



Einführung in Android im Hinblick auf den Schutz persönlicher Daten

Max Riegel

<riegel@max.franken.de>

Einführung in Android im Hinblick auf den Schutz persönlicher Daten

- Während das Apple iOS ein vollständig proprietäres System ohne Möglichkeit der Einsicht- und Einflussnahme durch die Benutzenden ist, basiert Android auf einem OpenSource Projekt, das von Google federführend vorangetrieben und leider durch proprietäre Komponenten weitgehend unter Kontrolle gehalten wird.
- Der Vortrag gibt einen Überblick über das Android Betriebssystem für Handys und Tablets insbesondere im Hinblick auf den Abgriff persönlicher Daten durch Google und andere Software-Hersteller. Es wird vorgestellt, wie man ein Android Handy oder Tablet auch ohne einen Google Account in Betrieb nehmen und nutzen kann, und was man auch sonst noch zum Schutz vor Überwachung und Manipulation machen kann.



Inhaltsübersicht

- Prolog
- Android Überblick
- Einfluss von Google auf Android
- Datenschutzbewusste Einrichtung von Android
- Zusammenfassung und Ausblick



Prolog

Über mich...

- Gründungsmitglied des KNF e.V. und KNF Kongressmaster
- Ehemals langjähriger Apple-Anwender
 - Macintosh ab 1986, iPhone ab 2007, iPad ab 2010
- Immer ‚multilingual‘ – früher privat Apple, beruflich Windows
- Hinwendung zu Linux/OpenSource ab ca 2015
 - Hauptgrund: Überwachung im Internet (E. Snowden, PRISM)
 - aber durchaus mit der Nutzer-Erwartung eines langjährigen Mac-Users 😊
- Notebook exklusiv mit Ubuntu seit 2019 (privat & beruflich)
- Migration zu Android OpenSource auf Handy/Tablet seit 2023
 - iPhone SE (2016) ==> Google Pixel 8/GrapheneOS im Mai 2025

Schwerpunktthema „Überwachung und Manipulation am Handy vermeiden“

- Schutz der Privatsphäre auf dem Handy ungleich schwieriger als auf dem Notebook/Desktop
 - Immer dabei, für alles genutzt
 - Sehr komplexe Vernetzung mit dem Internet durch App-Environment
- Lösungsansätze, aber keine wirklichen Lösungen
 - *„Lasst uns anfangen, auch wenn wir die Lösung noch nicht kennen!“*
- 4 Vorträge, 3 Lösungsansätze
 - Android Einführung zu den technisch-organisatorischen Grundlagen
 - LineageOS for microG (Max)
 - /e/ (Jan-Christoph)
 - GrapheneOS (Matthias)

Ist das nur ein Problem von Android?

Nein, überhaupt nicht!

- iPhones/iPads haben exakt die gleichen Probleme!

- ... aber als NutzerIn ist man voll Apple ausgeliefert,
- ... und Apple nutzt das schamlos aus.

- iOS und Android sind technisch sehr ähnlich, aber

- iOS ist vollständig proprietär und wird von Apple rigide kontrolliert,
- Android hat FOSS Anteile, die erlauben, Google zu vermeiden.

- Mit Android hat man eine Chance, sich selbst zu helfen.





Android Überblick

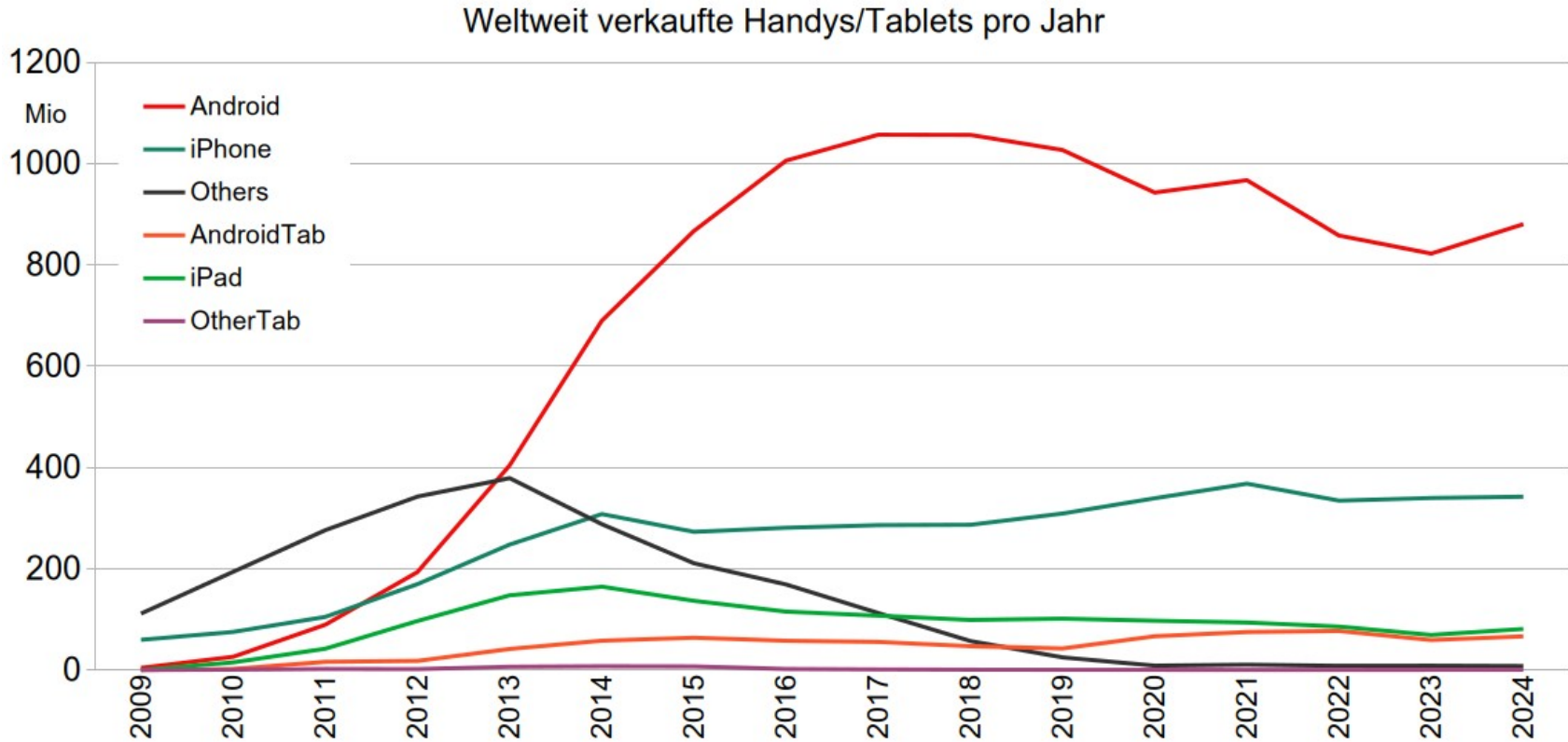
Die Entstehung von Android

- 2003: Gründung von Android Inc. durch Andy „Android“ Rubin and Chris White zur Entwicklung eines Softwaresystems für Mobilgeräte
- 2005: Übernahme von Android Inc. durch Google
- 2007: Google gründet mit 33 anderen Firmen die ‚Open Handset Alliance‘ zur Entwicklung eines OpenSource Betriebssystem für Mobiltelefone bekannt. Es wird das ‚Android Open Source Project (AOSP)‘ etabliert.
 - Verwendet den Linux Kernel (GPL)
 - Restliche FOSS hauptsächlich mit Apache Lizenz Modell
- 2008: Das erste Android Handy (HTC Dream) mit Android 1.0 erscheint.
- 2011: Es werden erstmals mehr Android Handys als iPhones verkauft.

Android Generationen

- **Android 1.0** [2008]: Erste offizielle Version mit Basis-Funktionen (Web, E-Mail, Kalender,...)
- **Android Eclair** (2.0) [2009]: Neue Benutzeroberfläche, mehrere Google-Konten
- **Android Honeycomb** (3.0) [2010]: Speziell für Tablets
- **Android Ice Cream Sandwich** (4.0) [2011]: Handy- und Tablet-Version in einem, Face Unlock
- **Android Lollipop** (5.0) [2014]: ‚Material Design‘ Oberfläche, verbesserte Benachrichtigungen
- **Android Marshmallow** (6.0) [2016]: App-Berechtigungen, Google Now on Tap
- **Android Nougat** (7.0) [2016]: Split-Screen-Multitasking, Google Assistant
- **Android Oreo** (8.0) [2017]: Bild-in-Bild-Modus, Inkrementelle Software-Updates
- **Android Pie** (9) [2018]: Gestensteuerung, adaptive Helligkeitssteuerung
- **Android 10** (Queen Cake) [2019]: Dunkelmodus, verbesserter Datenschutz und Sicherheit
- **Android 11** (Red Velvet Cake) [2020]: Verfeinerung der App-Berechtigungen
- **Android 12** (Snow Cone) [2021]: ‚Material You‘ Oberfläche, Datenschutzkontrolle
- **Android 13** (Tiramisu) [2022]: ‚Material You‘ Verbesserungen, verbesserte Tablet-Funktionen
- **Android 14** (Upside Down Cake) [2023]: Verbesserte Lokalisierung, Ultra HDR Fotos
- **Android 15** (Vanilla Ice Cream) [2024]: Private Space, Einführung von ‚Gemini‘ KI
- **Android 16** (Baklava) [2025]: ‚Material 3 Impressive‘ Oberfläche, Desktop-Modus

Android dominiert den Handy-Markt



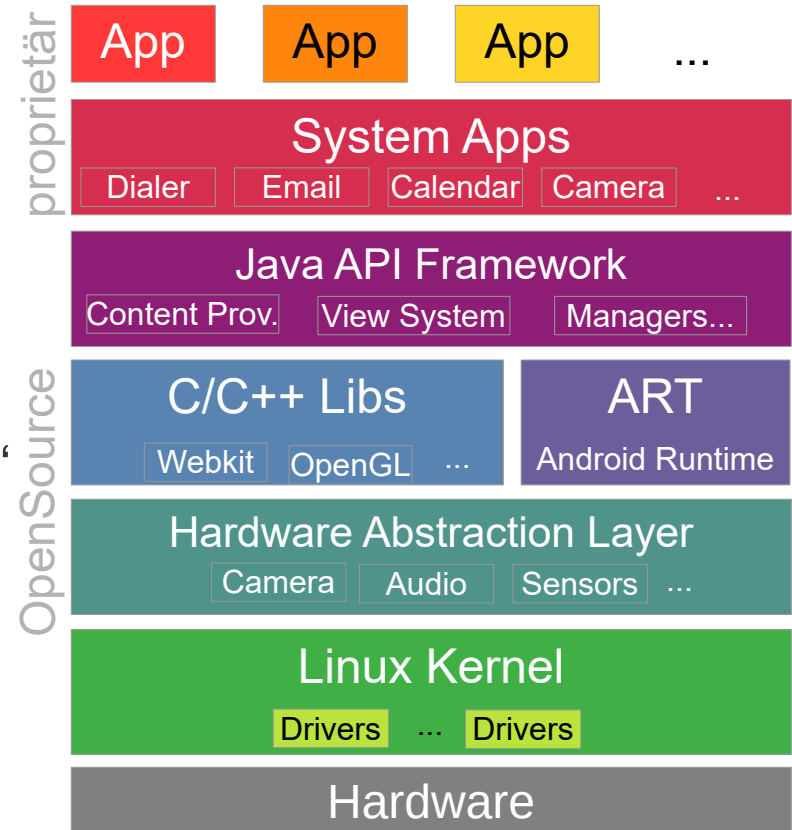
Quelle: IDC, Statcounter



Einfluss von Google auf Android

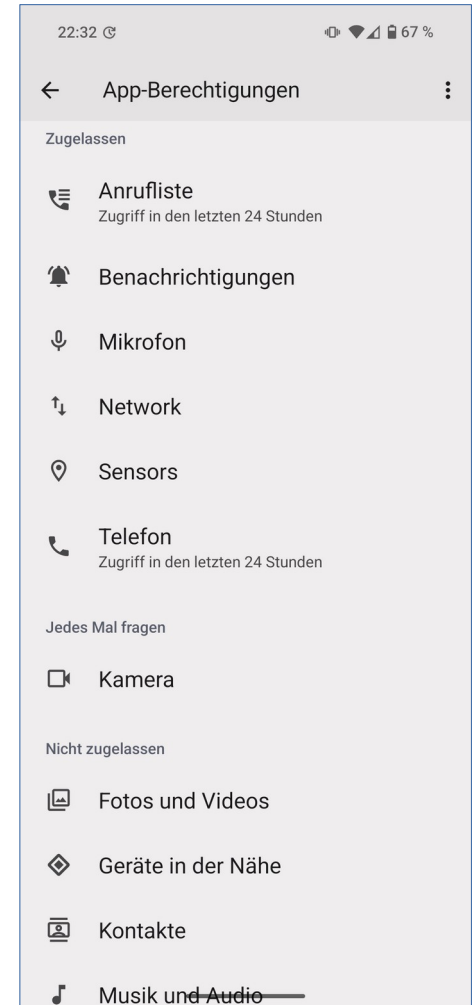
Android System Architektur

- Android ist eine Kombination von OpenSource und proprietärem Code.
 - Weiterentwicklung exklusiv durch Google
- Der OpenSource Anteil wird von Google im AOSP veröffentlicht.
- Google lizenziert seine proprietären System Apps als ‚Google Mobile Services‘ (GMS) an die Handy/Tablet-Hersteller.
- Viele wichtige Systemfunktionen (z.B. Standort, Benachrichtigungen) sind Teil der GMS App ‚Google Play Services‘



App Berechtigungen

- Apps sind streng voneinander isoliert und haben sehr beschränkten Zugriff auf Systemressourcen.
- Android besitzt ein sehr detailliertes System zur Rechteverwaltung von Apps.
 - Eingeschränkte Datenzugriffe
 - Eingeschränkte Aktionen
- Seit Android Marshmallow (6.0) müssen Apps ihre Berechtigungen explizit anfordern.
- Erteilte Berechtigungen können vom Benutzer jederzeit eingesehen und widerrufen werden.



System Apps – eine besondere Klasse

- Vom Hersteller im Systemverzeichnis vorinstalliert
- Können vom Benutzer nicht deinstalliert werden
- Stellen essentielle Gerätefunktionen zur Verfügung
 - Auch für andere Apps
- Haben ihre Berechtigungen per default
 - Benutzer hat nur beschränkten Einfluss auf die Berechtigungen von System Apps.

Liste von System-Apps

- com.android.bluetooth
- com.android.contacts
- com.android.keychain
- com.android.keyguard
- com.android.launcher
- com.android.nfc
- com.android.phone
- com.android.providers.downloads
- com.android.settings
- com.android.systemui
- com.android.vending
- com.google.android.deskclock
- com.google.android.dialer
- com.google.android.gms
- com.google.android.GoogleCamera
- com.google.android.gsf
- com.google.android.gsf.login
- com.google.android.inputmethod.latin
- com.google.android.marvin.talkback
- com.google.android.nfcprovision
- com.google.android.setupwizard
- com.google.android.webview

System Apps ,Google Mobile Services‘

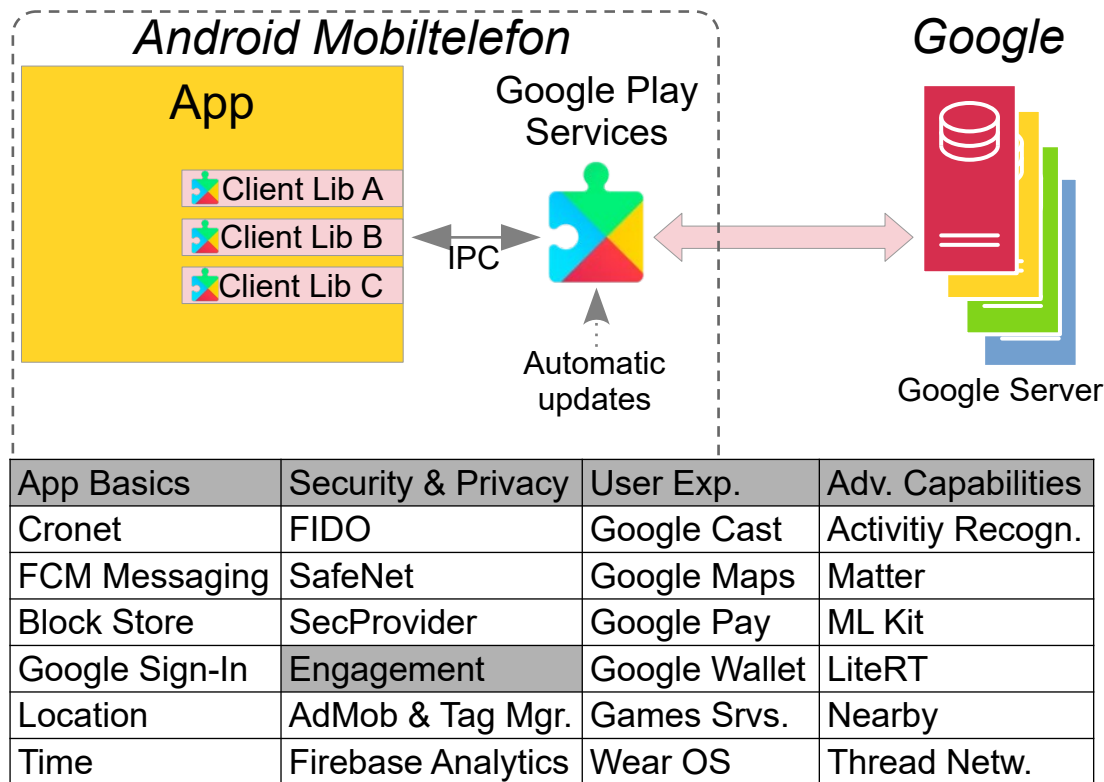
	Google Chrome	– Web Browser
	Gmail	– E-Mail Client
	Google Telefon	– Telefon
	Google Kontakte	– Adressbuch
	Google Kalender	– Kalender App
	Google Messages	– Kurznachrichten
	Google Meet	– online Konferenzen
	Google Maps	– Karten
	Google Photos	– Kamera App
	Google Drive	– Cloud Speicher
	Google Wallet	– Ticketspeicher
	YouTube	– Video Streaming
	Google Playstore	– App Store
	Google Play Services	– System services

Google Play Services

- Google stellt wichtige Funktionen für Apps zur Verfügung, z.B:

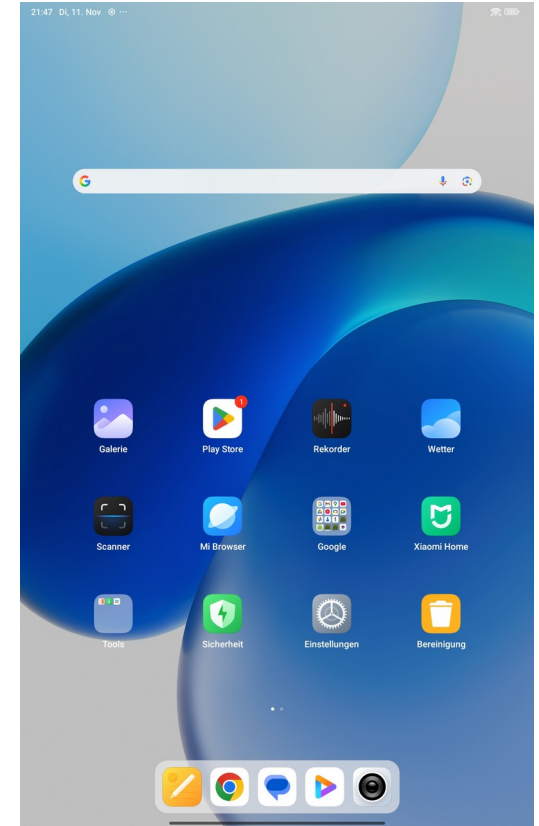
- Standort
- Authentisierung
- Benachrichtigung
- Sicherheitsprüfung
- Benutzer-Identifizierung
- Karten
- Bezahlendienste
- KI-Funktionen

- Google erhält damit Nutzer-Informationen auch von nicht-Google Apps.



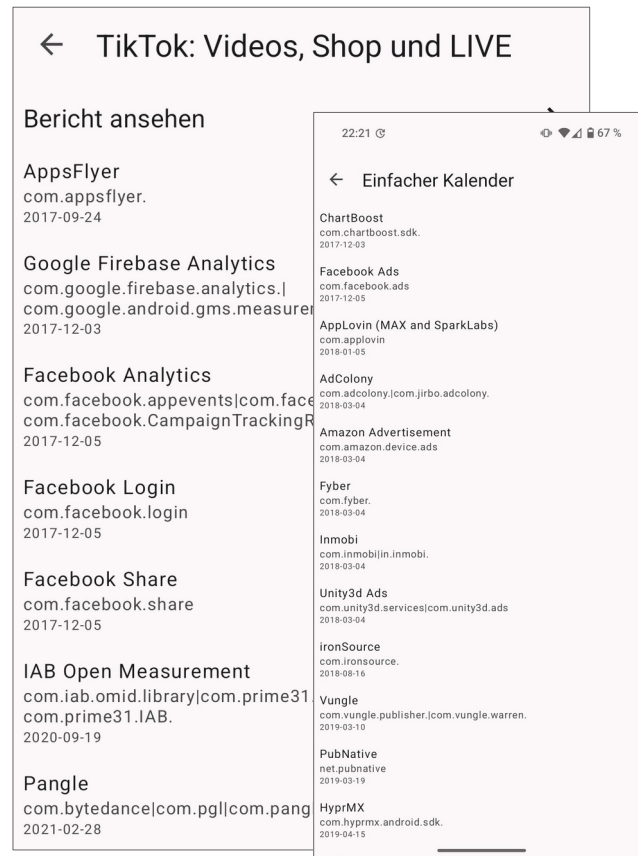
Das reale Android auf dem Gerät

- Vom Geräte-Hersteller aus AOSP + lizenziertes GMS + proprietäre Hardware-Driver erstellt
 - Wegen HW-Driver immer gerätespezifisch
- Häufig vom Geräte-Hersteller funktional angepasst und mit zusätzlichen System-Apps (Bloatware) ‚angereichert‘
 - Häufig auch Alternativen zu den GMS Apps
 - Zur Etablierung einer höheren Herstellerbindung
- Benutzer können konfigurieren, welche Apps zum Einsatz kommen.
 - Erlaubt nahezu unbegrenzte Konfigurierbarkeit von Android.



BTW: Nicht nur Google und Geräte-Hersteller spionieren...

- Auch andere Firmen stellen App-Entwicklern ‚hilfreiche‘ Libraries zur Erkundung der App-Nutzung und für Werbung zur Verfügung.
 - Tracker sind in Apps weit verbreitet
- Zur Information: Exodus Privacy (<https://exodus-privacy.eu.org/en/>) gibt Auskunft über Tracker in Apps
- Gerade ‚kostenlose‘ Apps übertreiben es manchmal mit dem Einsatz von Trackern.
 - Häufig technische Voraussetzung für Einnahmen aus Werbung





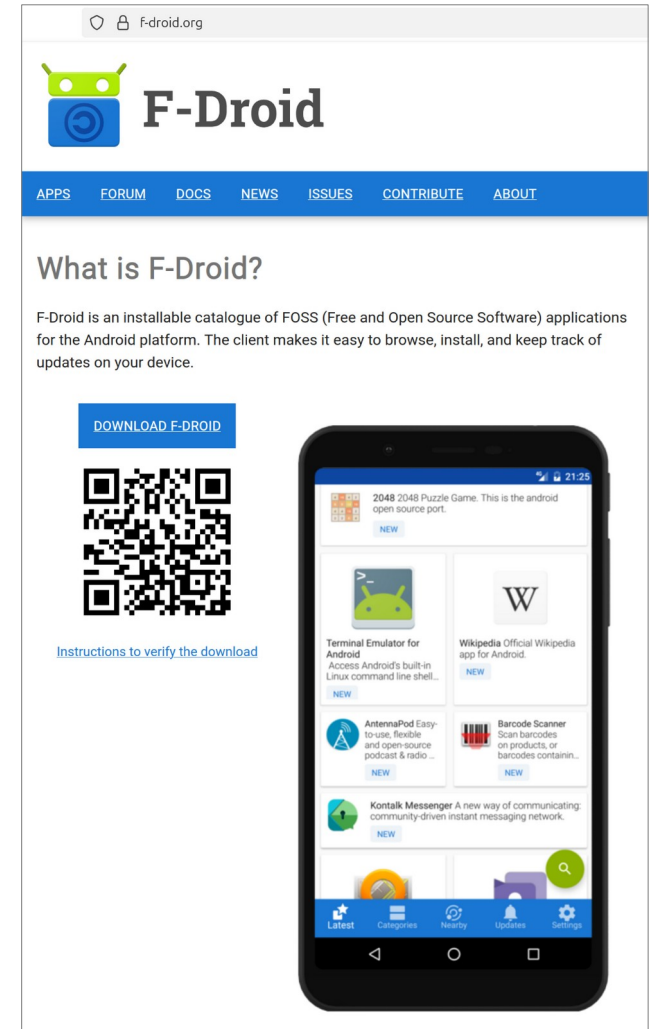
Datenschutzbewusste Einrichtung von Android

Datenschutzbewusste Einrichtung von Android

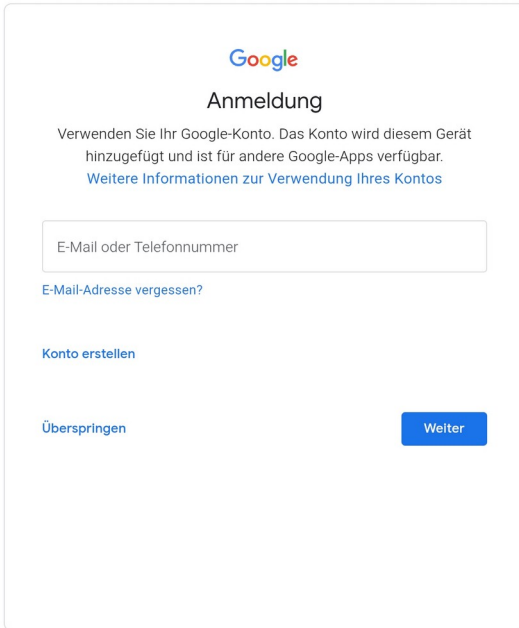
- Der unerwünschte Zugriff auf persönliche Daten kann beim Einrichten von Android stark beschränkt werden.
 - Keinen Google Account angeben
 - Beschränkt aber den Zugriff auf Google Dienste (z.B. Standort) erheblich
 - Berechtigungen so weit möglich abwählen
 - Keine Google Apps oder Dienste verwenden (z.B. Gmail)
 - Weitestgehend FOSS Apps aus dem F-Droid AppStore verwenden
 - Wenn notwendig, Google Playstore Apps anonym installieren.
- Möglicherweise Beschränkungen der Gerätefunktionalität, aber IMHO häufig akzeptierbar z.B. bei Tablets.

F-Droid AppStore

- Alternativer Android AppStore, der ausschließlich FOSS Apps bereithält.
- F-Droid baut selber die Installationspakete (.apk) aus den Sourcen und signiert sie mit dem F-Droid Schlüssel.
 - Sicherstellung dass die installierte App wirklich den frei zugänglichen Sourcen entspricht.
- F-Droid muss manuell auf dem Android Gerät installiert werden.



Keine Anmeldung bei Google



Google

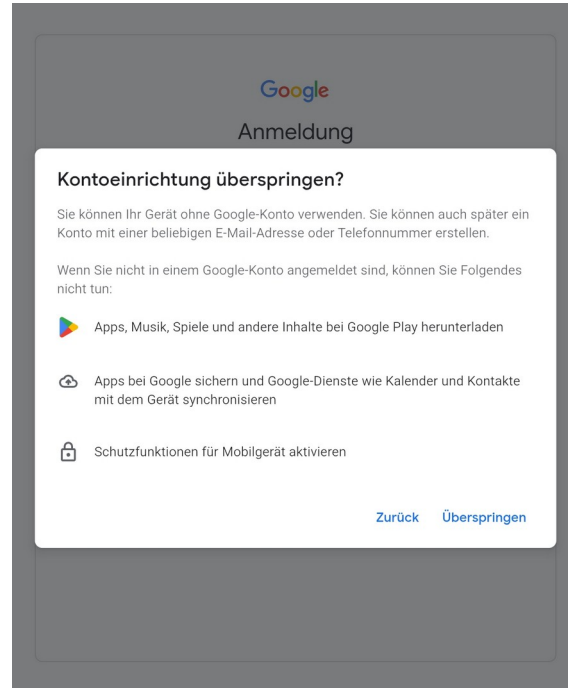
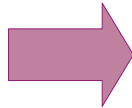
Anmeldung

Verwenden Sie Ihr Google-Konto. Das Konto wird diesem Gerät hinzugefügt und ist für andere Google-Apps verfügbar.
[Weitere Informationen zur Verwendung Ihres Kontos](#)

[E-Mail-Adresse vergessen?](#)

[Konto erstellen](#)

[Überspringen](#) [Weiter](#)






Google

Anmeldung

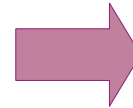
Kontoeinrichtung überspringen?

Sie können Ihr Gerät ohne Google-Konto verwenden. Sie können auch später ein Konto mit einer beliebigen E-Mail-Adresse oder Telefonnummer erstellen.

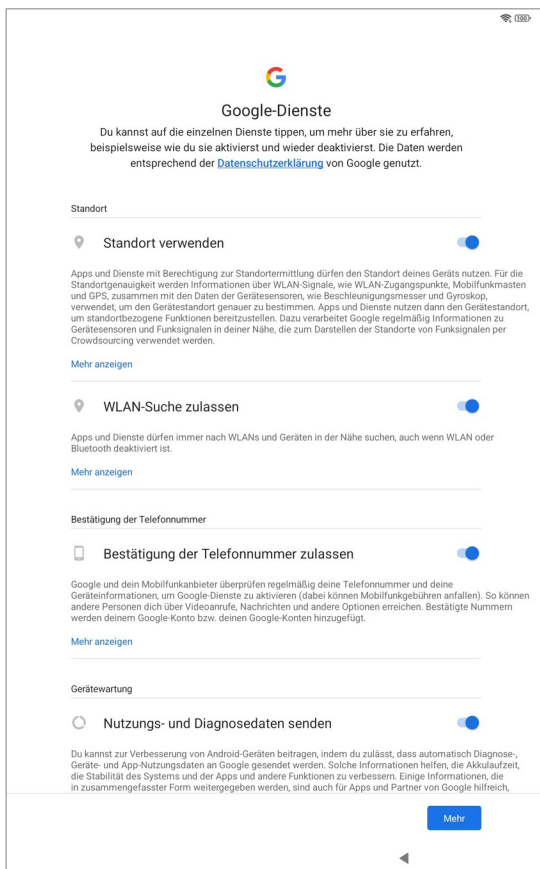
Wenn Sie nicht in einem Google-Konto angemeldet sind, können Sie Folgendes nicht tun:

-  Apps, Musik, Spiele und andere Inhalte bei Google Play herunterladen
-  Apps bei Google sichern und Google-Dienste wie Kalender und Kontakte mit dem Gerät synchronisieren
-  Schutzfunktionen für Mobilgerät aktivieren

[Zurück](#) [Überspringen](#)



Google Dienste abwählen



Google-Dienste

Du kannst auf die einzelnen Dienste tippen, um mehr über sie zu erfahren, beispielsweise wie du sie aktivierst und wieder deaktivierst. Die Daten werden entsprechend der [Datenschutzerklärung](#) von Google genutzt.

Standort

☒ Standort verwenden

Apps und Dienste mit Berechtigung zur Standortermittlung dürfen den Standort deines Geräts nutzen. Für die Standortgenauigkeit werden Informationen über WLAN-Signale, wie WLAN-Zugangspunkte, Mobilfunkmasten und GPS, zusammen mit den Daten der Gerätesensoren, wie Beschleunigungsmesser und Gyroskop, verwendet, um den Gerätestandort genauer zu bestimmen. Apps und Dienste nutzen dann den Gerätestandort, um standortbezogene Funktionen bereitzustellen. Dazu verarbeitet Google regelmäßig Informationen zu Gerätesensoren und Funksignalen in deiner Nähe, die zum Darstellen der Standorte von Funksignalen per Crowdsourcing verwendet werden.

[Mehr anzeigen](#)

WLAN-Suche zulassen

Apps und Dienste dürfen immer nach WLANs und Geräten in der Nähe suchen, auch wenn WLAN oder Bluetooth deaktiviert ist.

[Mehr anzeigen](#)

Bestätigung der Telefonnummer

☒ Bestätigung der Telefonnummer zulassen

Google und dein Mobilfunkanbieter überprüfen regelmäßig deine Telefonnummer und deine Geräteinformationen, um Google-Dienste zu aktivieren (dabei können Mobilfunkgebühren anfallen). So können andere Personen dich über Videoanrufe, Nachrichten und andere Optionen erreichen. Bestätigte Nummern werden deinem Google-Konto bzw. deinen Google-Konten hinzugefügt.

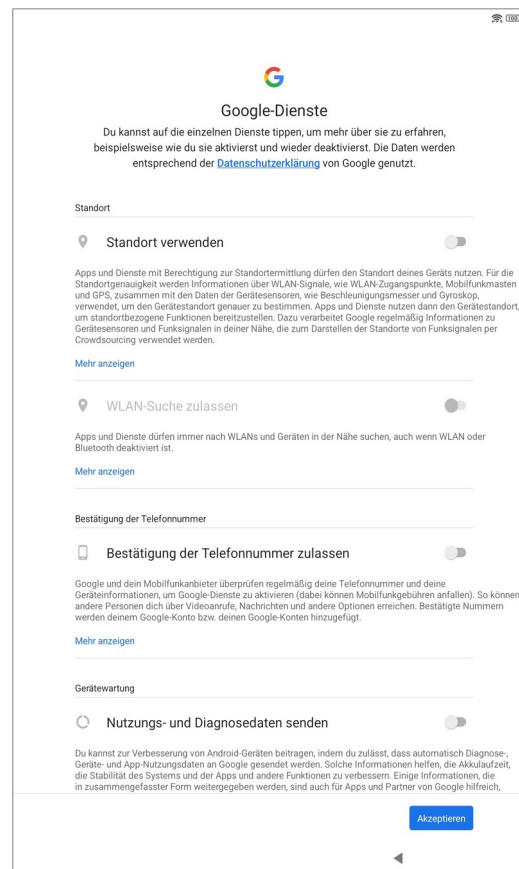
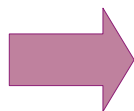
[Mehr anzeigen](#)

Gerätewartung

☒ Nutzungs- und Diagnosedaten senden

Du kannst zur Verbesserung von Android-Geräten beitragen, indem du zulässt, dass automatisch Diagnose-, Geräte- und App-Nutzungsdaten an Google gesendet werden. Solche Informationen helfen, die Akkulaufzeit, die Stabilität des Systems und der Apps und andere Funktionen zu verbessern. Einige Informationen, die in zusammengefasster Form weitergegeben werden, sind auch für Apps und Partner von Google hilfreich.

[Mehr](#)



Google-Dienste

Du kannst auf die einzelnen Dienste tippen, um mehr über sie zu erfahren, beispielsweise wie du sie aktivierst und wieder deaktivierst. Die Daten werden entsprechend der [Datenschutzerklärung](#) von Google genutzt.

Standort

☐ Standort verwenden

Apps und Dienste mit Berechtigung zur Standortermittlung dürfen den Standort deines Geräts nutzen. Für die Standortgenauigkeit werden Informationen über WLAN-Signale, wie WLAN-Zugangspunkte, Mobilfunkmasten und GPS, zusammen mit den Daten der Gerätesensoren, wie Beschleunigungsmesser und Gyroskop, verwendet, um den Gerätestandort genauer zu bestimmen. Apps und Dienste nutzen dann den Gerätestandort, um standortbezogene Funktionen bereitzustellen. Dazu verarbeitet Google regelmäßig Informationen zu Gerätesensoren und Funksignalen in deiner Nähe, die zum Darstellen der Standorte von Funksignalen per Crowdsourcing verwendet werden.

[Mehr anzeigen](#)

WLAN-Suche zulassen

Apps und Dienste dürfen immer nach WLANs und Geräten in der Nähe suchen, auch wenn WLAN oder Bluetooth deaktiviert ist.

[Mehr anzeigen](#)

Bestätigung der Telefonnummer

☐ Bestätigung der Telefonnummer zulassen

Google und dein Mobilfunkanbieter überprüfen regelmäßig deine Telefonnummer und deine Geräteinformationen, um Google-Dienste zu aktivieren (dabei können Mobilfunkgebühren anfallen). So können andere Personen dich über Videoanrufe, Nachrichten und andere Optionen erreichen. Bestätigte Nummern werden deinem Google-Konto bzw. deinen Google-Konten hinzugefügt.

[Mehr anzeigen](#)

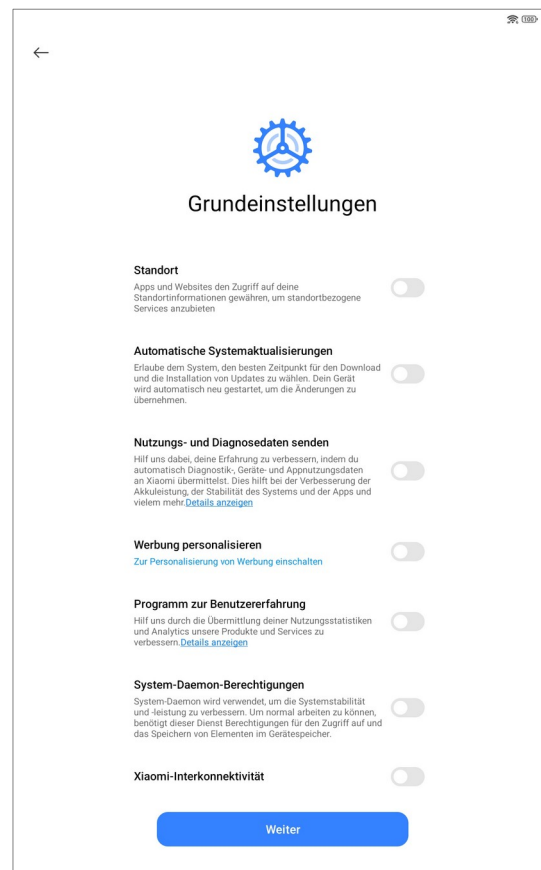
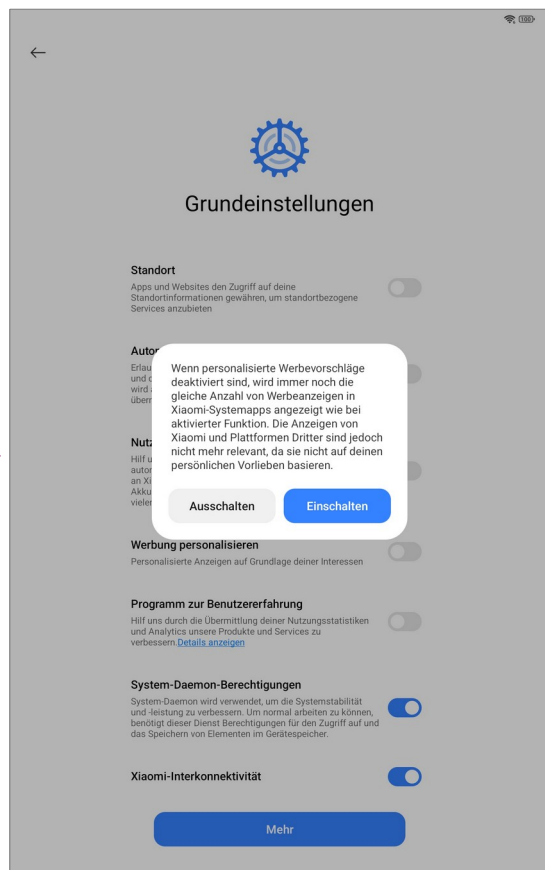
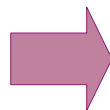
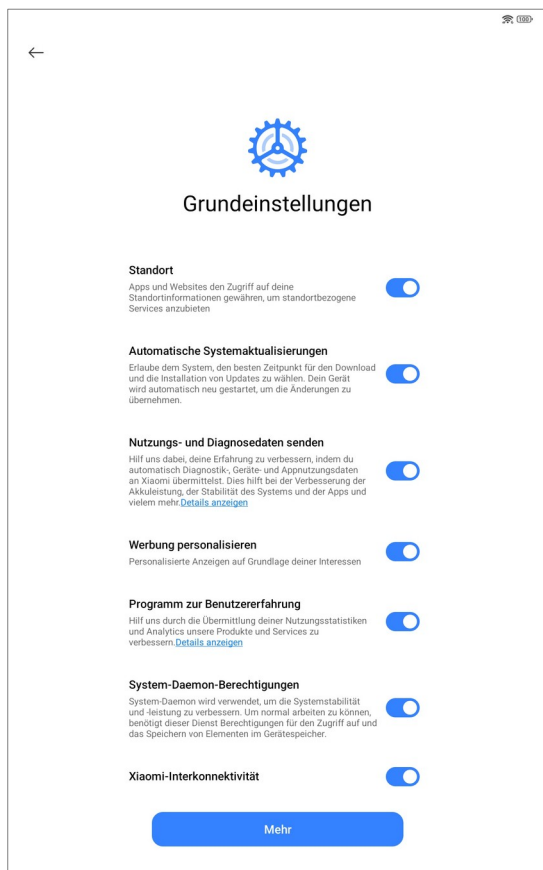
Gerätewartung

☐ Nutzungs- und Diagnosedaten senden

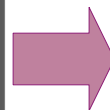
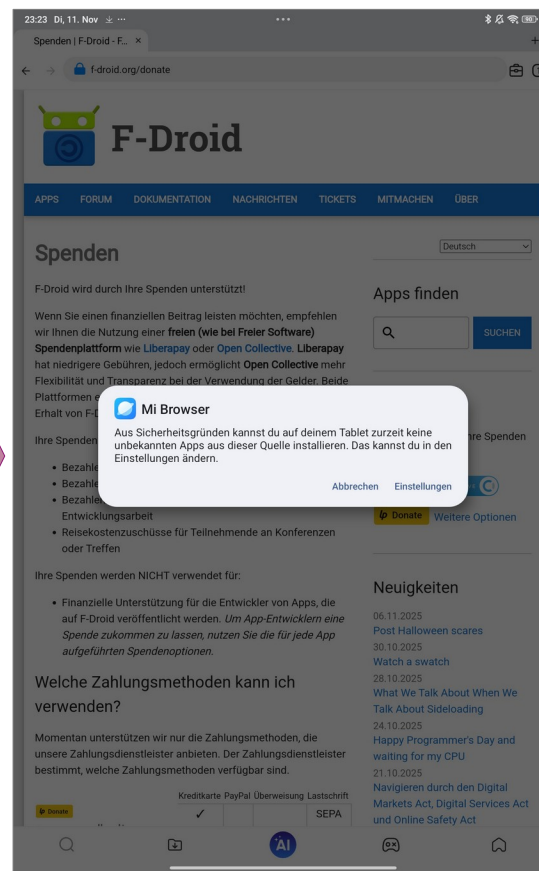
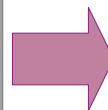
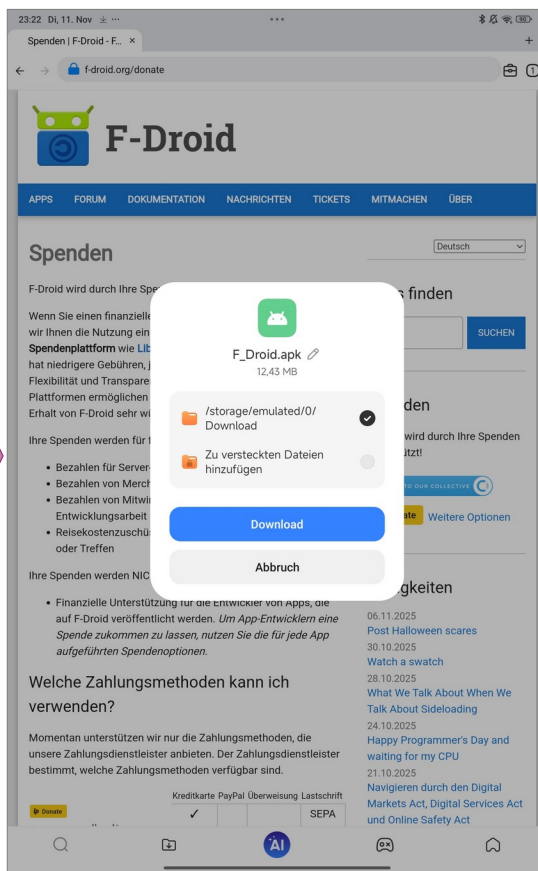
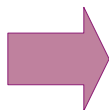
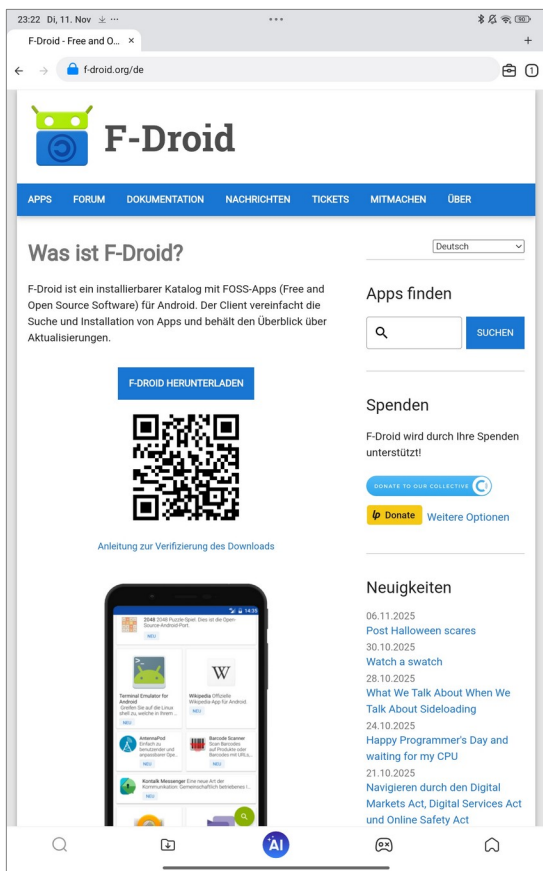
Du kannst zur Verbesserung von Android-Geräten beitragen, indem du zulässt, dass automatisch Diagnose-, Geräte- und App-Nutzungsdaten an Google gesendet werden. Solche Informationen helfen, die Akkulaufzeit, die Stabilität des Systems und der Apps und andere Funktionen zu verbessern. Einige Informationen, die in zusammengefasster Form weitergegeben werden, sind auch für Apps und Partner von Google hilfreich.

[Akzeptieren](#)

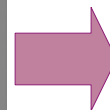
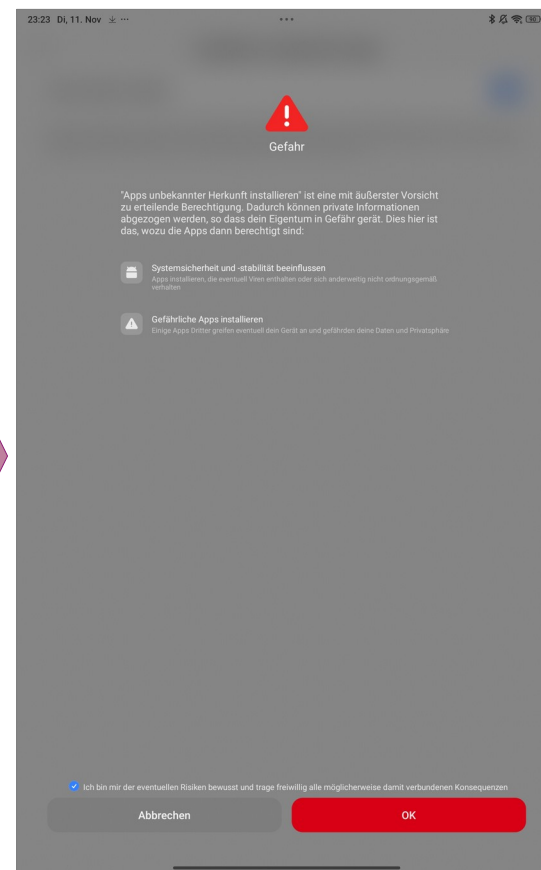
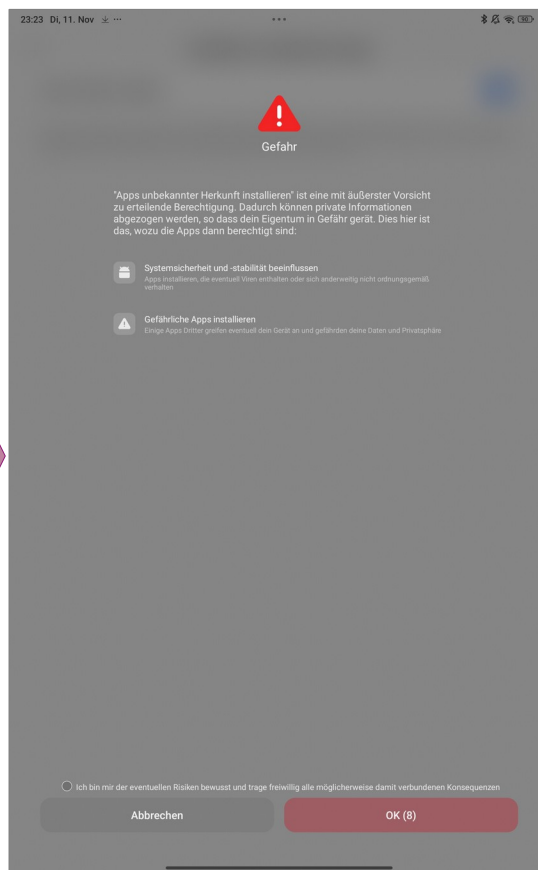
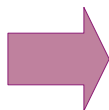
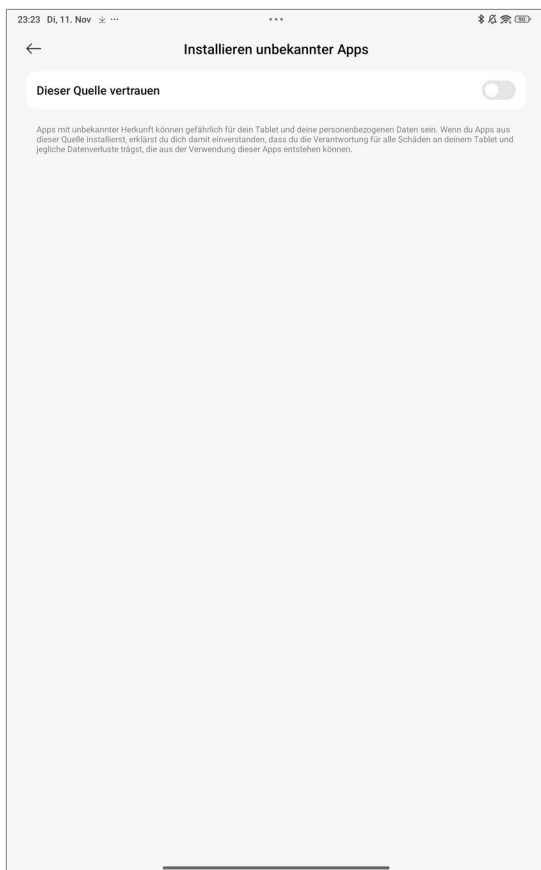
Hersteller Grundeinstellungen justieren



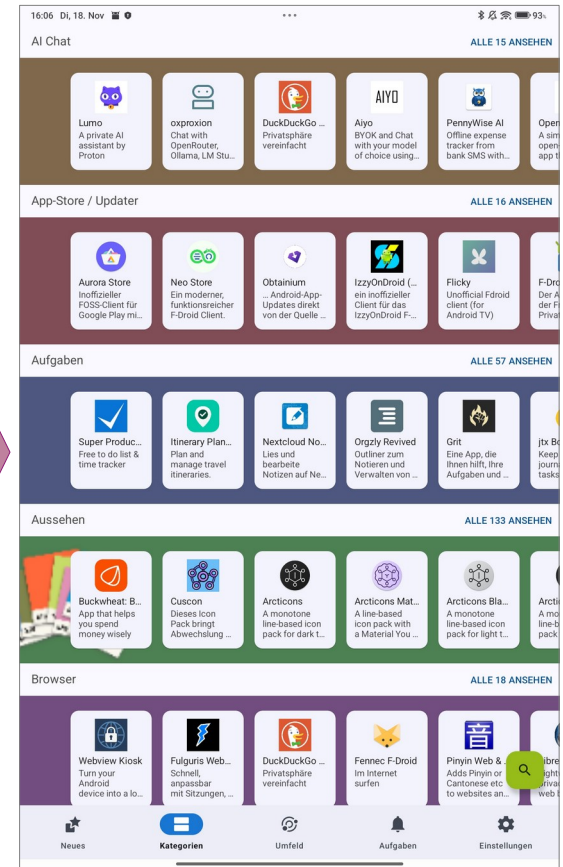
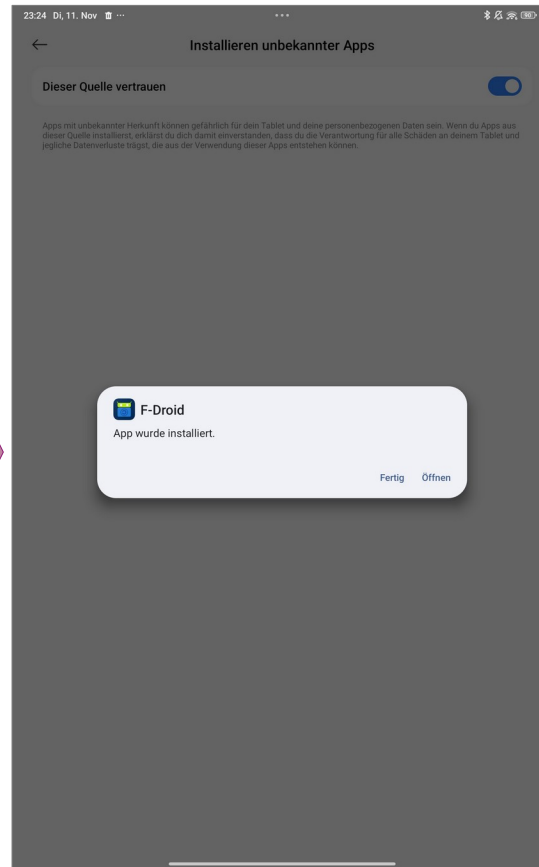
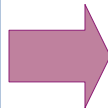
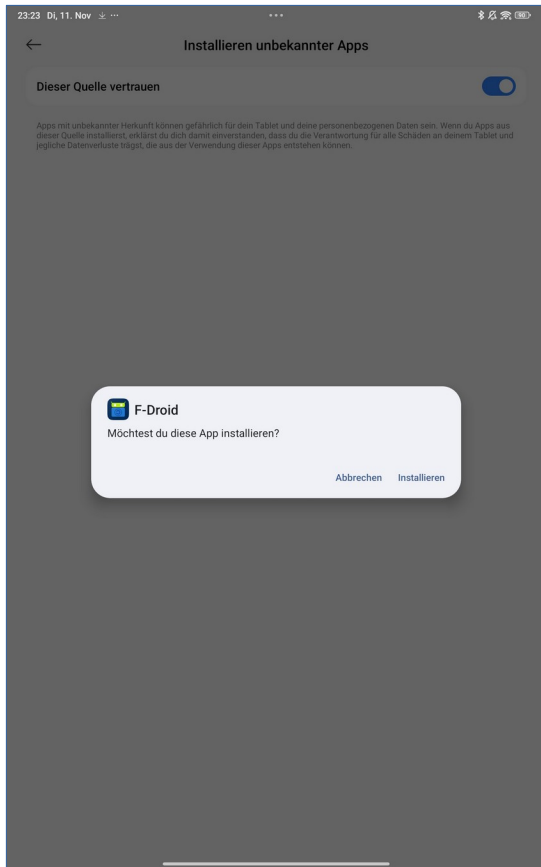
F-Droid AppStore installieren

















F-Droid AppStore installieren


















F-Droid installieren



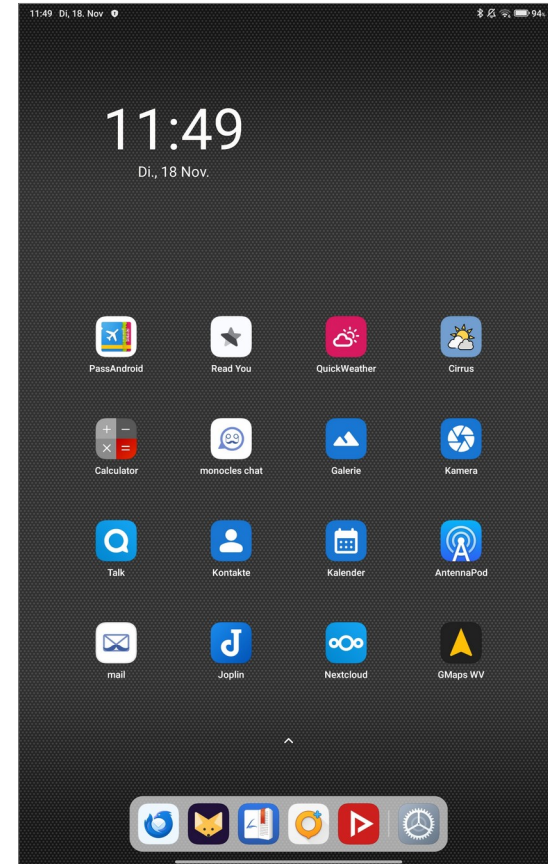
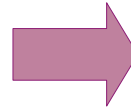
Alternative F-Droid Apps, z.B.:

 Google Chrome
 Gmail
 Google Telefon
 Google Kontakte
 Google Kalender
 Google Messages
 Google Meet
 Google Maps
 Google Photos
 Google Drive
 Google Wallet
 YouTube
 Google Playstore
 Google Play services

– Web Browser
– E-Mail Client
– Telefon
– Adressbuch
– Kalender App
– Kurznachrichten
– online Konferenzen
– Karten
– Fotoalbum
– Cloud Speicher
– Ticketspeicher
– Video Streaming
– App Store
– System services

 Fennec (Firefox)
 Thunderbird
 Fossify Phone
 Fossify Contacts
 Etar
 Fossify Messages
 Nextcloud Talk
 OsmAnd~  GMaps VM
 Fossify Gallery
 Nextcloud
 PassAndroid
 NewPipe
 F-Droid  Aurora
=> *nächste Vorträge*

Das Ergebnis: Ein datensparsames Tablet





Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

- Android geht auch datensparsam
 - ... aber man kann Google kaum vollständig vermeiden
- Custom ROMs
 - Alternative Betriebssystem-Images für Android Geräte auf AOSP-Basis
 - Mehrere Alternativen, z.B.
 - Lineage und Lineage-Derivate
 - Lineage for microG
 - /e/
 - GrapheneOS
 - Beschränkter Funktionsumfang, oder microG als Google-Alternative
 - ==> nächste Vorträge



Danke für eure Aufmerksamkeit!

Habt ihr Fragen oder Anmerkungen?