

04.09.2025

App-Berechtigungen: So behalten Sie die Kontrolle über Ihre Daten

Viele Apps verlangen beim Installieren mehr Zugriffsrechte, als für ihre Funktion notwendig ist. Wer Berechtigungen regelmässig überprüft und einschränkt, schützt nicht nur seine Privatsphäre, sondern verhindert auch die ungewollter Datennutzung im Hintergrund.

Egal ob Fotofilter, Spiele oder Social-Media-Apps, viele Anwendungen fordern Zugriff auf Funktionen und Daten auf Ihrem Smartphone. Sinnvoll ist das, wenn der Zugriff technisch erforderlich ist, etwa wenn eine Fotobearbeitungs-App auf die Galerie zugreifen muss oder eine Navigations-App Standortdaten benötigt. Häufig verlangen Apps jedoch weitreichendere Berechtigungen – wie etwa eine Taschenlampen-App, die auf Ihre Kontakte zugreifen möchte. Solche übermässigen Zugriffsrechte können Risiken bergen.

Das können Sie tun:

Android

- **Zugriffsrechte jederzeit anpassen:** In den Einstellungen können Sie App-Berechtigungen aktivieren oder entziehen.
- **Eingeschränkte Berechtigung:** Sensible Rechte wie Kamera, Mikrofon oder Standort können Sie seit Android 11 temporär «Nur diesmal» oder «Beim Verwenden der App erlauben» vergeben, statt dauerhaft.
- **Automatische Rücknahme bei Inaktivität:** Apps, die über längere Zeit nicht genutzt werden, verlieren automatisch sensible Zugriffsrechte, wie z.B. auf die Kamera oder Kontaktdaten.

iPhone

- **Berechtigungen gezielt verwalten:** Unter Einstellungen > Datenschutz & Sicherheit wählen Sie Kategorien wie Kamera, Mikrofon oder Ortungsdienste aus und sehen, welche Apps Zugriff haben und können diesen gezielt entziehen.
- **Eingeschränkte Berechtigung:** Sensible Rechte wie Kamera, Mikrofon oder Standort können Sie temporär «Einmal erlauben» oder «Beim Verwenden der App erlauben» vergeben, statt dauerhaft.
- **App Privacy Report:** Diese Funktion zeigt, wann und wie Apps auf Informationen von Kamera und Mikrofon sowie Netzwerkaktivitäten zugreifen.