

Mobilgeräte

Hinweis: Da Betriebssysteme für Mobilgeräte laufend weiterentwickelt und von den Geräteherstellern stark angepasst werden, ist es möglich, dass bestimmte Einstellungen bei dir nicht auffindbar oder unter anderen Menüpunkten zu finden sind.

Datenschutzfreundliche Einstellungen

- Smartphones gehen oft verloren oder werden geklaut. Damit Fremde nicht direkt auf dein Gerät zugreifen können, solltest du **einen Pin oder ein Passwort zum Entsperren** des Geräts wählen. Insbesondere Wischgesten und Sperrmuster bieten oft keinen ausreichenden Schutz vor Fremdzugriff.
- **WLAN, GPS, Bluetooth, etc. nur bei Bedarf aktivieren.** Dann werden auch keine unnötigen Daten versendet und der Akku geschont
- **Synchronisation abschalten** (Kalender, Kontakte, etc.). Diese privaten Daten musst du nicht mit Datenkraken teilen.
- **Browser** (Firefox) **konfigurieren:** Keine Cookies von Drittanbietern zulassen, Adblocker installieren, Do-Not-Track aktivieren, (Standard)Suchmaschine anpassen. Viele Empfehlungen unseres Browser-Handouts lassen sich auch parallel auf dem Smartphone umsetzen.
- Android:
 - **Datenschutzmodus standardmäßig aktivieren** (*Einstellungen* → *Datenschutz*). Unter *Einstellungen* → *Apps* unnötige App-Berechtigungen entziehen
 - In der App **Google-Einstellungen** alles Unnötige deaktivieren
- iOS:
 - Unter *Einstellungen* → *Datenschutz* **Zugriff von Apps beschränken.**

Dateisystem verschlüsseln

Damit die Daten auf dem Gerät bei Diebstahl oder Verlust nicht ausgelesen werden können, solltest du das Dateisystem verschlüsseln.

- **Android:** *Einstellungen* → *Sicherheit* → *Smartphone verschlüsseln*
- **iOS:** Ab Version 8 integriert

Verschlüsselt kommunizieren

E-Mail-Verschlüsselung ist auch auf Smartphones möglich. Unter Android geht dies mit **K-9 Mail** und **OpenKeychain**. Allerdings ist die Wahrscheinlichkeit mangels Gerätehoheit größer, dass du die Kontrolle über deinen privaten Schlüssel verlierst.

Als mögliche Alternative zu WhatsApp & Co ist **Signal** einen Blick wert, das im Gegensatz zu vielen Konkurrenten freie Software ist (Android: <https://signal.org/android/apk/>). Auch SMS & MMS (via **Signal**, **Silence**) und Chats via Jabber/XMPP (**Conversations** auf Android, **ChatSecure** auf iOS) lassen sich verschlüsseln.

Exkurs zu Android

Schritt 1: Google-Apps deinstallieren/deaktivieren

Unter **Einstellungen** → **Apps** kannst du Apps deinstallieren oder je nach Android-Version wenigstens deaktivieren, sofern du sie nicht unbedingt nutzen willst. Oft musst du ausprobieren, wie stark das Deaktivieren bzw. Deinstallieren dieser Apps den Betrieb deines Systems einschränkt. Hier ist eine Liste von (meist unfreier) Android-Software, deren Deaktivierung ihr in Erwägung ziehen könnt:

<https://github.com/jaredsburrows/android-bloatware/blob/master/disable-list.txt>

Schritt 2: Alternative zum Play Store nutzen

F-Droid ist ein alternatives Verzeichnis für Apps („App Store“). Dort findet man ausschließlich freie Software, die häufig größeren Wert auf eure Privatsphäre legt als viele Apps im Play Store. Alternativ können sämtliche Apps auch als APKs direkt von der Website heruntergeladen werden. <https://f-droid.org/>

Zur Installation von Apps aus F-Droid und APK-Dateien musst du ggf. **die Installation von Apps aus unbekannten Quellen zulassen** (*Einstellungen* → *Sicherheit* → *Unbekannte Herkunft*).

Schritt 3: Datenschutzfreundliche Apps & Dienste nutzen

Zu vielen unfreien, kostenpflichtigen Apps und vorinstallierten Diensten von Google gibt es freie Alternativen, bei denen in der Regel deutlich mehr Wert auf die Privatsphäre des Nutzers gelegt wird. Alle gelisteten Apps sind in **F-Droid** zu finden.

- **Amaze**: Ein schneller Dateimanager mit vielen Funktionen.
- **AntennaPod**: Verwaltung und Abspielen von Audiopodcasts.
- **AnySoftKeyboard**: Eine Alternative zur Hersteller/Android-Tastatur.
- **DAVdroid**: Kontakt-, Aufgaben und Kalendersynchronisation via CalDAV/CardDAV.
- **Etar**: Alternative Kalender-App zum Google Kalender.
- **Feeder**: Verwaltet und zeigt RSS/Atom-Feeds an.
- **FFUpdater**: Den Browser **Mozilla Firefox** herunterladen und aktualisieren.
- **Galerie**: Bild-/Medienbetrachter ohne Schnick-Schnack.
- **LibreOffice Viewer**: Betrachter für Office-Dateien, der besonders gut mit offenen Standards umgehen kann.
- **K-9 Mail**: Umfangreicher E-Mail-Client, kann in Verbindung mit OpenKeychain auch E-Mails verschlüsseln.
- **KeePassDroid**: Mit KeePassX kompatible Passwortverwaltung.
- **MuPDF**: Betrachter für PDF-Dateien.
- **Net Monitor**: Listet Netzwerkverbindungen aktiver Apps und Dienste auf.
- **NewPipe**: Client für YouTube, der auch Audio- und Videodownloads ermöglicht.
- **Obscr**: Ein flinker QR-Code-Scanner.
- **Offline Calendar**: Kalender ohne Online-Account/Synchronisation erstellen.
- **OpenKeychain**: GnuPG und Schlüsselmanagement unter Android
- **OsmAnd+**: Anwendung für Karten und Routenplanung, die auch offline funktioniert.

- **Transportr:** Öffentliche Verkehrsverbindungen und Fahrpläne abrufen.
- **Transistor:** Radio-/Audiostreams sammeln und abspielen.
- **Twidere:** Ein Twitter-/Microblogging-Client.
- **Vanilla Music:** Ein schlanker Musikplayer.
- **VLC:** Vom Desktop bekannter Video- und Audioplayer, der mit vielen Formaten umgehen kann. <https://www.videolan.org/vlc/download-android.html>

Weitere alternative Dienste zu unfreien Apps und Diensten findet ihr z.B. bei Prism-Break und bei der digitalen Selbstverteidigung bei DigitalCourage:

- <https://prism-break.org/de/categories/android/>
- <https://digitalcourage.de/digitale-selbstverteidigung/freie-apps-fuer-das-befreite-smartphone>

Schritt 4: Freies Android-Betriebssystem installieren (für Profis)

Vorinstallierte Versionen von Android enthalten oft Anpassungen des Herstellers und schränken die Anpassbarkeit stark ein. Auch die Dienste und Apps von Google sind häufig fest ins System integriert. Wer Google gänzlich entsagen will, sollte eine **alternative Android-Variante** auf seinem Gerät installieren. Das ist zwar meistens mit dem Verlust der Herstellergarantie verbunden, dafür wirst du wieder laufend mit Updates versorgt und hast auf deinem Gerät bei Bedarf Root-Zugriff (Stichwort **Gerätehoheit**), wodurch du jegliche Softwarekomponenten verändern kannst. Das Wiki von LineageOS (englisch) listet für viele Geräte die Schritte auf, wie man dort ein alternatives Betriebssystem installieren kann: <https://wiki.lineageos.org/>

WARNUNG: Installation auf eigene Gefahr! Wir können euch im Rahmen dieser Veranstaltung leider nicht bei der Installation unterstützen und haften nicht für Datenverlust, Geräteschäden und ähnliches.

- **LineageOS:** Der Quasi-Nachfolger zum beliebten CyanogenMod, der sich zwar noch in Entwicklung befindet, allerdings schon für über 150 Geräte verfügbar ist und grundsätzlich sehr stabil läuft.
 - <https://lineageos.org/>
- **Replicant:** Replicant will nicht nur einfach ein freies Betriebssystem sein, sondern setzt für die Hardwareunterstützung freie Gerätetreiber ein, die sonst von den Herstellern selbst oder Google stammen. Daher ist es nur für sehr wenige ältere Geräte verfügbar.
 - <https://www.replicant.us/>

Mike Kuketz hat in seinem Blog eine empfehlenswerte und äußerst detaillierte Artikelreihe **Your phone – your data: Android ohne Google** veröffentlicht, in der Schritt für Schritt erläutert wird, wie ihr euer Android-Smartphone und eure Daten den neugierigen Blicken von Google und anderen Datenkraken entziehen könnt. Zwar sind die Empfehlungen nicht mehr ganz auf dem aktuellen Stand (März 2016 mit Bezug auf das mittlerweile eingestellte CyanogenMod), allerdings gibt es nirgends einen ähnlich umfangreichen Guide, der sich mit der „Befreiung“ von Android-Smartphones beschäftigt: <https://www.kuketz-blog.de/your-phone-your-data-teil1/>

Einen aktuelle Artikelreihe zur datenschutzfreundlichen Einrichtung unter Android findet ihr dort ebenfalls: <https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/> (**Your Phone Your Data (light) – Android unter Kontrolle**)