

Klicken wir uns die Privatsphäre weg?

WILLKOMMEN IM AGB-DSCHUNDEL

Es ist bereits 18 Uhr. Der Chef will noch das Protokoll lesen, eine Kollegin braucht dringend Unterlagen, der Laptop verlangt nach einem Update, und irgendwo blinkt ein Fenster mit der Aufforderung, etwas zu akzeptieren. Sie stimmen zu. AGB lesen? Nein, oder kennen Sie jemanden, der das wirklich tut? Das kann jedoch Folgen haben, denn Sie haben soeben entschieden, was der Anbieter mit Ihren Daten machen darf. Sie sind für ihn pures Kapital.

Text: Corina Zingg

In meinen Seminaren frage ich die Teilnehmenden regelmässig, ob sie schon einmal die AGB einer App gelesen haben. Meist kommt ein müdes Lächeln zurück. Die Klassiker kenne ich inzwischen auswendig: «Niemand macht das», «zu kompliziert», «zu lang». Frage ich hingegen, ob jemand seine Nummer in ein Telefonbuch eintragen möchte, wird das vehement verneint. Hier schützen wir unsere Daten.

Aber: Verkaufen wir mit diesem Klick nicht ein Stück unserer Privatsphäre? Warum benötigt ein Spiel auf dem Smartphone Zugriff auf meine Kontakte und E-Mails? Nur wenn ich die AGB zumindest kurz prüfe, kann ich entscheiden: Will ich dieses Tool wirklich nutzen, oder suche ich mir eine weniger neugierige Alternative?

Was auf den ersten Blick schwierig erscheint, wird plötzlich einfacher, wenn man sich damit besser auskennt. Hier ein paar hilfreiche Tipps:

Der 7-Punkte-Quickscan für AGB

Nutzen Sie die Suchfunktion Ihres Computers, um diese Punkte zu finden. Überlegen Sie, ob das für die Anwendung nötig oder sinnvoll ist.

- 1. Training** (improve, machine learning): Dürfen Ihre Inhalte fürs Trainieren einer KI genutzt werden? Können Sie das ausschalten (opt out)?
- 2. Weitergabe** (share, affiliate, third party): Gehen Daten an Dienstleistende oder Partner?
- 3. Verknüpfungen** (sign in, connected, permissions, access): Was geben Sie frei, falls Sie sich mit einem Google- oder Facebook-Konto einloggen oder Konten verknüpfen?
- 4. Transfer** (region, outside, international): Wo werden Daten verarbeitet oder gespeichert?
- 5. Aufbewahrung** (retain, retention, logs, backup): Wie lange bleiben Inhalte, Protokolle oder Back-ups bestehen?
- 6. Kontrolle** (opt out, export, delete): Können Sie der Nutzung widersprechen, Daten exportieren oder löschen?
- 7. Änderungen** (change, update, notice): Wie werden neue Bedingungen in AGB kommuniziert?

Mit etwas Übung reichen bald ein bis zwei Minuten, um zu merken, ob ein Tool nötige Informationen braucht oder etwas zu neugierig ist. Es lohnt sich.



Daten löschen heisst nicht Daten vergessen

Bisher konnten Zustimmungen widerrufen und Daten vollständig gelöscht werden. Jedoch funktionieren Tools mit künstlicher Intelligenz (KI) anders: Was Sie in ein KI-Tool eingeben, lässt sich später kaum vollständig löschen. Zwar können Chats entfernt werden, aber es bleiben technische Spuren zurück. Stellen Sie es sich wie einen Tropfen Tinte in einem Glas Wasser vor. Es bleibt verbunden.

Auch die Einstellung «Nicht fürs Training verwenden» sichert Ihre Daten gut, aber nicht absolut, da Daten weiterhin verarbeitet werden müssen, damit der Dienst funktioniert. Darum gilt: Geben Sie keine sensiblen Informationen in eine KI ein.

Bekannte Tools und was Sie prüfen können

Microsoft-Konto: Personalisierte Werbung

Microsoft passt seine Werbung anhand von Signalen wie Suchanfragen, der Nutzung von Microsoft-Diensten und ähnlichen Kontosignalen an die Nutzerinnen und Nutzer an, damit sie besser zu ihnen passt. Wer das nicht möchte, kann diese Funktion ausschalten. Öffnen Sie die Seite «Personalisierte Anzeigen & Angebote» und stellen Sie den Schalter auf «Aus».

Apple: iPhone und MAC

Ist bei einem iPhone oder einem Mac eine PIN oder ein Passwort aktiviert worden, greift zusätzlich ein weiterer Schutzmechanismus und zwar eine Verschlüsselung der Daten. Dazu kommt die Funktion App Tracking Transparency: Apps müssen fragen, ob sie Sie fürs Tracking verfolgen dürfen. Wenn Sie mehr Schutz wollen, aktivieren Sie die Zwei-Faktor-Authentifizierung für die Apple-ID, schalten auf dem Mac FileVault ein und nutzen für iCloud bei Bedarf Advanced Data Protection.

Google: Kaum einer weiss mehr über uns

Wenn Sie Ihren Google-Datenschutz generell erhöhen wollen, starten Sie am einfachsten mit dem Privatsphäre-Check und der Aktivitätssteuerung im Google-Konto. Dort können Sie Web- und App-Aktivität sowie Standortverlauf und YouTube-Verlauf pausieren oder eine automatische Löschung aktivieren. Für weniger Tracking lohnt es sich zudem, die personalisierte Werbung in «Mein Anzeigen-Center» auszuschalten. Und im Sicherheitscheck aktivieren Sie die Zwei-Faktor-Authentifizierung und prüfen, welche Geräte und Apps Zugriff haben.

Schnelles Anmelden mit Google, Apple oder Facebook

Beim schnellen Log-in, zum Beispiel mit der Option «Mit Google anmelden», entstehen viele Datenflüsse. Damit geben Sie der App mindestens Ihre E-Mail-Adresse bekannt, wobei oft auch Name und Profilbild preisgegeben werden können. Je nach Berechtigungen in den AGB kann die App auf Kalender, Drive oder sogar Mails zugreifen. Das kann sinnvoll sein, aber nicht immer. Meine zwei Tipps:

1. Verknüpfen Sie keine Konten. Erstellen Sie für neue Apps stattdessen ein Log-in mit einer E-Mail-Adresse und einem neuen Passwort.
2. In den Google-Kontoeinstellungen sehen Sie alle verbundenen Apps und können unnötige Zugriffe mit wenigen Klicks entfernen.

LinkedIn: Networking mit KI-Training

Seit dem Update im Herbst 2025 nutzt LinkedIn die Daten und Inhalte seiner Mitglieder, um KI-Modelle zu trainieren. Private Nachrichten sind davon ausgenommen. Wer widersprochen hat, wurde davon ausgenommen.

So widersprechen Sie für künftige Anwendungen:

1. Öffnen Sie LinkedIn und gehen Sie zu **Einstellungen & Datenschutz**.
2. Wählen Sie links **Datenschutz**.
3. Öffnen Sie **Daten zur Verbesserung generativer KI**.
4. Schalten Sie **Ihre Daten zum Schulen von KI-Modellen verwenden, um Inhalte zu erstellen** auf **Aus**.

Ist die Einstellung aktiv, wirkt sie sich nur für die Zukunft aus, leider nicht rückwirkend.

ChatGPT: 3 kleine Schritte für besseren Datenschutz

Geben Sie keine sensiblen Infos ein, bevor Sie die Einstellungen geprüft haben. Mit drei Handgriffen können Sie die Nutzung Ihrer Inhalte fürs Training reduzieren und Ihre Privatsphäre verbessern.

1. Melden Sie sich an, öffnen Sie **Einstellungen → Datenkontrolle** und schalten Sie **«Das Modell für alle verbessern»** aus. So werden Ihre Chats nicht fürs Training der KI verwendet.
2. Für Vertrauliches nutzen Sie **Temporären Chat aktivieren** oben rechts in der App. Laut OpenAI wird er nicht in der History gespeichert. Für Sicherheitszwecke kann eine Kopie bis zu 30 Tage aufbewahrt werden.
3. Ersetzen Sie stets **sensible Daten** wie Namen, Telefon-, Kontonummern etc. mit Platzhaltern.

Viele KI-Tools bieten ähnliche Einstellungsmöglichkeiten an. Nutzen Sie diese Einstellungen, wo immer es möglich ist.

Fazit: Vertrauen ist gut, Kontrolle ist besser

AGB lesen sich nicht immer einfach. Ich gebe zu, auch ich bin nicht immer konsequent. Einige Tools haben sehr kurze AGB, andere schreiben mehr als 50 Seiten. Bei diesen langen Texten sollten Sie wirklich vorsichtig sein. Mit dem 7-Punkte-Quickscan finden Sie das Wichtigste sehr schnell. Ich verspreche Ihnen, sobald die Routine da ist, wird es immer einfacher.

Corina Zingg

ist Geschäftsführerin von CreaLengo, dem Weiterbildungsinstitut für Jobcoaches, Ausbilderin mit eidg. FA und MAS Business Psychology. Sie arbeitet regelmässig mit KI Tools und kennt sich mit den neuesten Trends aus.

crealengo.ch