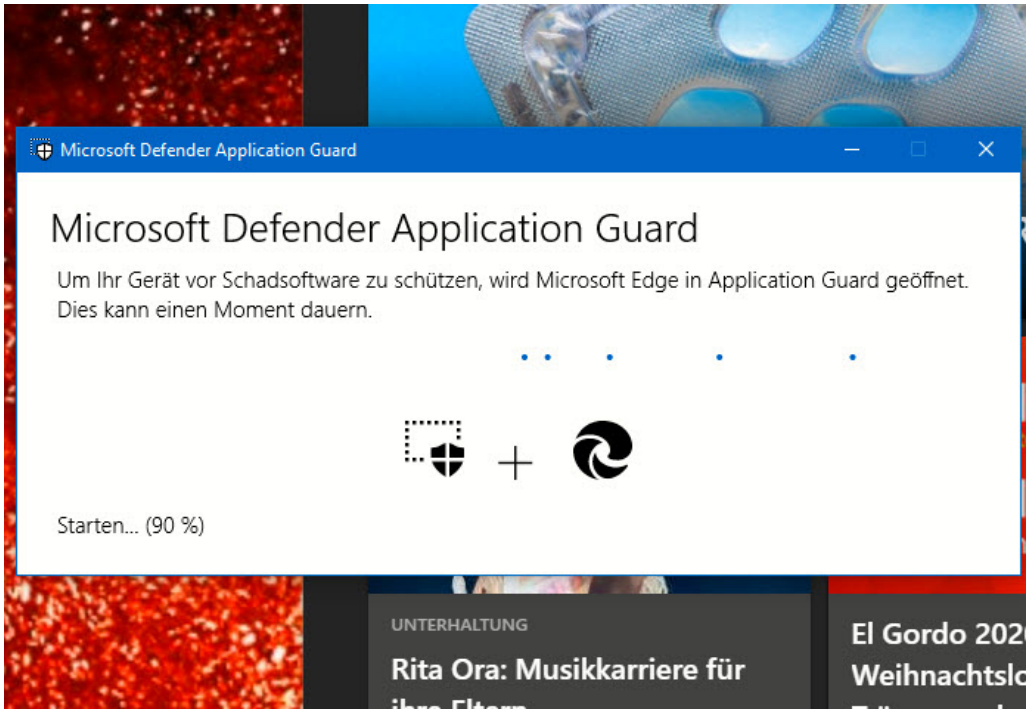


- Das Feature wird nun installiert, der Vorgang dauert einige Minuten
- Nach einem Neustart eures Rechners habt ihr in Edge im Menü einen neuen Punkt **Neues Application Guard-Fenster**. Klickt darauf, damit die virtuelle Umgebung installiert wird.



So geht’s leichter
So gebt Ihr weniger Daten preis

- Das kann einige Sekunden dauern, Edge zeigt euch den Fortschritt auf dem Bildschirm an. Sobald der Browser offen ist, könnt ihr wie gewohnt surfen. Ihr solltet euch bei aller Sicherheit aber bewusst sein, dass alles, was ihr in diesem Browser eingebt, natürlich immer noch ins Internet geht und abgefangen werden kann!



Anonym Surfen: Der Tor-Browser

Im Internet findet ihr nahezu alle Informationen, die ihr benötigt. Manchmal auch mehr, als ihr tatsächlich wissen wollt. Sicher ist aber: Eine Suche im Internet hinterlässt Spuren. Und bei bestimmten Themen ist es euch vielleicht nicht so recht, wenn man nachvollziehen kann, dass ihr eine Webseite besucht habt. Eine schnelle Lösung ist hier der kostenlose Tor-Browser.

So geht’s leichter
So gebt Ihr weniger Daten preis

Die Idee dahinter ist einfach: Das Internet kann Suchen und Webseitenbesuche ja nur deshalb zu euch zurückverfolgen, weil es über die IP-Adresse potenziell Zugriff zu Ihrem Anschluss hat. Der Tor-Browser löst das elegant: Er verwendet das Zwiebelschalenprinzip. Im Englischen heißt das Onion Routing, daher kommt auch der Name des Browsers: **T**he **O**nion **R**outer.

Die Idee: Im Internet laufen die Daten immer über verschiedene Knotenpunkte, damit ist eure Adresse auch all diesen Knoten bekannt. Beim Tor-Browser werden eure Daten an jedem Knoten neu ver- bzw. entschlüsselt. Damit sieht am Ende nur der letzte Knoten eure Daten im Klartext und kann überhaupt etwas damit anfangen.

Dazu kommt, dass die Daten durch die immer wieder durchgeführte Verschlüsselung immer anders aussehen, ein Tracking also nicht

So geht's leichter
So gebt Ihr weniger Daten preis

möglich ist. Und da jeder Knoten nur seinen Nachbarn kennt, kann die Seite, von der ihr Daten herunterladet bzw. an die ihr Daten sendet auch nicht identifizieren, dass ihr es seid. Anonymer könnt ihr kaum Surfen!

Tracking in Microsoft Edge verhindern

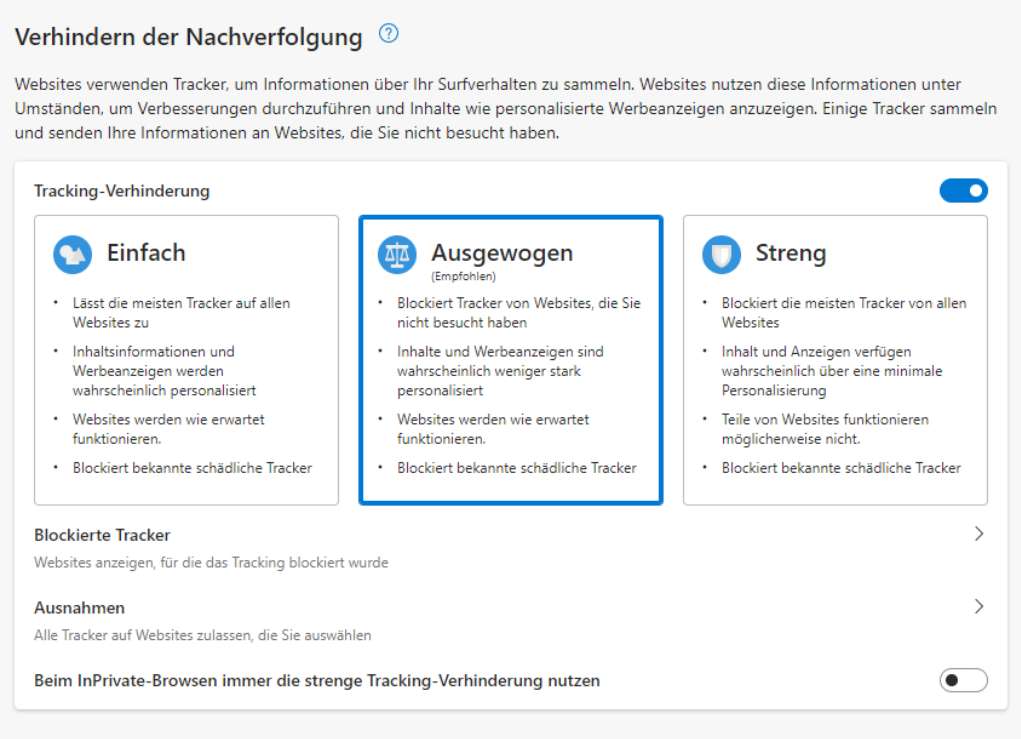
Die Währung des Internets: Eure Daten. Wenn ihr möglichst wenig über euer Surfverhalten preisgeben wollt: Nutzt die Anti-Tracking-Mechanismen von Microsoft Edge!

Wenn ihr im Internet surft, dann habt ihr - für euch unsichtbar - eine Menge an Daten im Gepäck: Den verwendeten Browser, das Betriebssystem, die Auflösung, installierte Schriftwarten, die Cookies und eine Menge mehr an Informationen, die alleine keinen Rückschluss erlauben. Zusammengenommen aber erlauben die eine Identifikation des Nutzers und damit die Verfolgung über Webseiten hinweg. Euer Einkaufsverhalten, eure aus den besuchten Seiten abgeleiteten Interessen, all das wird ausgewertet.

Microsoft Edge bietet im Standard schon einen sehr ausgeklügelten Trackingschutz:

- Klickt in den Einstellungen auf **Datenschutz, Suche und Dienste**.
- Aktiviert die Option **Trackingverhinderung**.
- Empfohlen wird die Einstellung **Ausgewogen**, damit versucht Edge, eine Balance zwischen Schutz und Nutzbarkeit der Webseiten einzustellen.

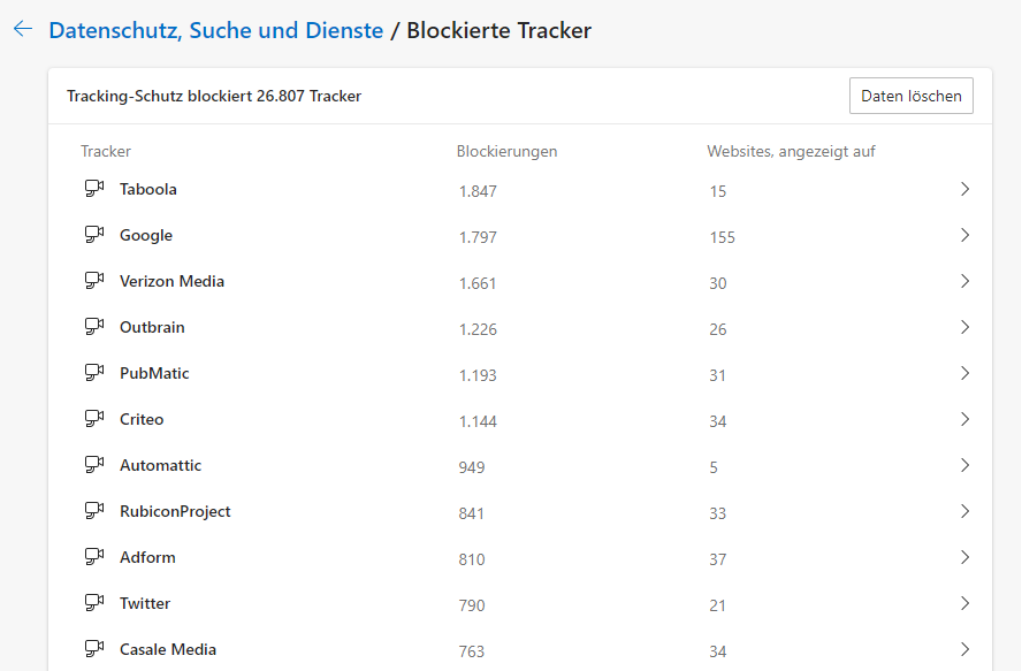
So geht’s leichter
So gebt Ihr weniger Daten preis



- Wenn ihr Webseiten besucht, auf denen ihr eher einen hohen Schutz haben wollt, dann werdet ihr im Normalfall ohnehin den **Privaten Modus** nutzen.
- Aktiviert in den Einstellungen von Edge **Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen**, dann erhöht ihr den Tracking-Schutz, ohne euch auf normalen Seiten allzu sehr einzuschränken.
- Wenn ihr sehen wollt, welche Seiten euch besonders intensiv verfolgen wollen, dann klickt auf den Pfeil neben **Blockierte Tracker**. Hier seht ihr pro Tracker die Seiten, die ihn verwenden.
- Beim Durchschauen findet ihr schnell heraus, welche Internetseiten dauernd in der Liste auftauchen. Überlegt, diese zu meiden.

Bei den anderen Browsern funktioniert das ähnlich.

So geht’s leichter
So gebt Ihr weniger Daten preis



Löschanträge bei Suchmaschinen stellen

Das Internet ist ein Elefant: Es vergisst freiwillig erst einmal nichts. Das ist im Sinne einer Historie vielleicht nicht einmal schlecht, nicht alle Informationen werden über die Zeit falsch oder ungültig. Wenn es aber über individuelle Suchergebnisse geht, dann kann das durchaus anders aussehen: Nur, weil ihr in der Vergangenheit einmal in eine Zwangsversteigerung gerutscht seid, ist das Jahr später nicht mehr relevant, sondern eher schädlich. In solchen Fällen könnt ihr einen Löschantrag an den Suchmaschinenbetreiber stellen.

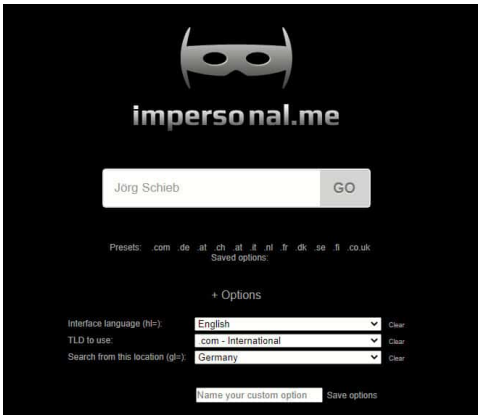
Hintergrund der Betrachtung ist der Prozess eines Spaniers gegen einen solchen Fall: Google fand immer noch den Artikel einer Zeitung, in der das Haus als in der Versteigerung befindlich dargestellt wurde. Die Schuld war lange getilgt, und dieses Suchergebnis erweckte den

So geht's leichter
So gebt Ihr weniger Daten preis

Eindruck, dass er immer noch Schulden habe. Nach langen Prozessen hat der EUGH klargemacht: Diese Einträge sind zu löschen.

Was könnt ihr aber jetzt aktiv tun?

- Kontrolliert regelmäßig, welche Suchergebnisse eine Suche nach eurem eigenen Namen ergibt. Idealerweise mit einer Suchmaschine wie impersonal.me, die die Suche über Google durchführt, eure Identität aber verschleiert.



- Damit bekommt ihr ein nicht an euch ausgerichtetes Suchergebnis.
- Findet ihr in diesem Suchergebnis Links, die falsch oder veraltet sind und euch Schaden zufügen können, dann könnt ihr diese in diesem Formular bei Google melden und die Löschung anfordern.
- Wichtig dabei: Eine Löschung der Webseite - so diese noch existiert – erreicht ihr damit nicht und müsst diese manuell anfordern!

Schnell reagieren: Anmeldungen fremder Geräte

Je mehr ihr euch im Internet bewegt, desto mehr potenzielles Risiko auf Datenverlust habt ihr. Wenn einer der Dienste, die ihr nutzt, euch über einen fremden Anmeldeversuch informiert, dann solltet ihr schnell reagieren!

So geht's leichter
So gebt Ihr weniger Daten preis

Viele Anbieter wie Google, Netatmo, Microsoft und viele mehr überwachen die Anmeldungen an die von ihnen angebotenen Diensten sehr genau. Ihr Nutzungsverhalten gibt klare Hinweise, wann und vor allem von wo eine Anmeldung "normal" ist, und eben auch, wann nicht. Wenn ihr in Deutschland sitzt und eine Anmeldung aus Russland erfolgt, dann ist das klar zumindest fragwürdig. Wenn ihr eine E-Mail mit einer Warnung vor einem solchen Anmeldeversuch erhaltet, dann reagiert umgehend.

- Zuerst: Auch solche E-Mails können gefälscht sein. Klickt keinesfalls auf einen Link, der sich in der E-Mail befindet. Der kann bei einer Fälschung schnell auf eine Fake-Seite leiten, die eure Anmeldedaten klaut.

Wir haben eine Anmeldung bei deinem Konto an einem neuen Standort oder über ein neues Gerät erkannt.

Ort: Russland

Gerät: okhttp 4.4.1 Other

Datum: Freitag, 24. September 2021 um 07:38:22 Moskauer Normalzeit

- Stattdessen ruft manuell die Seite des Anbieters auf und meldet euch an eurem Konto an.
- Kontrolliert, ob irgendwelche Änderungen vorgenommen wurden, Bestellungen ausgelöst wurden, die ihr nicht gemacht habt etc. Und: Ändert umgehend das Passwort!

Wenn der Google-Sicherheitscheck sich meldet

Ein weiterer Schreckmoment: Google meldet, es habe kompromittierte Passwörter gefunden. Google-Dienste sind kaum wegzudenken: Als Android auf einem Smartphone, die Nutzung der Suchmaschine, Google-Dienste wie Drive oder die Office-Apps.

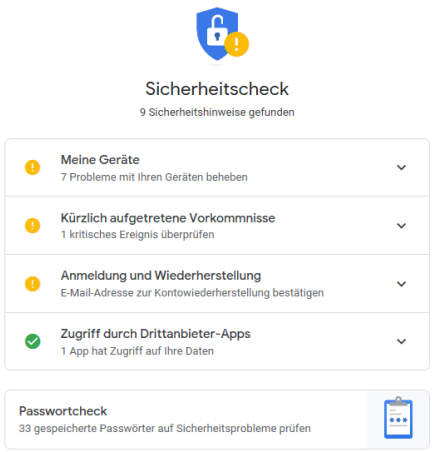
So geht’s leichter
So gebt Ihr weniger Daten preis

- Lest die Meldung, die als E-Mail zugestellt wird, genau: In den meisten Fällen handelt es sich um einen Regelcheck, den Google über die im Konto gespeicherten Passwörter durchführt.
- Wird in diesem automatischen Abgleich zwischen Datenbanken über Datenlecks und euren gespeicherten Passwörtern eine Übereinstimmung gefunden, dann bekommt ihr diese Warn-E-Mail.
- Diese Meldung bezieht sich nicht auf euer Google-Konto, sondern "nur" auf die darin gespeicherten Passwörter.

- Diese sind nicht bei Google abhandengekommen, mehrheitlich sind es Datenlecks, die auf irgendwelchen Webseiten entstanden sind.
- Um dies zu kontrollieren und die betroffenen Passwörter zu ändern, klickt auf **Sicherheitscheck durchführen** oder ruft diesen direkt auf.

So geht's leichter
So gebt Ihr weniger Daten preis

- Nach Aufruf der Seite und Anmeldung mit euren Google-Kontodaten zeigt euch der Sicherheitscheck die gefundenen Sicherheitsrisiken an.



- Keine Sorge: Nicht alle sind wirklich gefährlich, sollten aber einzeln betrachtet werden.
- Unter **Meine Geräte** zeigt Google alle Geräte an, die schon länger nicht mehr mit den Google-Diensten verbunden waren. Das passiert vor allem dann, wenn ihr ein Gerät verkauft habt
- Da ihr das sicherlich gelöscht habt, kann damit nichts mehr passieren. Trotzdem: Löscht nicht mehr vorhandene Geräte aus dem Google-Konto!
- **Kürzlich aufgetretene Vorkommnisse** sind Anmeldungen, die von fremden Geräten oder unüblichen Orten durchgeführt wurden. Kontrolliert hier, ob das wirklich von euch ausgelöst wurde.
- Wenn nicht, klickt auf **Nein, das war ich nicht**. In einem solchen Fall solltet ihr dringend euer Kennwort ändern!

Datensammler in Windows ausschalten

Windows ist als Betriebssystem im Standard so konfiguriert, dass es für die meisten Anwender alle Möglichkeiten bietet. Dann kommen noch die Hersteller und packen das eine oder andere Programm dazu, das sie testen und möglichst kaufen sollen. All das läuft im Hintergrund und

So geht's leichter
So gebt Ihr weniger Daten preis

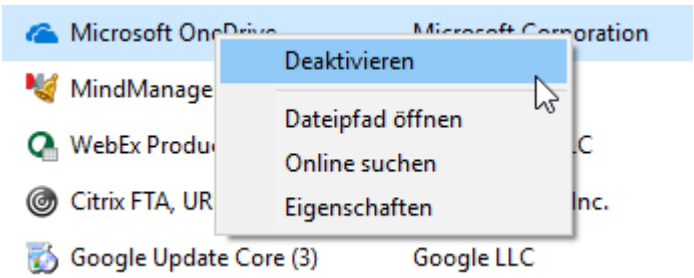
nimmt Einfluss auf die Performance Ihres Rechners. Vor allem aber sammeln diese Programme fleissig Daten, was ihr sicherlich nicht wollt. Statt nun in die Falle zu tappen: Räumt auf!

Unnötige Programme aus dem Autostart löschen

Windows versucht, euch alle benötigten Dienste und Programme direkt beim Systemstart zur Verfügung zu stellen. Diese Auswahl wird allerdings auch davon beeinflusst, dass installierte Programme und Apps oft der Meinung sind, sie seien unverzichtbar, und sich auch zum direkten Start registrieren lassen. Ein Paradies für Datensammler!

Das führt schnell dazu, dass Programme im Hintergrund laufen, die ihr gar nicht braucht, der Start des Systems verzögert, CPU-Zeit verschwendet und unnötig Daten gesammelt werden.

- Statt diese immer wieder manuell zu beenden, verhindert einfach ihren automatischen Start!

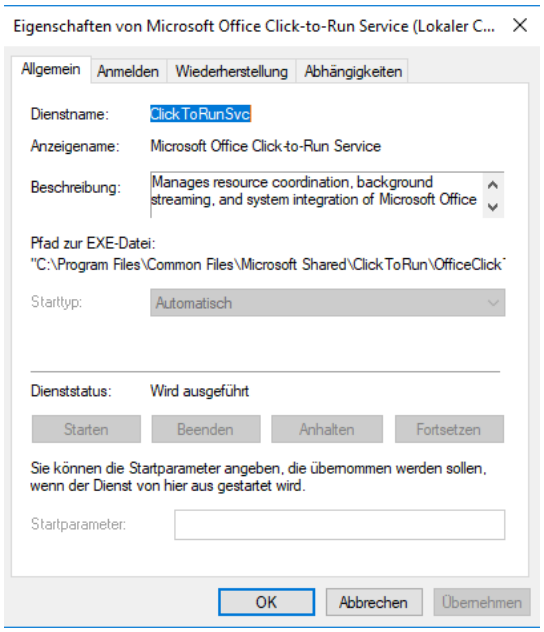


- Klickt dazu im Task Manager auf den Reiter **Autostart**, dann mit der rechten Maustaste auf den Dienst/das Programm.
- Ein Klick auf **Deaktivieren** verhindert den automatischen Start. Sollte das zu Problemen führen, könnt ihr ihn jederzeit auf demselben Weg wieder aktivieren.

So geht's leichter
So gebt Ihr weniger Daten preis

Unnötige Dienste beenden

Mit den Diensten verhält es sich wie mit den Programmen: Windows 11 startet viele automatisch mit, aktiv, benötigt ihr aber nur einen Teil davon. Die anderen langweilen sich und verbrauchen nur Rechner-Kapazitäten oder sammeln eure Daten. Auch Dienste könnt ihr davon abhalten, automatisch gestartet zu werden.



- Drückt **Windows** und **R**, dann gebt in das Eingabefeld als Befehl **services.msc** ein.
- Windows zeigt euch nun alle Dienste an, die auf dem PC vorhanden sind.
- In der Spalte **Status** könnt ihr sehen, ob der Dienst gerade läuft („wird ausgeführt"). Klickt mit der rechten Maustaste darauf und dann auf **Eigenschaften**.
- Ein Klick auf **Beenden** beendet einen laufenden Dienst. Unter **Starttyp** könnt ihr festlegen, dass der Dienst nur **manuell** gestartet wird, nicht automatisch.
- Gerade bei Diensten zu Programmen, die ihr eher selten braucht, kann das das System spürbar beschleunigen. Im Normalfall startet das Programm beim Start die Dienste ohnehin, wenn sie bisher nicht laufen.
- Beendete Dienste sammeln keine Daten und in der Folge übermitteln sie auch keine Daten (mehr).

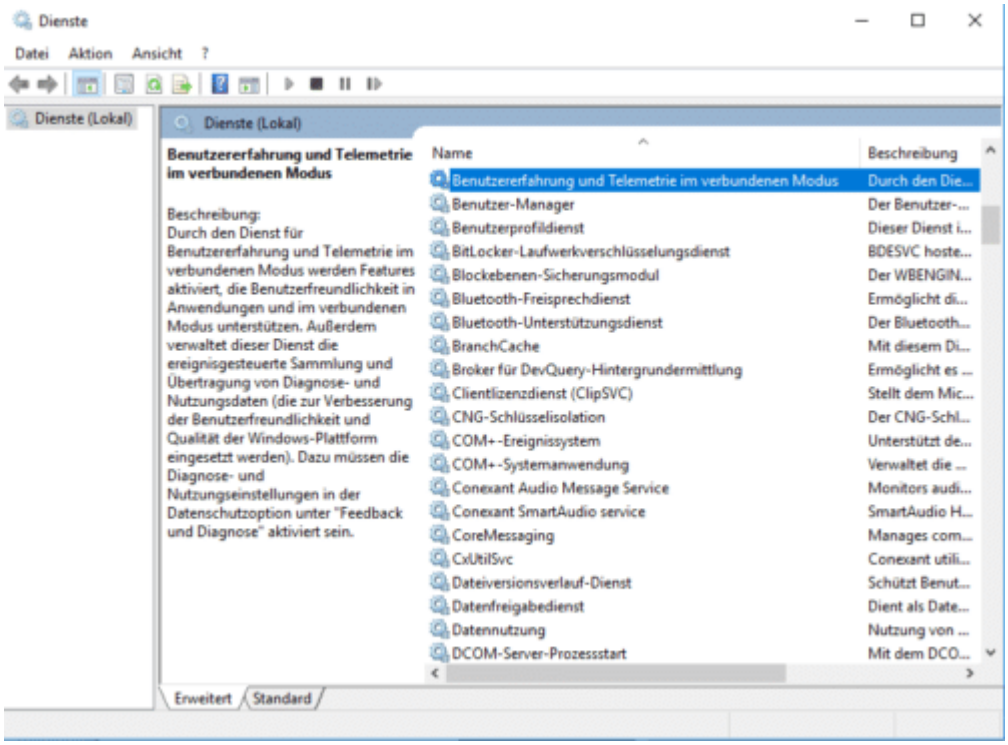
So geht's leichter
So gebt Ihr weniger Daten preis

Telemetrie in Windows einschränken

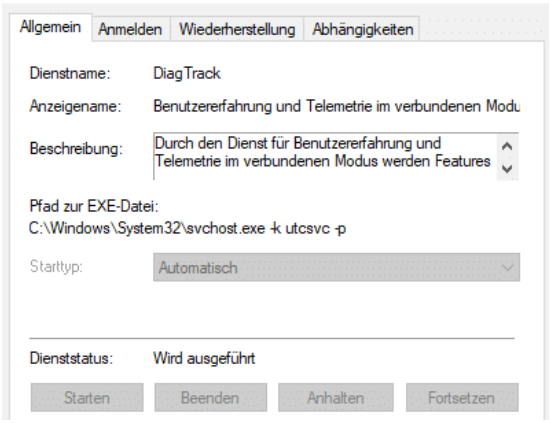
Datenschutz ist ein heiß diskutiertes Thema auch unter Windows 11. Daten werden immer und überall gesammelt, und dem einen oder anderen Anwender ist das suspekt. In den Datenschutzeinstellungen von Windows 11 lassen sich einige Einstellungen verändern, die Erfassung der Diagnosedaten aber nicht. Diese wird über einen Systemdienst gesteuert, den ihr aber selber ausschalten könnt.

- Um an die Dienste zu kommen, gebt unten im Suchfeld der Taskleiste **services.msc** ein. Windows startet nun die Diensteverwaltung, die alle auf dem PC installierten Dienste anzeigt.
- In der Spalte **Status** könnt ihr sehen, ob ein Dienst gerade läuft. Ist die Spalte neben einem Dienst leer, dann ist er gerade nicht aktiv.
- Im Normalfall steuern Windows selbst, Treiber für Hardware und Apps die Dienste selber. Für den Telemetriedienst greift manuell ein.

So geht’s leichter
So gebt Ihr weniger Daten preis



- Sucht nun den Dienst **Benutzererfahrung und Telemetrie im verbundenen Modus** und klickt doppelt darauf.
- Unter **Allgemein** > **Dienststatus** seht ihr, dass dieser aktuell ausgeführt wird.
- Klickt auf die Schaltfläche **Beenden**, um diesen zu stoppen. Klicken nun auf **Starttyp**, und wählt in der Liste **manuell** aus.
- Nach einem Neustart ist der Telemetriedienst dann weiterhin nicht mehr aktiv, weil der automatische Start durch euren Eingriff verhindert wird. Damit werden



So geht's leichter
So gebt Ihr weniger Daten preis

keine Telemetriedaten mehr gesammelt.

- Eine Änderung dieser Einstellungen ist nur dann möglich, wenn ein Administrator dies nicht verhindert hat. Auf dem eigenen PC wird das nicht der Fall sein, auf einem Firmen-PC eher schon.

Gesammelte Daten wieder löschen lassen

Recht zu haben ist nicht schwer, Recht zu bekommen allerdings schon: Incogni ist ein praktischer Service von Surfshark, der dafür sorgt, dass Data Broker über Euch gespeicherte Daten löschen.

Wir wissen es eigentlich alle – und ergeben uns viel zu häufig: Trotz DSGVO werden jede Menge Daten von uns erhoben und gespeichert. Keineswegs nur Daten, die wir selbst irgendwo eingeben, sondern auch und vor allem Daten, die Tracker in Apps, Anwendungen und auf Webseiten gnadenlos einsammeln und an sogenannte „Data Broker" verkaufen.

Wer die kostenlose App benutzt oder im kostenlosen Game daddelt, bemerkt nicht, dass im Hintergrund diverse Tracker aktiv sind und Daten sammeln. Diese Daten werden eingesammelt und an die Broker verkauft. In der Regel, ohne dass wir es wissen – und ohne unsere ausdrückliche Zustimmung. Wenn überhaupt, gibt es verquaste Paragrafen in den Datenschutzbestimmungen („Dürfen wir Daten mit Dritten teilen"), die niemand infrage stellt.

Schlimm genug, dass der Gesetzgeber das erlaubt.

So geht's leichter
So gebt Ihr weniger Daten preis

Data Broker werfen ihre Krakenarme aus

Dieses Business ernährt Hunderte von Agenturen weltweit, die auf diese Weise (meist unbemerkt und leise) sensible Daten einsammeln, Datenbanken aufbauen, Profile erstellen und die Daten gewinnbringend verkaufen. Darunter persönliche Daten wie:

- Name
- Alter
- Adresse
- E-Mail-Adresse
- Bewegungsdaten
- Interessen
- Telefonnummer
- Beschäftigungsverhältnisse
- Finanzdaten
- Medizinische Daten

Oft werden diese persönlichen Daten mit der Advertising-ID verknüpft. Das ist eine unverwechselbare ID, die jedes Smartphone besitzt. Sind Datensätze mit dieser eineindeutigen Advertising-PC verknüpft, lassen sich Daten aus unterschiedlichen Quellen (von unterschiedlichen Brokern) mit vergleichsweise geringem Aufwand verknüpfen. Auf diese Weise sind Datenjournalisten und Ermittler zum Beispiel den Personen auf die Schliche gekommen, die im Januar 2021 das Capitol in Washington DC gestürmt haben.

So geht's leichter
So gebt Ihr weniger Daten preis

Doch personalisierte Werbung ist nur das geringste Problem hierbei. Die unrechtmäßig eingesammelten Daten werden auch für Scamming (etwa fingierte Telefonanrufe), Identitätsdiebstahl oder Stalking missbraucht.

DSGVO: Recht auf Auskunft

Wir haben grundsätzlich ein Recht – das sieht vor allem die DSGVO vor – von jedem Anbieter oder Onlinedienst zu erfahren, welche Daten er über uns gespeichert hat. Ganz konkret. Das gilt keineswegs nur für die offensichtlichen Kandidaten wie Facebook, Google, Amazon, Microsoft und Co., sondern ganz allgemein. Jede(r) muss diese Auskunft erteilen. Und wir haben auch das Recht, die Löschung der Daten zu verlangen.

Nur: Wer macht das schon? Die meisten Verbraucher denken, die Daten landen nur bei Google, Facebook, Twitter und Co. Da landen sie auch – aber eben auch bei Hunderten Brokern weltweit.

Hier kommt ein neuer Service ins Spiel, den ich wirklich klasse und sehr interessant finde: **Incogni** von Surfshark.

So geht's leichter
So gebt Ihr weniger Daten preis

Wer sich hier anmeldet, kann Incogni damit beauftragen, bei Dutzenden von bekannten Data Brokern (aktuell sind es 130) ganz offiziell – formell und rechtskonform – die Löschung der eigenen persönlichen Daten zu beauftragen.

Das macht Incogni vollkommen automatisch. Incogni erledigt sozusagen den „Papierkram": Der Dienst verschickt auf unseren Wunsch entsprechende Schreiben (in der Regel E-Mails) an die bekannten Data Broker dieser Welt. E-Mails. formal formuliert und juristisch korrekt, die – in unserem Namen – die entsprechende Auskunft verlangen.

Rund 130 solcher Broker hat Incogni bereits in seiner Datenbank. Weltweit soll es mindestens 1200 Broker geben. Die Liste der Broker, die Incogni automatisiert anschreibt, um unsere Interessen und Rechte durchzusetzen, wird stets länger und umfangreicher.

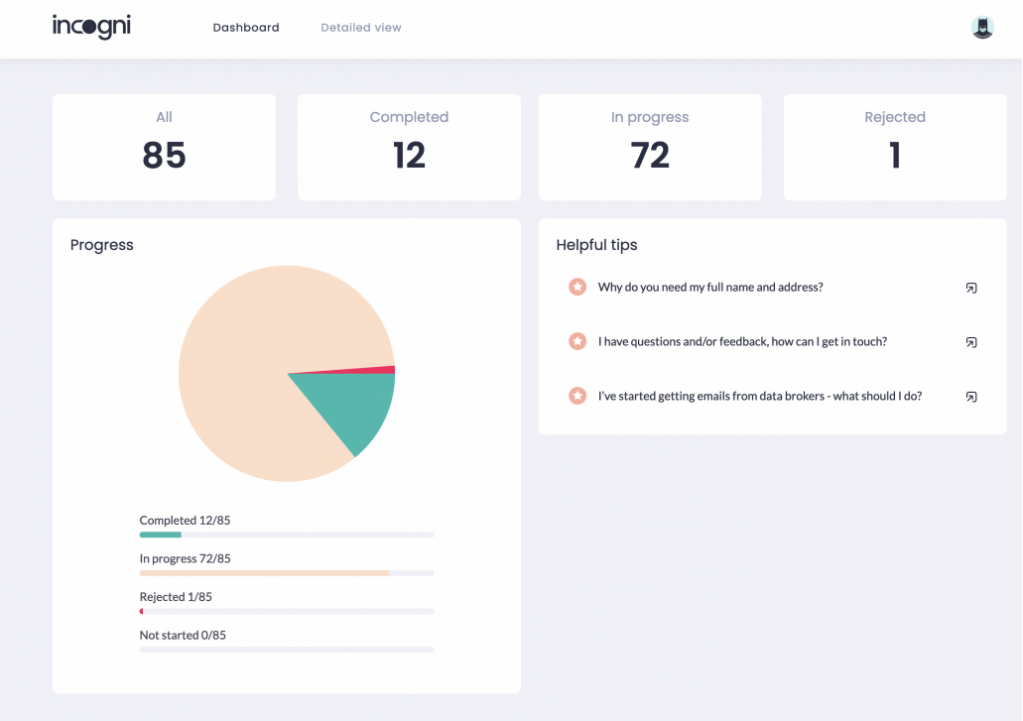
PRO

- Verschickt automatisch offizielle Lösch-Anforderungen an Data Broker
- Trackt die Antworten der Broker
- Wiederholtes Nachfragen, wenn nötig
- Vergleichsweise günstig

CONS

- Es gibt keine offiziellen Löschbestätigungen
- Bearbeitet (noch) keine People-Suchdienste

So geht's leichter
So gebt Ihr weniger Daten preis



Incogni Dashboard

Vollautomatische Rechtspflege

Incogni funktioniert wie ein eifriger Rechtsbeistand, der formal Beschwerde einlegt, Daten abruft und Löschungen beauftragt. Das allein ist schon ein Fest, weil es die Data Broker beschäftigt. Sollten Sie nicht antworten, verhalten sie sich nichts rechtskonform – und ein solcher massenhafter Verstoß ließe sich dank Incogni leicht belegen und ahnden.

Wer den Dienst bucht, sieht, welche Data Broker der Service schon angeschrieben hat – und ob es zu Reaktionen gekommen ist. Hier darf man nicht ungeduldig sein. Denn da diese Prozesse im Hintergrund per E-Mail erfolgen, kann es tagelang dauert, bis eine Antwort eintrifft. Incogni hakt nacht, sollte ein Data Broker der Ansicht sein, er müsse sich nicht bewegen.

So geht’s leichter
So gebt Ihr weniger Daten preis

Incigoni ist ein gebührenpflichtiger Service. Wer mag, kann monatsweise buchen – oder jahresweise. Verglichen mit Anwaltskosten sind die Gebühren gering. Mir ist es wert, für diesen Service zu bezahlen.

Aber eigentlich ist es eine Schande, dass der Gesetzgeber zulässt, dass so viele Daten unbemerkt gesammelt werden können – und dass wir als Konsumenten die Arbeit und die Kosten haben, um unser Recht in Anspruch zu nehmen.

Hier bekommt Ihr Incogni aktuell mit hohen Rabatten (für 70 EUR/Jahr)

Wer sich für das Jahresabo entscheidet, spart 50%.