

Welche Daten gebe ich bei Benutzung von Apps frei

1. Gesammelte Nutzerdaten nach Unternehmen (Google, Meta, Microsoft, Samsung, Apple)

Gesammelte Nutzerdaten nach Unternehmen

Unternehmen	Gesammelte Daten
Google	Persönlich: Name, E-Mail, Telefonnummer, Geburtsdatum, Geschlecht, Adresse, Zahlungsdaten (Google Pay), Sprachaufnahmen (Assistant). Nutzung: Suchverlauf, YouTube-Verlauf, Standorthistorie, App-Nutzung, Geräte-IDs, IP-Adresse, Cookies. Inhalte: E-Mails (Gmail), Fotos (Google Fotos), Dokumente (Drive), Kalendereinträge. Kontakte: Adressbuch (bei Sync). Sensoren: Bewegungsdaten (Fitbit), Mikrofon.
Meta (Facebook, Instagram, WhatsApp)	Persönlich: Name, E-Mail, Telefonnummer, Geburtsdatum, Geschlecht, Profilbilder, Beziehungen. Nutzung: Likes, Shares, Kommentare, Suchanfragen, Standorthistorie, Geräte-IDs, IP-Adresse, Cookies, Zeitstempel. Inhalte: Fotos/Videos (hochgeladen), Nachrichten-Metadaten (nicht Inhalte bei WhatsApp). Kontakte: Adressbuch (bei Sync). Biometrie: Gesichtsgeometrie (in einigen Regionen). Zahlungen: Marketplace/Werbeanzeigen.
Microsoft	Persönlich: Name, E-Mail, Telefonnummer, Geburtsdatum, Adresse, Zahlungsdaten (Xbox/Store). Nutzung: Suchverlauf (Bing), Browserverlauf (Edge), Standorthistorie, App-Nutzung (Office/Windows), Geräte-IDs, IP-Adresse, Cookies. Inhalte: E-Mails (Outlook), Dokumente (OneDrive), Kalendereinträge, Chats (Skype/Teams). Kontakte: Adressbuch (bei Sync). Sensoren: Mikrofon (Cortana), Kamera.
Samsung	Persönlich: Name, E-Mail, Telefonnummer, Samsung-Konto. Nutzung: App-Nutzung, Geräte-IDs, IP-Adresse, Standorthistorie, Suchanfragen (Samsung Browser). Inhalte: Fotos/Videos (Galerie), Notizen, Kalendereinträge, Sprachnotizen. Kontakte: Adressbuch (bei Sync). Sensoren: Bewegungsdaten (Samsung Health), Biometrie (Fingerabdruck/Gesicht). Zahlungen: Samsung Pay. Sprache: Bixby-Aufnahmen.

Apple **Persönlich:** Name, E-Mail, Telefonnummer, Apple-ID, Adresse, Zahlungsdaten (App Store/Apple Pay).

Nutzung: App-Nutzung, Geräte-IDs, IP-Adresse, Standorthistorie, Suchanfragen (Safari).

Inhalte: Fotos/Videos (iCloud), Notizen, Kalendereinträge, E-Mails (iCloud Mail), Sprachnotizen.

Kontakte: Adressbuch (bei iCloud-Sync).

Sensoren: Bewegungsdaten (Apple Watch/Health), Biometrie (Touch ID/Face ID).

Sprache: Siri-Aufnahmen (anonymisiert).

2. Vorteile und Nachteile: Anmeldung mit Benutzername/Passwort vs. Google-/Apple-/Microsoft-Konto

Vorteile und Nachteile der Anmeldemethoden

Kriterium	Benutzername + Passwort	Google-/Apple-/Microsoft-Konto
Vorteile	Datenschutz: Weniger Daten werden mit Dritten geteilt. Kontrolle: Volle Kontrolle über die Anmeldedaten. Sicherheit: Keine Abhängigkeit von externen Anbietern.	Bequemlichkeit: Kein neues Passwort merken, schnelle Anmeldung. Integration: Zugriff auf zusätzliche Dienste (z. B. Kalender, Kontakte, Cloud-Speicher). Sicherheit: Oft Zwei-Faktor-Authentifizierung (2FA) standardmäßig aktiviert.
Nachteile	Aufwand: Viele Passwörter merken oder Passwort-Manager nutzen. Sicherheitsrisiko: Schwache Passwörter oder Wiederverwendung erhöhen das Risiko von Hacking.	Datenschutz: Mehr persönliche Daten werden mit dem Anbieter (Google/Apple/Microsoft) geteilt. Abhängigkeit: Bei Problemen mit dem Hauptkonto (z. B. Sperrung) ist der Zugriff auf alle verknüpften Dienste blockiert. Tracking: Anbieter können Nutzerverhalten über mehrere Dienste hinweg verfolgen.
Empfehlung	Für Nutzer, die Datenschutz und Kontrolle priorisieren.	Für Nutzer, die Bequemlichkeit und Integration bevorzugen und den Anbietern vertrauen.

3. Instagram, Facebook, WhatsApp: Gesammelte Daten, Nicht gesammelte Daten, Einsehbare Daten (auch bei E2E-Verschlüsselung)

Daten bei Meta-Diensten (Instagram, Facebook, WhatsApp)

Dienst	Gesammelte Daten	Nicht gesammelte Daten	Einsehbare Daten (auch bei E2E-Verschlüsselung)
Instagram	Profilinformationen, Fotos/Videos, Likes, Kommentare, Suchanfragen, Standorthistorie, Geräte-IDs, IP-Adresse, Cookies, Kontakte (bei Sync), Nachrichten-Metadaten.	Inhalte privater Direktnachrichten (DMs) (nur bei E2E-Verschlüsselung in Secret Chats).	Metadaten: Wer kommuniziert mit wem, wann, wie oft, Geräteinformationen, IP-Adresse, Standort (bei Freigabe).
Facebook	Profilinformationen, Posts, Likes, Shares, Kommentare, Suchanfragen, Standorthistorie, Geräte-IDs, IP-Adresse, Cookies, Kontakte (bei Sync), Gruppenmitgliedschaften, Events.	Inhalte privater Nachrichten (Messenger) (nur bei E2E-Verschlüsselung in Secret Chats).	Metadaten: Absender/Empfänger, Zeitstempel, Geräteinformationen, IP-Adresse, Standort (bei Freigabe).
WhatsApp	Telefonnummer, Profilname, Profilbild, Kontakte (bei Sync), Geräte-IDs, IP-Adresse, Standorthistorie (bei Freigabe), Nachrichten-Metadaten (wer, wann, wie lange).	Inhalte der Nachrichten, Fotos, Videos, Sprachnachrichten, Dateien (bei E2E-Verschlüsselung).	Metadaten: Wer kommuniziert mit wem, wann, wie oft, Geräteinformationen, IP-Adresse, Standort (bei Freigabe).

Hinweise zu WhatsApp:

- **End-zu-End-Verschlüsselung (E2E):** Betrifft **nur die Inhalte** der Nachrichten (Text, Fotos, Videos, Sprachnachrichten). **Metadaten** (z. B. wer mit wem schreibt, wann, wie lange) sind für Meta einsehbar.
- **Backups:** Wenn Backups in Google Drive/iCloud gespeichert werden, sind diese **nicht E2E-verschlüsselt** (außer bei WhatsApp-Backup-Verschlüsselung).
- **Gruppenchats:** Bei Gruppenchats sieht Meta, wer in der Gruppe ist und wer Nachrichten sendet, aber nicht den Inhalt (bei E2E).

Fazit:

- **E2E-Verschlüsselung schützt nur die Inhalte**, nicht die Metadaten.
 - **Meta sammelt keine Inhalte** von E2E-verschlüsselten Chats, aber alle Metadaten.
 - **Einsehbar sind immer die Metadaten**, auch bei E2E.
-

Glossar:

Social Login	Der Social Login ist eine vereinfachte Anmeldemethode, die es Nutzern ermöglicht, sich über ihre bestehenden Konten bei sozialen Netzwerken auf Drittanbieter-Websites anzumelden. Dies reduziert den Aufwand für die Erstellung neuer Konten und bietet Entwicklern wertvolle demografische Daten. Social Login – Definition, Erklärung und Tipps
Identity Provider	Ein Identitätsanbieter (IdP) ist ein Dienst, der die Identität eines Benutzers speichert und verifiziert. IdPs sind in der Regel Cloud-gehostete Dienste. Oft arbeiten sie mit Single-Sign-On-Providern (SSO) zusammen, um Benutzer zu authentifizieren. Es gibt Unternehmen (Google, Facebook, etc., die gegenüber Drittanbietern als IdP auftreten)
Drittanbieter-Website	Eine Drittanbieter-Webseite ist eine Website oder ein Dienst, der von einem Unternehmen oder Entwickler betrieben wird, der nicht der ursprüngliche Anbieter der Hauptwebsite ist, und kann Funktionen, Inhalte oder Datenzugriffe bereitstellen. 8 Gebräuchlichste Drittanbieterdienste auf Websites und deren Datenschutzrisiken
2FA	Zweifaktoraauthifizierung: Quelle: Microsoft Das Wichtigste in Kürze • Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit bei der Anmeldung, indem zwei unterschiedliche Formen der Identitätsprüfung verlangt werden. • Die Verwendung von 2FA hilft, unbefugten Zugriff zu verhindern, selbst wenn ein Kennwort gestohlen oder kompromittiert wurde. • Gängige 2FA-Methoden umfassen Push-Benachrichtigungen in mobilen Apps mit Genehmigungen, SMS-Codes, Biometrie und physische Sicherheitscodes. • 2FA verringert die Auswirkungen von Phishing, Diebstahl von Zugangsdaten und Brute-Force-Angriffen. • Die Implementierung von 2FA unterstützt die Einhaltung von Vorschriften und schützt sowohl persönliche als auch organisatorische Daten. • Integrierte Microsoft-Tools wie Authenticator und MFA machen sichere Anmeldungen einfach und skalierbar.
Tracking im Kontext von Social Login	In der Welt des Social Login ist Tracking oft mit der Überwachung und Analyse von Aktivitäten in sozialen Medien verbunden. Es umfasst die Sammlung von Daten über Nutzer, um Verhaltensmuster und Präferenzen zu identifizieren. Dies kann zu Risiken für die Privatsphäre führen, da persönliche Daten ohne Zustimmung gesammelt werden können. Methoden zum Schutz vor Social Media Tracking umfassen die Nutzung von Datenschutzeinstellungen und VPNs. Regelmäßige Datenschutzprüfungen und -aktualisierungen sind wichtig, um die Privatsphäre in sozialen Medien zu schützen. DigitalCheckNRW

Schritt für Schritt Anleitung zum Herausfinden, bei welchen **Drittanbieter-Diensten oder Apps** man mit einem **Google-, Meta (Facebook/Instagram), Apple- oder Microsoft-Konto** angemeldet ist.

1. Google-Konto: Verknüpfte Apps & Dienste

So findest du alle Dienste, die mit deinem Google-Konto verknüpft sind:

1. Gehe zu myaccount.google.com und melde dich an.
2. Klicke links im Menü auf "Sicherheit".
3. **Scrolle nach unten zu "Drittanbieter-Apps mit Kontozugriff".
 - Hier siehst du eine **Liste aller Apps/Dienste**, die Zugriff auf dein Google-Konto haben (z. B. für Anmeldung oder Datenzugriff).
4. Klicke auf eine App, um Details zu sehen (z. B. Berechtigungen).
5. Entferne Zugriff, falls eine App verdächtig oder nicht mehr benötigt wird.

Zusätzlich:

- Unter "Passwortmanager" (links im Menü) siehst du **gespeicherte Logins** für Websites, bei denen du dich möglicherweise mit Google angemeldet hast.
-

2. Meta (Facebook/Instagram): Verknüpfte Apps & Websites

So prüfst du, welche Apps/Websites mit deinem Facebook- oder Instagram-Konto verknüpft sind:

Für Facebook:

1. Gehe zu [Facebook](https://facebook.com) und melde dich an.
2. Klicke auf dein Profilbild (oben rechts) → "Einstellungen & Privatsphäre" → "Einstellungen".
3. Gehe zu "Apps und Websites" (links im Menü).
 - Hier siehst du eine **Liste aller Apps/Dienste**, die mit deinem Facebook-Konto verknüpft sind.
4. Klicke auf eine App, um zu sehen, welche **Berechtigungen** sie hat.
5. Entferne Apps, die du nicht mehr verwendest (Button "Entfernen").

Für Instagram:

1. Öffne die Instagram-App oder gehe zu instagram.com.
2. Gehe zu deinem Profil → "Einstellungen" → "Sicherheit" → "Apps und Websites".
 - Hier siehst du **aktive und abgelaufene Verknüpfungen**.

3. Apple-ID: Verknüpfte Apps & Dienste

So findest du Dienste, die mit deiner Apple-ID verknüpft sind:

1. Gehe zu appleid.apple.com und melde dich an.
2. **Scrolle nach unten zu "Sicherheit" und klicke auf "Apps & Websites, die deine Apple-ID verwenden".
 - Hier siehst du eine **Liste aller Apps/Dienste**, die mit deiner Apple-ID verknüpft sind (z. B. für "Mit Apple anmelden").
3. **Klicke auf eine App**, um Details zu sehen oder den Zugriff zu **entfernen**.

Alternative (auf dem iPhone/iPad):

- **Einstellungen** → [Dein Name] → "Passwörter & Sicherheit" → "Apps, die deine Apple-ID verwenden".

4. Microsoft-Konto: Verknüpfte Apps & Dienste

So prüfst du, welche Apps mit deinem Microsoft-Konto verknüpft sind:

1. Gehe zu account.microsoft.com und melde dich an.
2. **Klicke auf "Sicherheit"** (oben im Menü).
3. **Gehe zu "Berechtigungen für andere Apps" oder "Apps mit Zugriff auf dein Konto"**.
 - Hier siehst du eine **Liste aller Apps/Dienste**, die Zugriff auf dein Microsoft-Konto haben.
4. **Klicke auf eine App**, um Berechtigungen zu prüfen oder den Zugriff zu **entfernen**.

Zusätzlich:

- Unter "**Geräte**" siehst du, auf welchen Geräten dein Microsoft-Konto aktiv ist.

Zusammenfassung der Links für schnellen Zugriff

Anbieter	Link zur Verwaltung verknüpfter Apps/Dienste
Google	myaccount.google.com → Sicherheit → Drittanbieter-Apps
Meta (Facebook)	Facebook-Einstellungen → Apps und Websites
Meta (Instagram)	Instagram-Einstellungen → Sicherheit → Apps und Websites
Apple	appleid.apple.com → Sicherheit → Apps & Websites
Microsoft	account.microsoft.com → Sicherheit → App-Berechtigungen

Tipps für mehr Sicherheit

✅ **Regelmäßig prüfen:** Überprüfe diese Listen alle **3–6 Monate**. ✅ **Unbekannte Apps entfernen:** Falls du eine App nicht kennst, entferne den Zugriff. ✅ **Zwei-Faktor-Authentifizierung aktivieren** für alle Konten. ✅ **Passwortmanager nutzen** (z. B. Bitwarden, 1Password), um Logins zu tracken.

Falls du Hilfe bei einem bestimmten Anbieter brauchst oder etwas unklar ist, lass es mich wissen! **Welchen Anbieter möchtest du als Erstes überprüfen?**

Schritt-für-Schritt-Anleitungen, zum Herausfinden wo man mit Konten (Samsung, Google, Facebook) angemeldet ist:

1. Google-Konto: Geräte und Standorte anzeigen

Schritte:

1. **Öffne einen Browser** und gehe zu myaccount.google.com.
2. **Melde dich an** mit deinem Google-Konto.
3. **Klicke links im Menü** auf **"Sicherheit"**.
4. **Scrolle nach unten** zu **"Ihre Geräte"** und klicke darauf.
5. Hier siehst du eine **Liste aller Geräte**, auf denen dein Konto aktiv ist, inklusive **Standort, Datum und Uhrzeit der letzten Nutzung**.
6. **Klicke auf ein Gerät**, um Details wie IP-Adresse und ungefähren Standort zu sehen.

Zusätzlich:

- Unter **"Sicherheitswarnungen"** siehst du verdächtige Anmeldungen.
 - Du kannst **unbekannte Geräte entfernen**, indem du auf **"Mehr Details"** und dann **"Abmelden"** klickst.
-

2. Samsung-Konto: Angemeldete Geräte prüfen

Schritte:

1. **Öffne die Samsung-Website** unter account.samsung.com und melde dich an.
2. **Klicke auf dein Profilbild** (oben rechts) und wähle **"Kontoeinstellungen"**.
3. **Gehe zu "Sicherheit" oder "Geräteverwaltung"**.
4. Hier siehst du eine **Liste aller Geräte**, die mit deinem Samsung-Konto verknüpft sind, inklusive **Modell und letzte Anmeldung**.
5. **Klicke auf ein Gerät**, um Details zu sehen oder es zu entfernen.

Alternative (auf dem Smartphone):

- Öffne die **Einstellungen** → **"Konten und Backup"** → **"Konten verwalten"** → Wähle dein Samsung-Konto → **"Geräteverwaltung"**.

3. Facebook-Konto: Aktive Sitzungen prüfen

Schritte:

1. **Öffne Facebook** in einem Browser oder in der App.
2. **Klicke auf dein Profilbild** (oben rechts) und wähle **"Einstellungen & Privatsphäre"** → **"Einstellungen"**.
3. **Gehe zu "Sicherheit und Anmeldung"** (links im Menü).
4. **Scrolle nach unten zu "Wo du angemeldet bist"**.
5. Hier siehst du eine **Liste aller aktiven Sitzungen** mit:
 - **Gerätetyp** (z. B. iPhone, Android, Windows)
 - **Standort** (Stadt/Land)
 - **Datum und Uhrzeit der Anmeldung**
6. **Klicke auf die drei Punkte (:)** neben einer Sitzung, um sie zu **beenden** (falls verdächtig).

Tipp:

- Aktiviere **"Zwei-Faktor-Authentifizierung"** für mehr Sicherheit.

Wichtig bei verdächtigen Anmeldungen

- **Ändere sofort dein Passwort** für das betroffene Konto.
- **Aktiviere die Zwei-Faktor-Authentifizierung**, falls noch nicht geschehen.
- **Überprüfe deine E-Mails** auf verdächtige Anmeldebenachrichtigungen.

Erstellt mit KI Mistral le Chat / Vibes

13.07.2026 / Jaqueline Harr / Peter Schafroth