LWsystems
OPEN SOURCE IT-Lösungen

GrapheneOS vs. Android/iOS –

Datenschutz und Sicherheit im Vergleich

Zusammenstellung und Feature-Vergleich der Eigenschaften von GrapheneOS gegenüber den Smartphone-Betriebssystemen Google Android und Apple iOS

Stand: Mai 2025

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Inhaltsverzeichnis

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Haftungsausschluss

Die nachfolgende Darstellung der Features von GrapheneOS und die gegenüberstellenden Vergleiche zwischen GrapheneOS, Standard Android und iOS erhebt keinen Anspruch auf Vollständigkeit. Sie wurde in Teilen unter Zuhilfenahme des KI-Chatbots Claude von Anthropic erstellt. Die erhaltenen Informationen basieren (soweit dies bei der Nutzung des Chatbots ersichtlich war) auf öffentlich zugänglichen Quellen und wurden im Zuge der Erstellung dieser Ausarbeitung geprüft sowie teilweise redigiert und ergänzt.

Alle Informationen in diesem Handout wurden sorgfältig zusammengestellt und geprüft. Trotzdem können wir keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der Angaben übernehmen. Dies gilt insbesondere für die Inhalte externer Websites, auf die wir in diesem Handout verweisen. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

Die bereitgestellten Informationen dienen lediglich zu Informationszwecken und stellen keine rechtliche, steuerliche oder finanzielle Beratung dar. Wir empfehlen, sich bei Bedarf professionellen Rat einzuholen.

Alle Angaben erfolgen ohne Gewähr. Irrtümer und Änderungen vorbehalten.

Haftungsausschluss:

Wir haften nicht für Schäden, die durch die Nutzung oder Nichtnutzung der in diesem Handout bereitgestellten Informationen entstehen. Dies gilt sowohl für direkte als auch indirekte Schäden, einschließlich entgangener Gewinne, Datenverlust oder sonstige Folgeschäden.

Durch die Nutzung dieses Handouts erklären Sie sich mit den oben genannten Bedingungen einverstanden.

GrapheneOS vs. Android/iOS

Management Summary

GrapheneOS ist wie ein "Super-Datenschutz-Android" - es nimmt das normale Android-System und entfernt **alles**, was Daten sammeln könnte. Gleichzeitig fügt es **viele neue Schutzfunktionen** hinzu, die es bei anderen Handys **nicht** gibt.

Der große Unterschied: Während Samsung/Google und Apple persönliche Daten für Werbung und Dienste nutzen, sammelt GrapheneOS **überhaupt keine** Daten. Anwender haben außerdem **viel feinere Kontrolle** darüber, was jede App auf dem Handy darf.

Der Haken: Es ist etwas komplexer in der Handhabung und es gibt Apps (z.B. einzelne Banking-Apps, die App der Techniker Krankenkasse, ...) die nicht richtig funktionieren. GrapheneOS ist hauptsächlich für Menschen geeignet, die bereit sind, Komfort für **maximale Privatsphäre und Sicherheit** zu tauschen.

Was ist GrapheneOS?

GrapheneOS ist ein spezielles Android-Betriebssystem, das **vollständig** auf **Datenschutz und Sicherheit** ausgelegt ist. Es läuft nur auf Google Pixel-Geräten und entfernt alle Google-Dienste sowie viele andere Datensammler.

Detaillierter Feature-Vergleich

Feature/Bereich	GrapheneOS	Standard Android (z.B. Samsung)	Apple iOS
Google-Dienste	❌ Komplett entfernt	✅ Vollständig integriert	❌ Nicht vorhanden
Datensammlung durch Hersteller	❌ Keine	⚠️ Umfangreich (Samsung, Google)	⚠️ Begrenzt (Apple)
App-Berechtigungen	🔒 Sehr detailliert steuerbar	⚠️ Grundlegend steuerbar	⚠️ Grundlegend steuerbar
Netzwerk-Berechtigungen	🔒 Pro App einzeln kontrollierbar	❌ Nicht möglich	❌ Nicht möglich
Sensor-Zugriff blockieren	🔒 Mikrofon, Kamera, GPS einzeln sperrbar	❌ Nur über App-Berechtigungen	❌ Nur über App-Berechtigungen
Contact Scopes	🔒 Apps erhalten nur ausgewählte Kontakte	❌ Alle oder keine Kontakte	❌ Alle oder keine Kontakte
Storage Scopes	🔒 Apps erhalten nur aus-	❌ Zugriff auf alle Dateien	❌ Zugriff auf alle Fotos/

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Feature/Bereich	GrapheneOS	Standard Android (z.B. Samsung)	Apple iOS
	gewählte Dateien	der Kategorie	Dateien
Sandboxed Google Play	🔒 Google Play läuft ohne Systemrechte	❌ Nicht verfügbar	❌ Nicht verfügbar
Auto-Reboot	🔒 Handy startet nach Zeit ohne Entsperrung neu	❌ Nicht verfügbar	❌ Nicht verfügbar
Duress PIN/Password	🔒 Notfall-PIN löscht alle Daten des Handys	❌ Nicht verfügbar	❌ Nicht verfügbar
Encrypted DNS	🔒 Standardmäßig aktiviert	⚠️ Manuell einstellbar	⚠️ Begrenzt verfügbar
MAC-Randomisierung	🔒 Erweitert und verbessert	⚠️ Grundlegend	⚠️ Grundlegend
Exploit-Schutz	🔒 Hardened Memory Allocator	⚠️ Standard-Schutz	⚠️ Guter Schutz
Verified Boot	🔒 Erweitert und gehärtet	⚠️ Standard	✅ Sehr gut
App-Store	🔒 F-Droid, Aurora Store, optional Google Play	✅ Google Play Store	✅ Apple App Store
Updates	🔒 Monatlich, 5+ Jahre Support	⚠️ Herstellerabhängig	✅ Lange Support-Zeit
Benutzerfreundlichkeit	⚠️ Erfordert etwas Einfühlungsvermögen	✅ Sehr einfach	✅ Sehr einfach
App-Kompatibilität	⚠️ Einzelne Apps funktionieren nicht	✅ Alle Android-Apps	✅ Alle iOS-Apps
USB nach Sperre	🔒 Automatisch gesperrt	⚠️ Oft noch aktiv	🔒 Automatisch gesperrt nach 1h
ADB-Schutz	🔒 Verstärkt	🔒 Verstärkt	🔒 Kein ADB vorhanden
Bad USB Schutz	🔒 Verbessert	🔒 Begrenzt	🔒 Sehr gut (sandboxed)
Forensik-Schutz	🔒 Sehr gut	⚠️ Schwach	🔒 Sehr gut
USB-Accessories	🔒 Warnung bei neuen Geräten	⚠️ Meist ohne Warnung	🔒 "Zubehör vertrauen?" Dialog
Benutzerfreundlichkeit	⚠️ Mehr Klicks nötig	✅ Einfacher	⚠️ Sicherheitsdialoge

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Fachbegriffe erklärt

Sandboxed Google Play

Google Play läuft in einer "Sandbox" (dt. Sandkasten) – einem abgeschotteten Bereich ohne besondere Systemrechte. Dadurch kann Google nicht mehr ins System eindringen und Daten sammeln.

Contact/Storage Scopes

Anstatt einer App Zugriff auf ALLE Kontakte oder Fotos zu geben, können Sie gezielt auswählen, auf welche Kontakte oder Dateien die App zugreifen darf.

Auto–Reboot

Das Handy startet sich automatisch neu, wenn es längere Zeit nicht entsperrt wurde. Nach dem Neustart sind die Daten komplett verschlüsselt und selbst bei physischem Zugriff auf das Gerät faktisch nicht zu knacken.

Duress PIN

Ein Notfall-Code (separate PIN), den man bspw. bei Bedrohung oder Zwang zur Entsperrung des Gerätes eingeben kann. Schützt davor, dass ein Angreifer merkt, dass eine Notfall-PIN verwendet wird. Das Handy löscht direkt nach Eingabe **alle** Daten **unwiderbringlich**!

MAC–Randomisierung

Das Handy sendet normalerweise eine feste ID (MAC-Adresse) über WLAN. Mit Randomisierung wird diese ID ständig geändert, sodass Sie schwerer verfolgbar sind.

Hardened Memory Allocator

Ein verbesserter Speicherschutz, der es Hackern deutlich schwerer macht, Schadsoftware in den Arbeitsspeicher einzuschleusen.

Verified Boot

Das System prüft beim Start, ob die Software verändert wurde. GrapheneOS macht dies noch gründlicher als Standard-Android.

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

> **USB nach Sperre:** Bestimmt, ob der USB-Anschluss nach dem Sperren weiterhin Daten übertragen kann oder nur noch zum Laden funktioniert.

> **ADB–Schutz:** Android Debug Bridge ist eine Entwicklerschnittstelle, über die Computer tief auf Android-Geräte zugreifen können - ein häufiger Angriffsvektor für Hacker.

> **Bad USB Schutz:** Schutz vor USB-Sticks oder Kabeln, die sich als harmlose Geräte tarnen, aber in Wirklichkeit schädliche Befehle wie eine Tastatur eingeben.

> **Forensik–Schutz:** Schutz vor professionellen Geräten (wie Cellebrite), die Polizei und Geheimdienste verwenden, um Daten aus gesperrten Handys zu extrahieren.

> **USB–Accessories:** Behandlung von USB-Zubehör wie Tastaturen, Mäusen oder USB-Sticks, die an das Handy angeschlossen werden.

> **Benutzerfreundlichkeit:** Wie einfach oder kompliziert es für normale Nutzer ist, USB-Funktionen zu verwenden, ohne dabei die Sicherheit zu gefährden.

Sicherheitsfeatures, die Standard–Android und iOS NICHT haben

- **Contact/Storage Scopes** (siehe oben, sehr einzigartig)
- **Network Permission Toggle** (kein anderes System hat das)
- **Sensors Permission** auf dieser Detailebene
- **Profile–basierte Isolation** in dieser Tiefe
- **Hardware Security Features** so gut ausgenutzt

Diese Features machen GrapheneOS zu einem der **sichersten mobilen Betriebssysteme überhaupt**.

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Ausgewählte besondere Features von GraheneOS

- **Geschützter Bereich ohne Google:** Geschäftsdaten komplett getrennt ohne Google-Abhängigkeit
- **Stärkere Verschlüsselungsalgorithmen** als Standard-Android
- **Besserer Schutz** der Verschlüsselungsschlüssel
- **Härtung gegen Hardware–Angriffe**
- **Warnung vor gefälschten Mobilfunkmasten** (IMSI Catcher Detection)
- RAM wird **bei Sperrung teilweise überschrieben**
- Apps können **nicht heimlich Zwischenablage lesen**
- Apps können **Bildschirmaufnahmen blockieren**
- **Strenge Kontrolle** über App-Aktivitäten
- **Hardware–Disconnect Simulation:** Apps denken, Hardware ist nicht vorhanden
- **Fake Camera/Mic Data:** Apps erhalten leere/gefälschte Daten statt Blockierung

Vor– und Nachteile im Überblick

✅ Vorteile von GrapheneOS

- **Maximaler Datenschutz**: Keine Datensammlung durch Google oder andere Konzerne
- **Erweiterte Sicherheit**: Schutz vor Hackern und Malware ist deutlich besser
- **Granulare Kontrolle**: Sie bestimmen sehr genau, welche App was darf
- **Keine Werbung**: Kein Tracking für personalisierte Werbung
- **Open Source**: Der Code ist öffentlich einsehbar und prüfbar
- **Rasche Entwicklung:** GrapheneOS entwickelt sich schnell weiter
- **USB-Sicherheit:** GrapheneOS hat mehrere wichtige Sicherheitsfeatures implementiert, die über Standard-Android hinausgehen

❌ Nachteile von GrapheneOS

- **Nur für Pixel-Geräte**: Läuft ausschließlich auf Google Pixel Smartphones
- **Komplexe Installation**: Erfordert technisches Verständnis (Geräte sind vorinstalliert und „ready to run“ erhältlich)
- **App-Probleme**: bestimmte Apps funktionieren nicht oder nur eingeschränkt
- **Weniger Komfort**: Viele praktische Features von Standard-Android fehlen
- **Lernkurve**: Die Bedienung ist ggf. etwas gewöhnungsbedürftig

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

Für wen ist GrapheneOS geeignet?

✅ Geeignet für:	❌ Weniger geeignet für:
• Personen mit hohen Datenschutz-Anforderungen	• Durchschnittsnutzer ohne technische Kenntnisse
• Journalisten, Aktivisten, Anwälte	• Personen, die auf Banking-Apps angewiesen sind
• Technik-interessierte Nutzer	• Nutzer, die maximale App-Kompatibilität brauchen
• Personen, die Komfort gegen Privatsphäre tauschen möchten	• Personen, die ein "funktioniert sofort"-Erlebnis erwarten

Fazit

GrapheneOS bietet den derzeit **besten Datenschutz und die beste Sicherheit** für Smartphones, erfordert aber ggf. etwas technisches Verständnis und evtl. Kompromisse bei der Benutzerfreundlichkeit.

TIEFERER EINBLICK
für technisch Interessierte

USB

GrapheneOS bietet deutlich verbesserte USB-Sicherheit im Vergleich zu Standard-Android: Der USB-Port ist nach dem Sperren standardmäßig auf "Nur Laden" beschränkt und blockiert automatisch **jede** Datenübertragung, was vor "Bad USB"-Angriffen, Juice Jacking und forensischen Tools wie *Cellebrite* schützt. USB-Debugging ist standardmäßig deaktiviert und schwerer zu aktivieren, während der USB-Zugriff nach einer bestimmten Zeit automatisch gesperrt wird und eine Geräte-Entsperrung für neue Verbindungen erfordert. Diese Maßnahmen erschweren sowohl Gelegenheitsangriffe an öffentlichen Ladestationen als auch professionelle forensische Zugriffe erheblich, erfordern jedoch manchmal einen zusätzlichen Klick für normale Datenübertragungen.

GrapheneOS macht USB-Verbindungen deutlich sicherer, erfordert aber manchmal einen zusätzlichen Klick mehr für normale Nutzung. Der Sicherheitsgewinn ist aber erheblich, besonders gegen professionelle Angriffe.

Verschlüsselung bei GrapheneOS nach dem Neustart

Nach dem Neustart des Gerätes sind alle Daten verschlüsselt. Es gibt verschiedene "Verschlüsselungsebenen":

Before First Unlock (BFU) = Maximale Sicherheit

Nach dem Neustart, bevor das erste Mal die PIN eingeben wurde:

- ✅ **Alle Daten sind vollständig verschlüsselt**
- ✅ **Schlüssel sind nur im Arbeitsspeicher, nicht dauerhaft verfügbar**
- ✅ **Selbst bei physischem Zugriff sind Daten praktisch unknackbar**
- ✅ **Apps können NICHT auf ihre Daten zugreifen**

After First Unlock (AFU) = Reduzierte Sicherheit

Nachdem das Gerät das erste Mal nach dem Neustart entsperrt wurde:

- ⚠️ **Daten bleiben verschlüsselt, aber Schlüssel sind im Speicher**
- ⚠️ **Apps können auf Daten zugreifen, auch wenn das Handy gesperrt ist**
- ⚠️ **Bei forensischen Angriffen sind manche Daten zugänglich**

GrapheneOS vs. Android/iOS -

Datenschutz und Sicherheit im Vergleich

GrapheneOS Besonderheiten

Auto–Reboot Feature

- Startet das Handy automatisch neu nach X Stunden ohne Entsperrung
- **Zwingt zurück in den BFU–Zustand** (maximale Verschlüsselung)
- Macht forensische Angriffe deutlich schwieriger

Verbesserte Verschlüsselung

- Stärkere Verschlüsselungsalgorithmen als Standard-Android
- Besserer Schutz der Verschlüsselungsschlüssel
- Härtung gegen Hardware-Angriffe

Praktisches Beispiel

Szenario: Polizei beschlagnahmt das Handy

Standard–Android (nach Entsperrung):

- Viele Daten sind mit speziellen Tools auslesbar
- Apps haben oft bereits auf Daten zugegriffen

GrapheneOS mit Auto–Reboot:

- Handy startet sich automatisch neu → BFU-Zustand
- Daten sind praktisch unknackbar
- Selbst mit teuren forensischen Tools sehr schwer zu knacken

Weitere wichtige GrapheneOS Features:

User Profiles (Erweitert)

- **Vollständig isolierte Benutzerprofile** - wie separate Handys in einem Gerät
- **Work Profile ohne Google:** Geschäftsdaten komplett getrennt ohne Google-Abhängigkeit
- **Profile können komplett "unsichtbar" gemacht werden**

Network Security

- **Captive Portal Detection ohne Google:** Funktioniert ohne Google-Server
- **Enhanced DNS over HTTPS/TLS:** Bessere DNS-Verschlüsselung als Standard
- **Network Time Protocol (NTP) gehärtet:** Verhindert Zeit-basierte Angriffe

Hardware Security

- **Titan M Chip Nutzung:** Bessere Ausnutzung des Google Pixel Sicherheitschips
- **Hardware–backed Keystore erweitert:** Kryptographische Schlüssel besser geschützt

- **Rollback Protection:** Verhindert Downgrade auf unsichere Versionen

Memory Protection

- **Kernel ASLR verbessert:** Arbeitsspeicher-Layout wird zufällig verändert
- **Stack Canaries:** Schutz vor Pufferüberläufen
- **Control Flow Integrity:** Verhindert Code-Injection-Angriffe

Camera & Microphone

- **Hardware-Disconnect Simulation:** Apps denken, Hardware ist nicht vorhanden
- **Fake Camera/Mic Data:** Apps erhalten leere/gefälschte Daten statt Blockierung
- **Per-App Sensor-Blocking:** Sehr granular steuerbar

Cellular Security

- **Baseband Isolation verbessert:** Mobilfunk-Chip besser vom System getrennt
- **IMSI Catcher Detection:** Warnung vor gefälschten Mobilfunkmasten
- **Cellular Data per App:** Mobilfunk-Zugriff pro App steuerbar

App Sandbox Improvements

- **SELinux Policies gehärtet:** Strengere App-Isolation
- **Seccomp-BPF Filter:** Apps haben weniger Systemzugriff
- **Namespace Isolation:** Apps sind stärker voneinander getrennt

Bluetooth Security

- **MAC Address Randomization erweitert:** Besserer Bluetooth-Tracking-Schutz
- **Pairing-Schutz:** Strengere Bluetooth-Verbindungsregeln
- **Audio-Codec Hardening:** Schutz vor Bluetooth-Audio-Exploits

File System Protection

- **F2FS Encryption erweitert:** Bessere Dateisystem-Verschlüsselung
- **Metadata Encryption:** Auch Datei-Informationen verschlüsselt
- **Secure Deletion:** Dateien werden sicher überschrieben

Weniger bekannte, aber wichtige Features

Anti-Forensics

- **Memory Scrambling:** RAM wird bei Sperrung teilweise überschrieben
- **Cold Boot Attack Protection:** Schutz vor RAM-Auslesungen
- **DMA Attack Prevention:** Schutz vor direkten Speicherzugriffen

Timing Attack Prevention

- **Login Timing Normalization:** Gleiche Antwortzeiten bei richtig/falsch

- **Network Timing Obfuscation:** Erschwert Traffic-Analyse

Advanced Permissions

- **Clipboard Access Control:** Apps können nicht heimlich Zwischenablage lesen
- **Screenshot Protection per App:** Apps können Bildschirmaufnahmen blockieren
- **Background Activity Restrictions:** Strengere Kontrolle über App-Aktivitäten

Fazit Verschlüsselung

GrapheneOS bietet **deutlich besseren Verschlüsselungsschutz** als Standard-Android, besonders durch:

- Automatischen Neustart (Auto-Reboot)
- Verbesserte Verschlüsselungsimplementierung
- Längere Verweildauer im sicheren BFU-Zustand