Digitale Senioren Weimar

Meine Daten im Internet

Vorteile nutzen, Gefahren erkennen

Welche Daten werden erfasst

System- und Geräte-Telemetry

Daten	Warum sie erhoben werden	Wo sie hinfließen
Geräte-ID (IMEI, Seriennummer, Android-ID / iOS-Identifier)	Geräte-Authentifizierung, Netzwerk-optimierung, Fehlersuche	Hersteller (Google, Apple), Mobilfunk-Operator, ggf. Dritt-App-Entwickler (wenn sie SDKs einbinden)
Betriebssystem-Version, Patch-Level	Sicherheitspatches, Update-Management	Hersteller-Server (Google Play Services, Apple Update-Server)
Hardware-Status (CPU-Auslastung, Speicher-Nutzung, Batteriezustand)	Performance-Optimierung, Energie-Management	Hersteller-Analytics (z. B. Google Analytics for Firebase, Apple Analytics)
Crash-Reports (Stack-Trace, Log-Dateien)	Fehlerbehebung	Entwickler-Console (Firebase Crashlytics, Apple Bug Reporter)

Welche Daten werden erfasst

Standort- und Bewegungsdaten

Daten	*Zweck*	*Empfänger*
GPS-Koordinaten, WLAN-/Bluetooth-Beacons, Zell-Towers	Karten- und Navigationsdienste, ortsbasierte Werbung, Notfalldienste	Karten-Apps (Google Maps, Apple Maps), Werbenetzwerke, Behörden (im Notfall)
Bewegungs-/Aktivitäts-Erkennung (Schritte, Gesten)	Fitness-Tracking, Kontext-aware-Features	Gesundheits-Apps (Google Fit, Apple Health), Dritt-Apps (z. B. Strava)

App-Zugriff - Diese Daten muss man ggf. für Apps bei der Installation oder Benutzung freigeben. Oder ggf. später den Zugriff wieder entziehen

! Tipp ! → Wenn notwendig nur bei Verwendung der App freigeben!

Welche Daten werden erfasst

Kommunikations- und Interaktionsdaten

Daten	Nutzung	Empfänger
Anrufe, SMS/MMS-Metadaten (Zeit, Dauer, Nummer)	Anruf-Protokoll, Spam-Erkennung	Telefon-App-Hersteller, ggf. Cloud-Backup-Dienste
E-Mails, Chat-Nachrichten (Inhalt, Metadaten)	Messaging-Funktionen	Anbieter der jeweiligen Dienste (Gmail, WhatsApp, Signal etc.) – Ende-zu-Ende-verschlüsselte Dienste speichern nur minimale Metadaten
Mikrofon- und Kamera-Zugriffe (Audio-/Video-Aufnahmen)	Sprach- und Video-Calls, Bild-Analyse	Apps, die Zugriff erhalten (z. B. Zoom, Instagram) – Daten werden meist an deren Server gesendet, wenn Sie die Aufnahme teilen oder streamen

Welche Daten werden erfasst

App-bezogene Daten (Permissions)

Typ	Beispiele	Wo sie landen
Kontakte & Kalender	Namen, Telefonnummern, Termine	Cloud-Synchronisation (Google Contacts, iCloud), Dritt-Apps (z. B. CRM-Tools)
Fotos & Medien	Bilder, Videos, Audio-Dateien	Cloud-Backup (Google Photos, iCloud), soziale Netzwerke (Facebook, Instagram)
Dateisystem-Zugriff	Dokumente, Downloads	App-interner Server (z. B. Cloud-Speicher-Apps)
Sensor-Daten (Beschleunigungsmesser, Gyroskop, Magnetometer)	Spiele, AR-Funktionen, Gestensteuerung	App-Server, Analyse-SDKs (z. B. Unity Analytics)

Welche Daten werden erfasst

Netzwerk- und Nutzungsdaten

Daten	Zweck	Empfänger
IP-Adresse, MAC-Adresse	Netzwerk-Routing, Geoblocking	ISP, Wi-Fi-Router, Cloud-Dienste
App-Nutzungsstatistiken (Öffnungs-/Schließ-Zeit, Klick-Pfad)	Produkt-Verbesserung, personalisierte Werbung	App-Entwickler, Analyse-Plattformen (Firebase, Mixpanel)
Such- und Browsing-Verlauf (innerhalb von Apps)	Autovervollständigung, Empfehlungen	Such-Engine-Provider (Google, Bing), In-App-Browser

Nutzen & Vorteile

- Systemdaten werden genutzt um Updates (Sicherheit, Nutzbarkeit) anzustoßen → erhöht die Sicherheit auf Deinem Smartphone

- Nutzungsdaten und Nutzerdaten (Wohnort, Alter, Familie, Beruf, Hobbies) werden genutzt um personalisierte Werbung und Angebote zu schalten

- Kommunikation / Vernetzung → einfache schnelle Kommunikation mit Familie und Freunden

- Navigation über Google-Maps oder andere Apps

- Standortdaten teilen - „Mein Gerät finden“ (Google) oder „Wo ist“ (Apple) → falls Gerät verloren oder verlegt wurde einfache Lokalisierung und ggf. Deaktivierung → zweites Gerät (Laptop, Smartphone, Tablet) notwendig

- Automatisches Ausfüllen von Adressdaten in Online-Diensten

Gefahren & Risiken

- Persönliche Daten werden weitergegeben um Phishing oder Betrugsangriffe durchzuführen
- Identitätsdiebstahl um in meinem Namen Onlinetransaktionen durchzuführen (Einkaufen, Buchungen, Geldtransfer, …)
- Cyberangriff auf meine Geräte zu Betrugszwecken oder Erpressungen
- Personenprofil erstellen um entsprechend meinen persönlichen Vorlieben oder Interessen unseriöse oder betrügerische Angebote oder falsche Informationen (Fake News) zu senden
- Mein Gerät benutzen um betrügerische Aktionen durchzuführen

!! Wichtig !! **Auch die Daten von Familie und Freunden auf meinem Gerät sind zu schützen!**
Auch Fotos sind persönliche Daten!!

Schutz meiner Daten, was kann ich tun (1/2)

- Datenschutzeinstellungen im Google- oder Apple-Konto anpassen
- Keine sensible Kommunikation (Online-Shopping, Online-Banking, Krankenkasse, Behörden, …) in öffentlichen Netzwerken durchführen
- Wenn möglich Zwei-Faktor-Authentifizierung (2FA) für Online-Dienste und Apps verwenden
- Starke Passwörter verwenden (mindestens 8 Zeichen, keine Wörter, Sonderzeichen, Zahlen, Groß- und Kleinschreibung,…)
- Passwörter nicht auf Zettel notieren (Passwortmanager verwenden)
- Weitergabe von persönlichen Daten nur an vertrauenswürdige Dritte
- Software-Updates regelmäßig durchführen (am besten automatische Updates zulassen)

Schutz meiner Daten, was kann ich tun (2/2)

- Keine Zugangsdaten telefonisch weitergeben
- Vorsicht bei Direktlinks in E-Mails, immer den offiziellen Zugang zu behördlichen oder Bankportalen verwenden (Gefahr von Spoofing-Seiten)
- Kein E-Mail Anhänge von unbekannten Absender öffnen (Gefahr von Viren, Malware, Trojanern,…)
- Sensible Daten in der Cloud verschlüsseln (z.B. Cryptomator, AxCrypt, …)
- Suchmaschine wechseln (z.B. Ecosia, DuckDuckGo, …)

Erste Schritte zum Schutz meiner Daten

Mein Google-Konto:

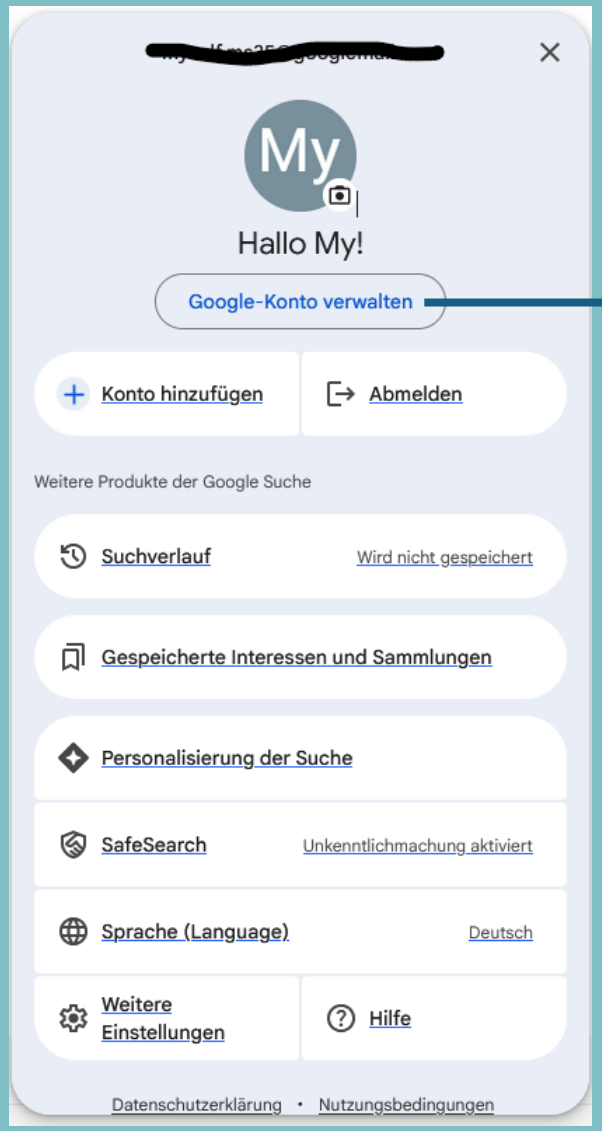
- Kontoeinstellungen Durchgehen:
  - Sind alle Daten OK
  - **Datenschutzpersonalisieren**

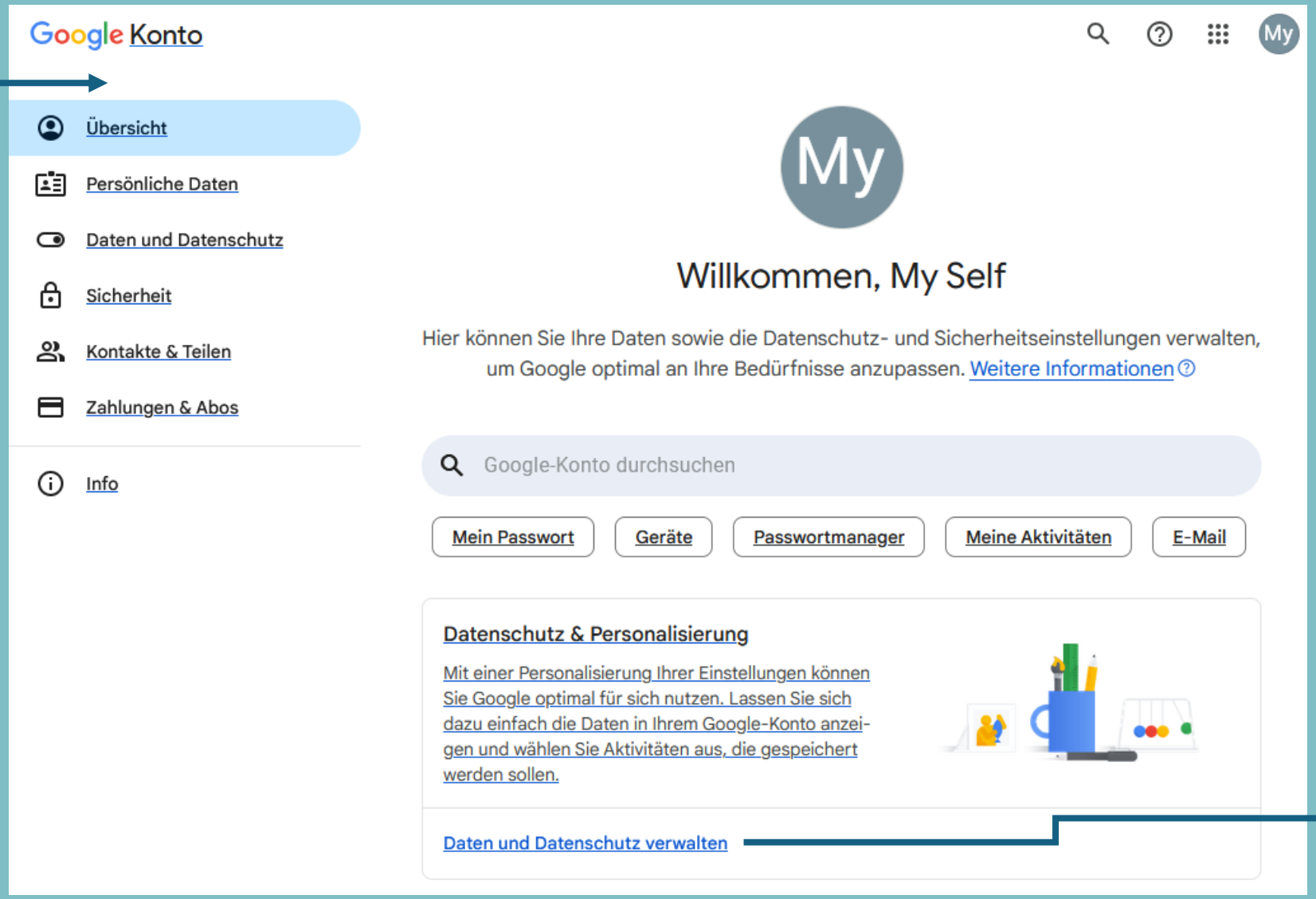
  → **Persönliche Daten müssen nicht der Wahrheit entsprechen (Name, Alter, Geschlecht, …)**

Surfen im Internet:

- Alternativen zum Chrome Browser (Firefox, Opera, Microsoft Edge, Brave, …)
- In öffentlichen Netzen (z.B. Caffè) keine sensiblen Daten austauschen (z.B. Online-Banking) oder VPN verwenden
- Nicht jeden Link in e-mails oder anderen Nachrichten (z.B. WatsApp) anlklicken, vorher genau ansehen
- Cookies immer Ablehnen („Nur notwendige erlauben“)
- Immer misstrauisch sein und gesunden Menschenverstand verwenden

Google-Konto - Datenschutzeinstellungen





Google-Konto - Datenschutzeinstellungen

Daten und Datenschutz

Wichtige Datenschutzeinstellungen, mit denen Sie festlegen können, welche Daten in Ihrem Konto gespeichert werden, welche Werbung Ihnen angezeigt wird, welche Informationen Sie mit anderen teilen und vieles mehr

Datenschutz-Tipps verfügbar

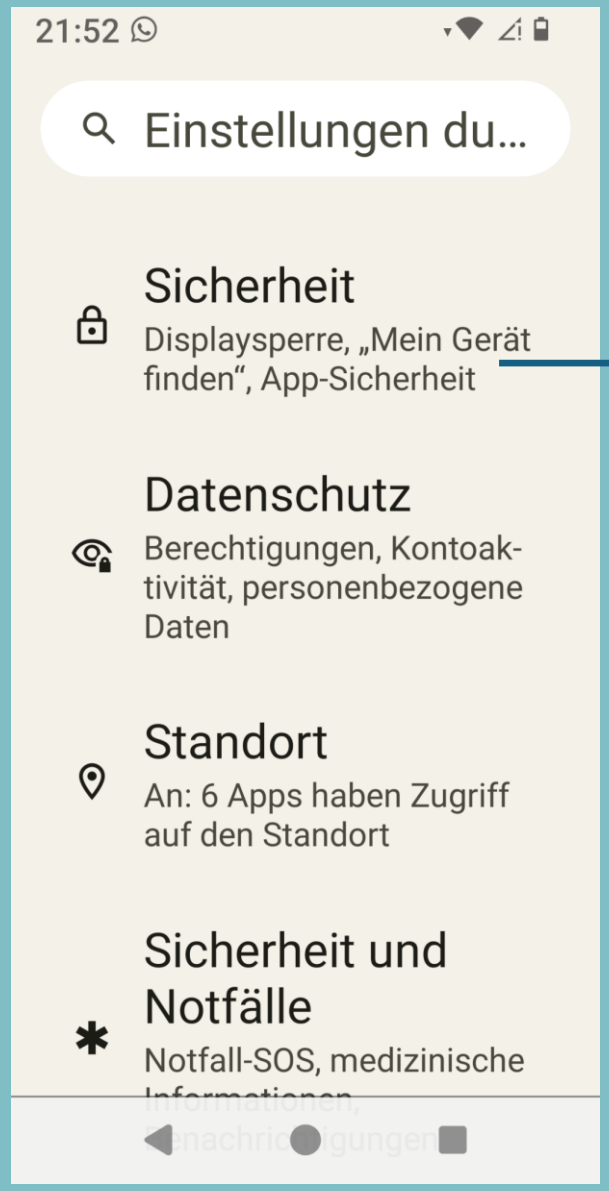
Nutzen Sie den Privatsphärecheck und wählen Sie die Einstellungen aus, die zu Ihren Anforderungen passen

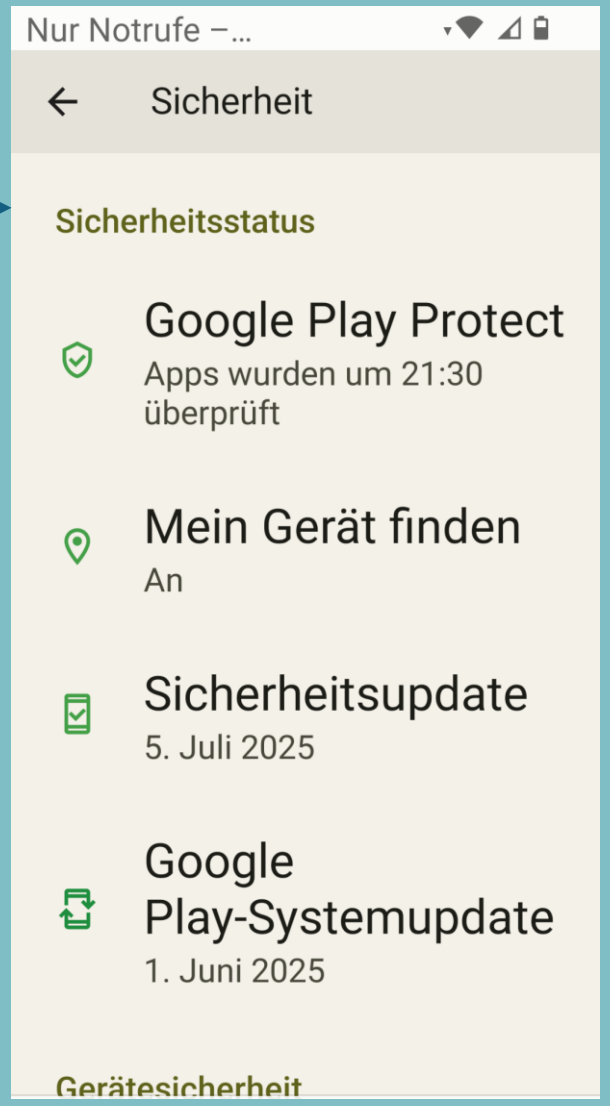
Vorschläge prüfen (2)

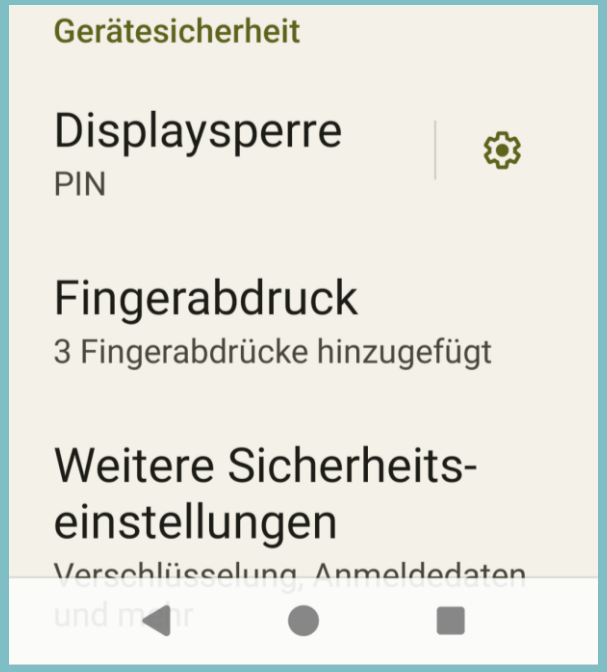
Optionen für Daten und Datenschutz

- Aktivitäten und besuchte Orte
- Informationen, die Sie mit anderen teilen können
- Daten aus Apps und Diensten, die Sie nutzen
- Weitere Optionen

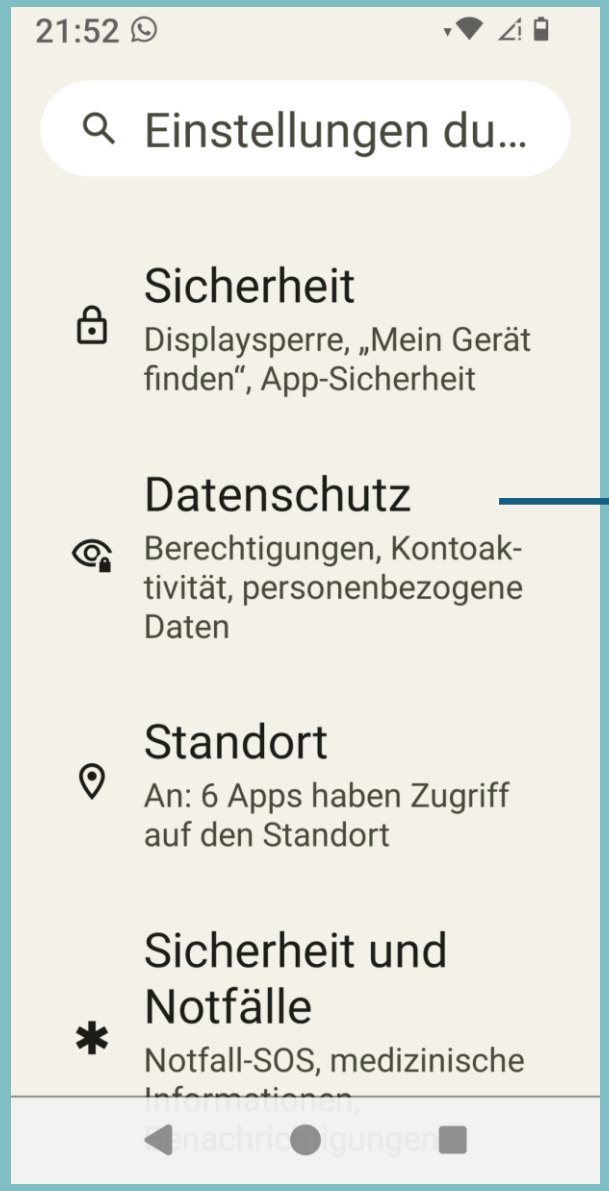
Android - Einstellungen

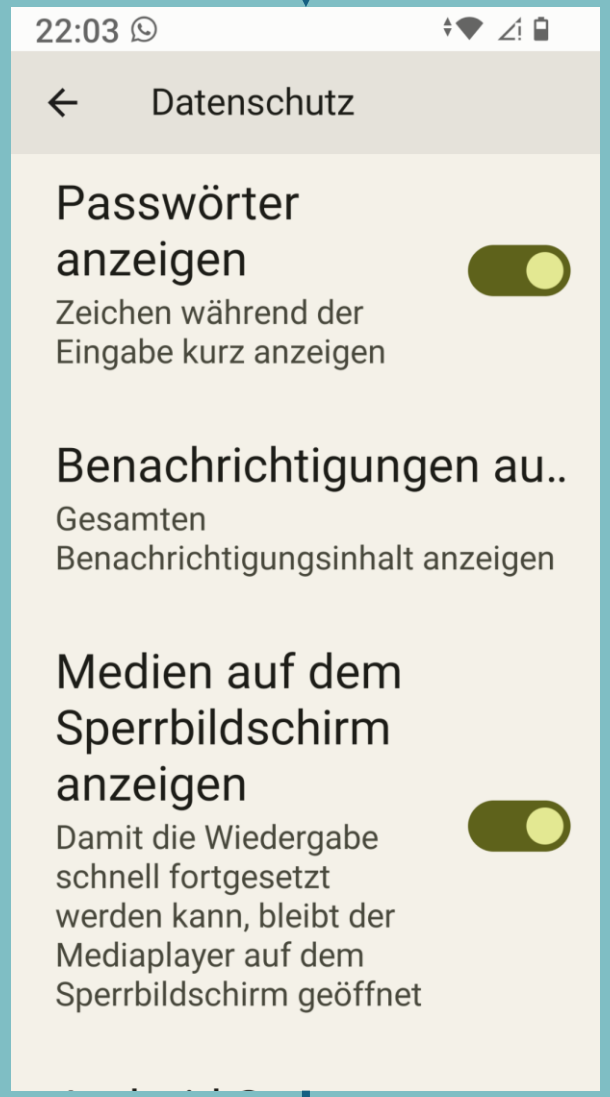




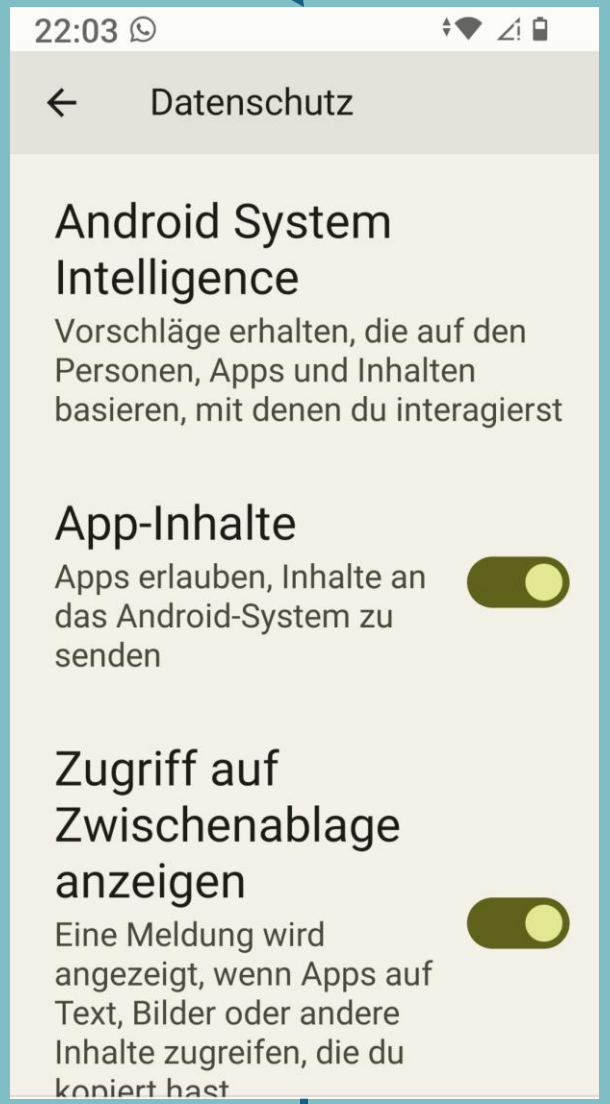


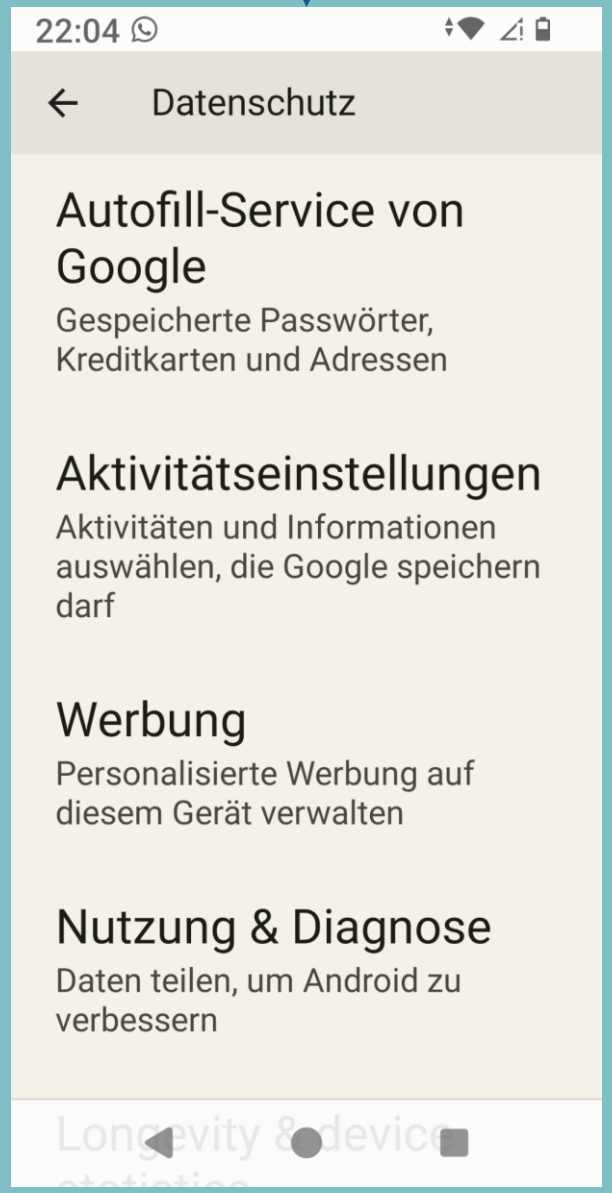
Android - Einstellungen





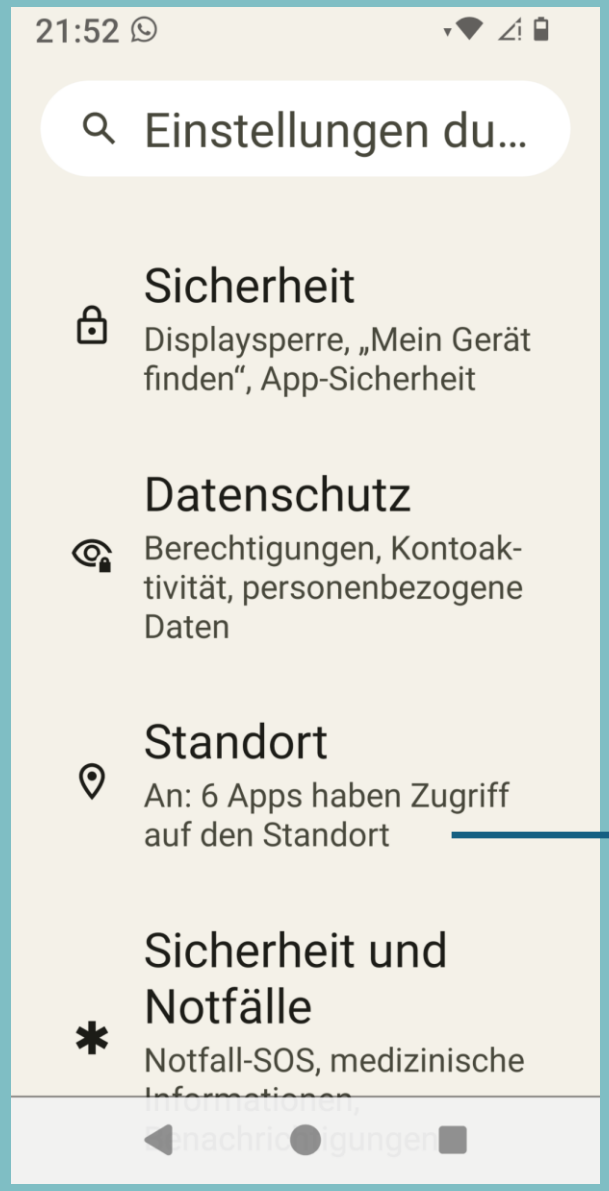
Android - Einstellungen

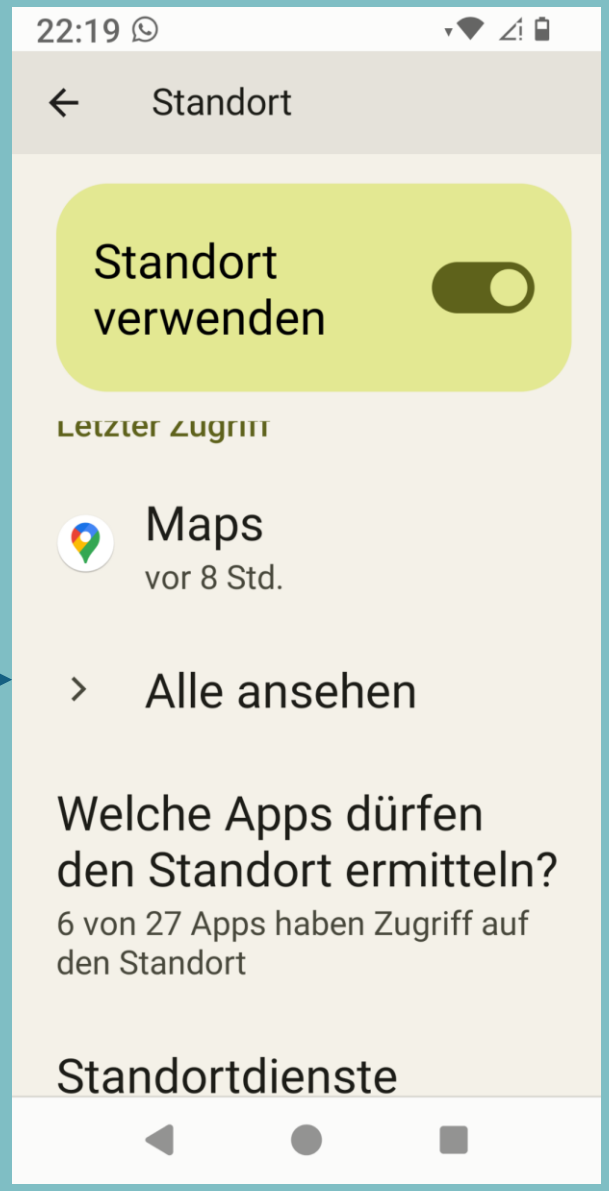




Jeder einzelne Punkt sollte individuell angepasste werden!

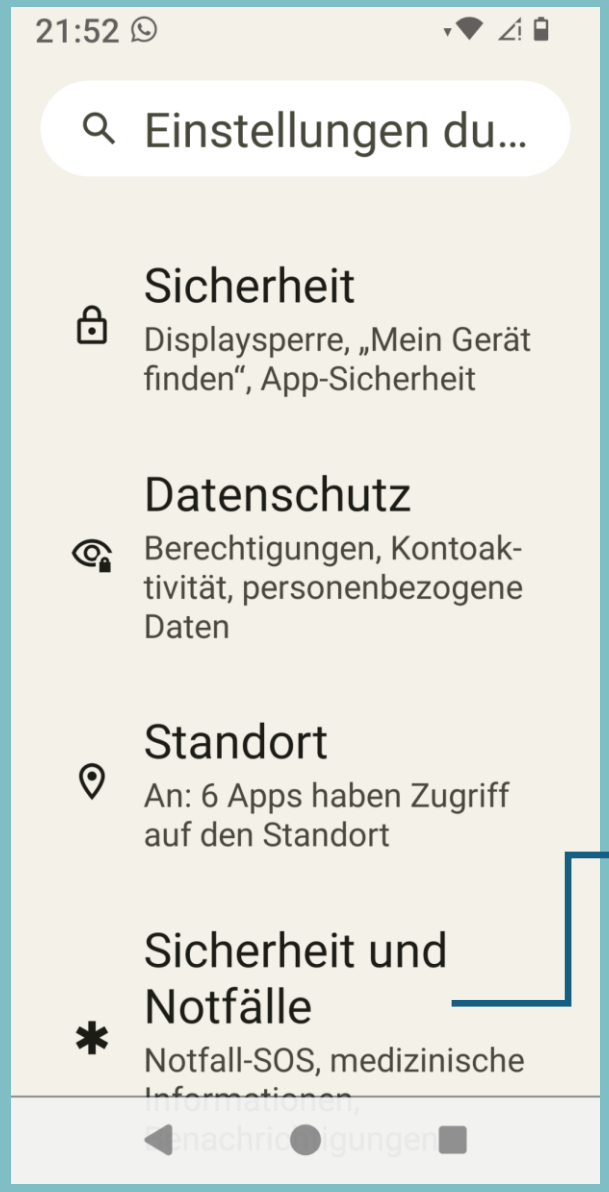
Android - Einstellungen

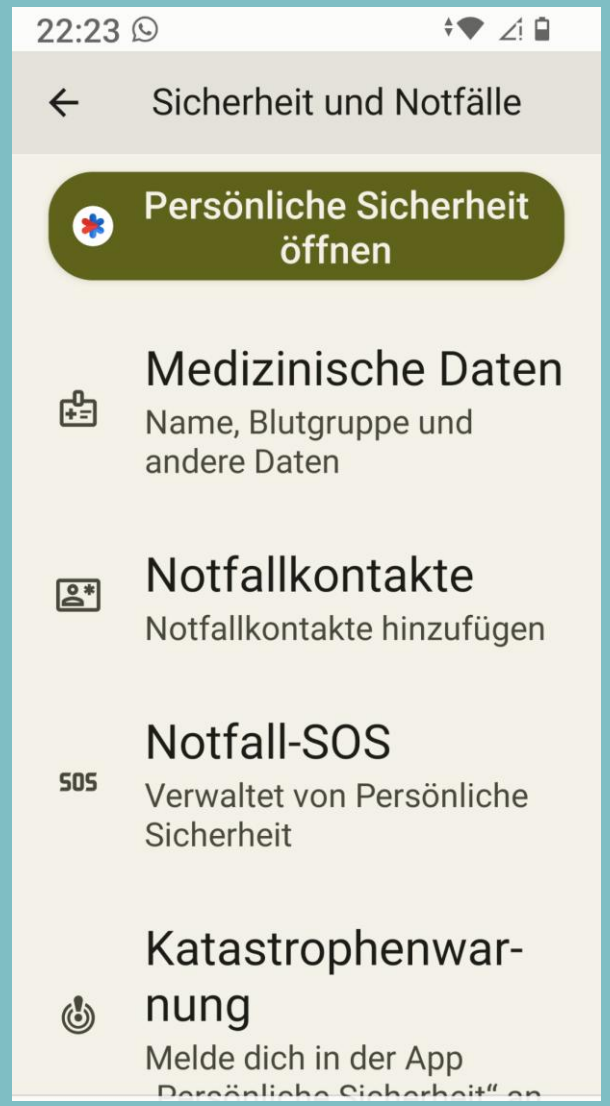


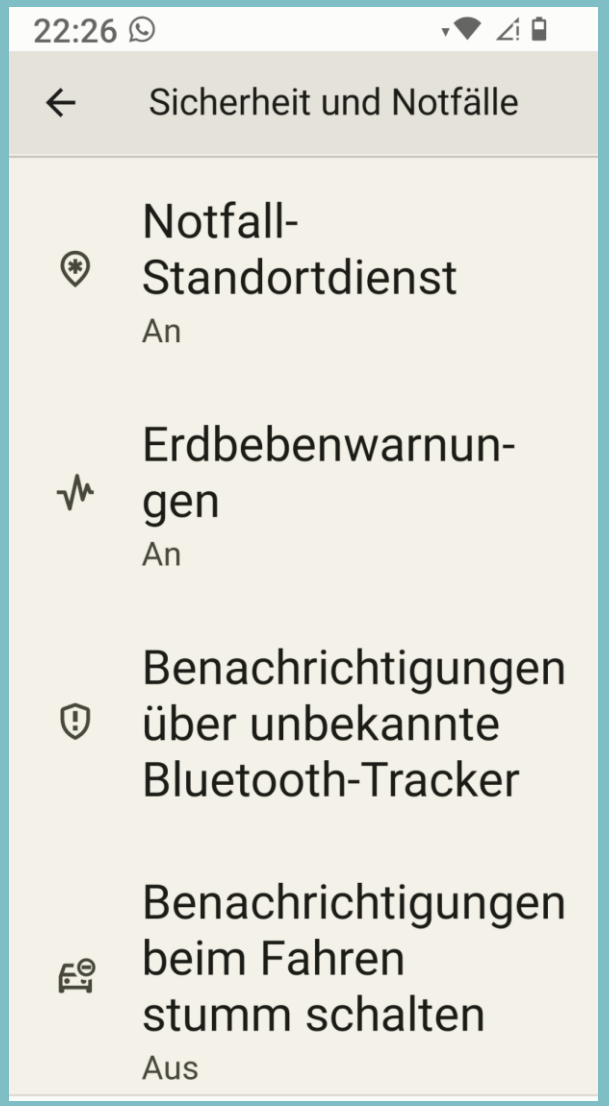


Überprüfen welche Apps Zugriff auf meine Standortdaten haben und für die zulassen die diese wirklich benötigen. (z.B. Maps)

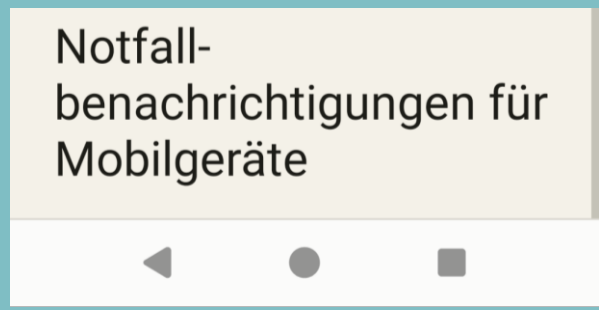
Android - Einstellungen



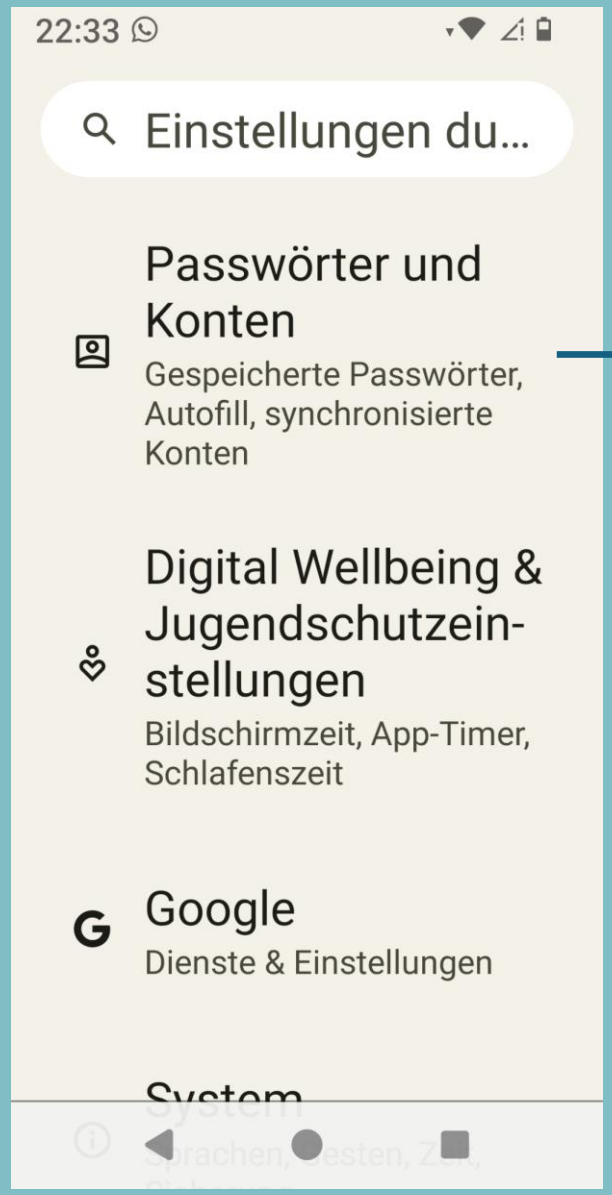


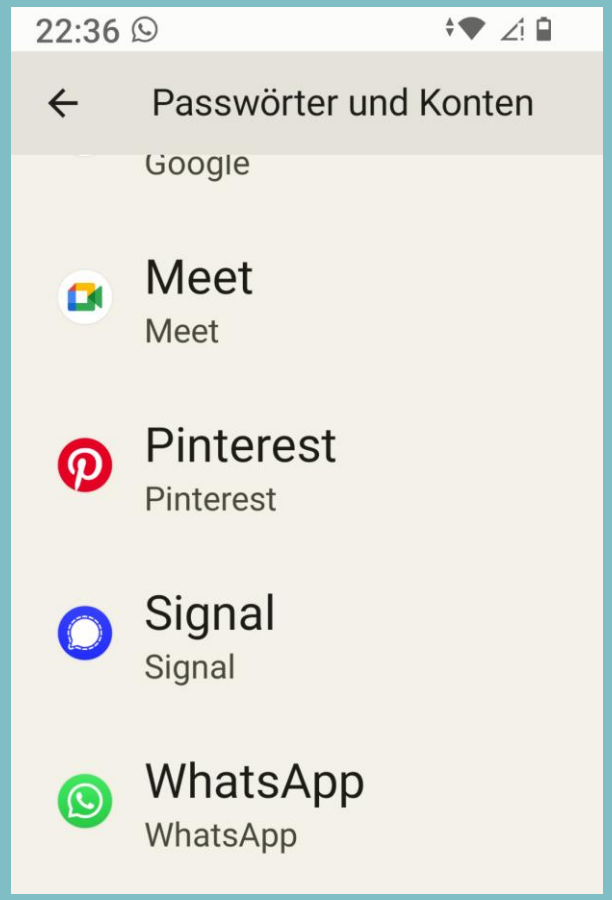


Überprüfen welche Daten Du preisgeben willst mit welchem Nutzen.



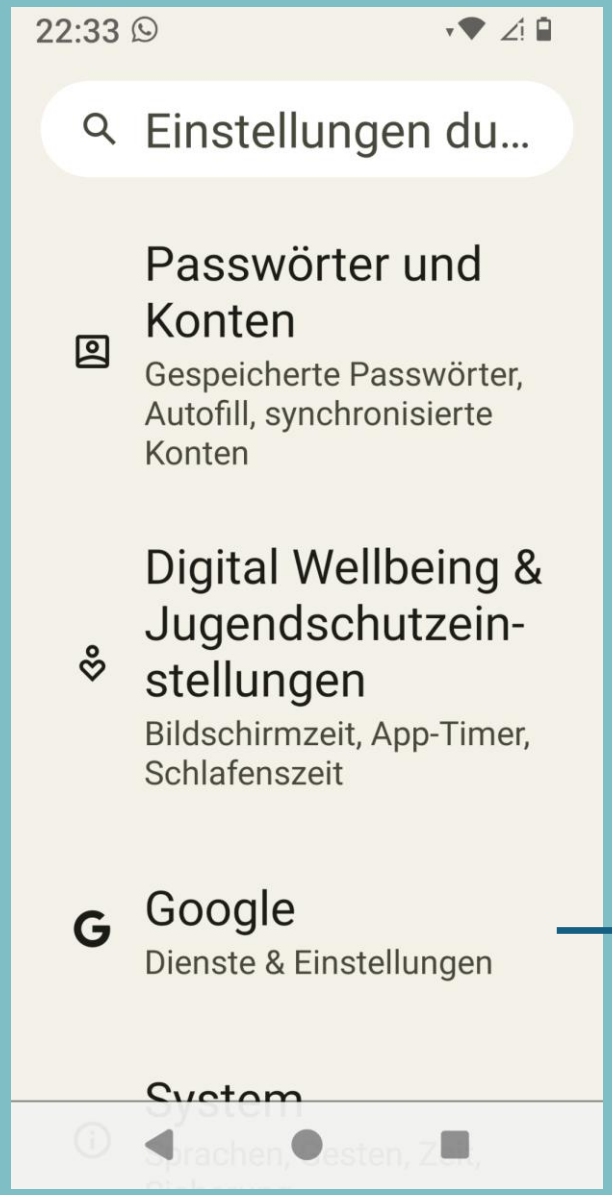
Android - Einstellungen

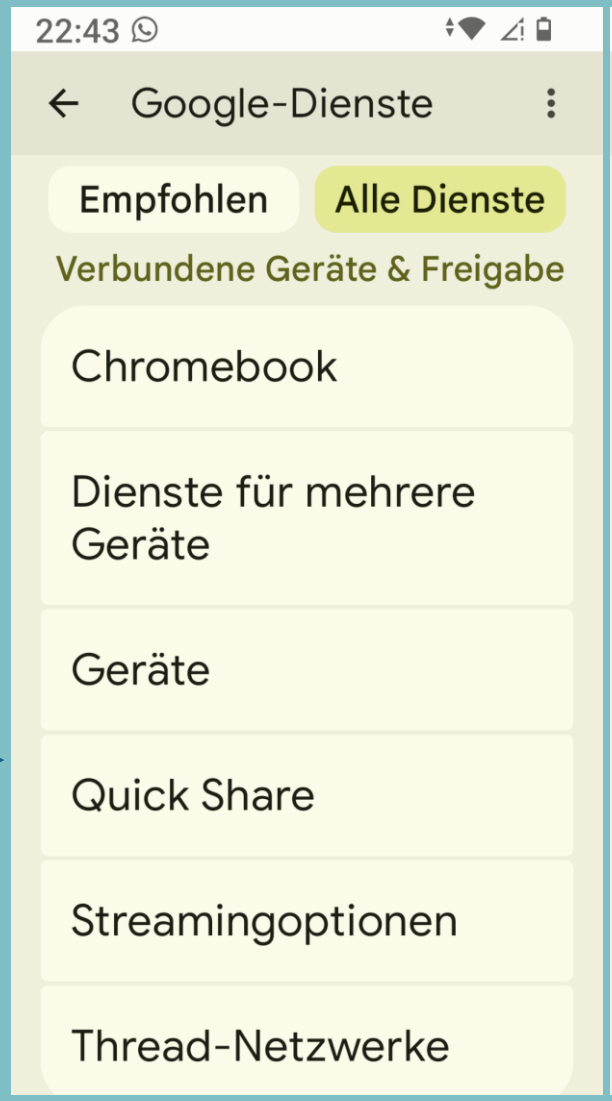


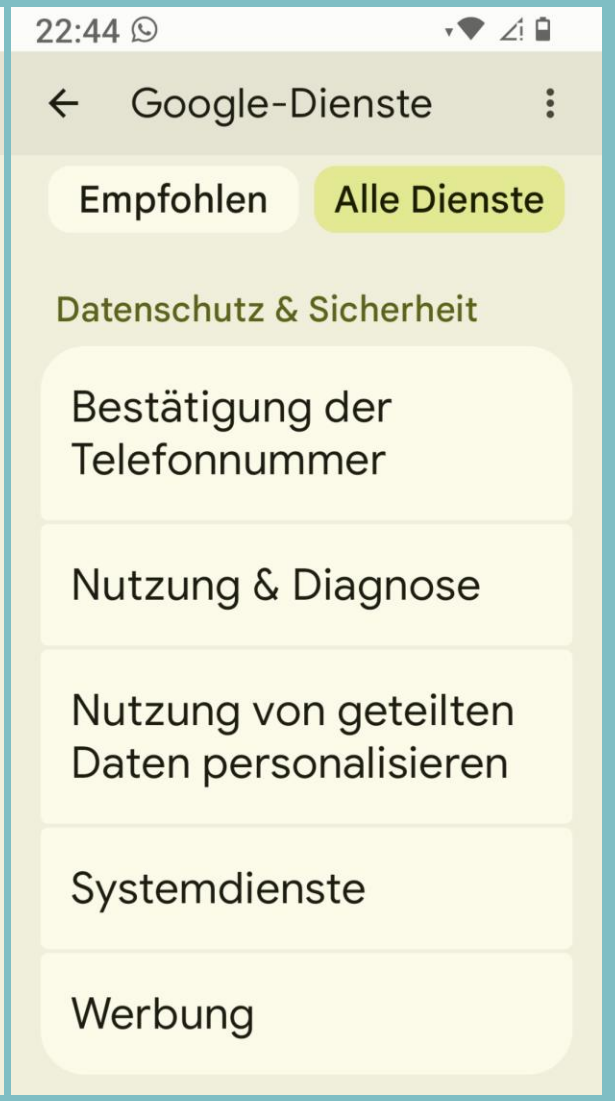


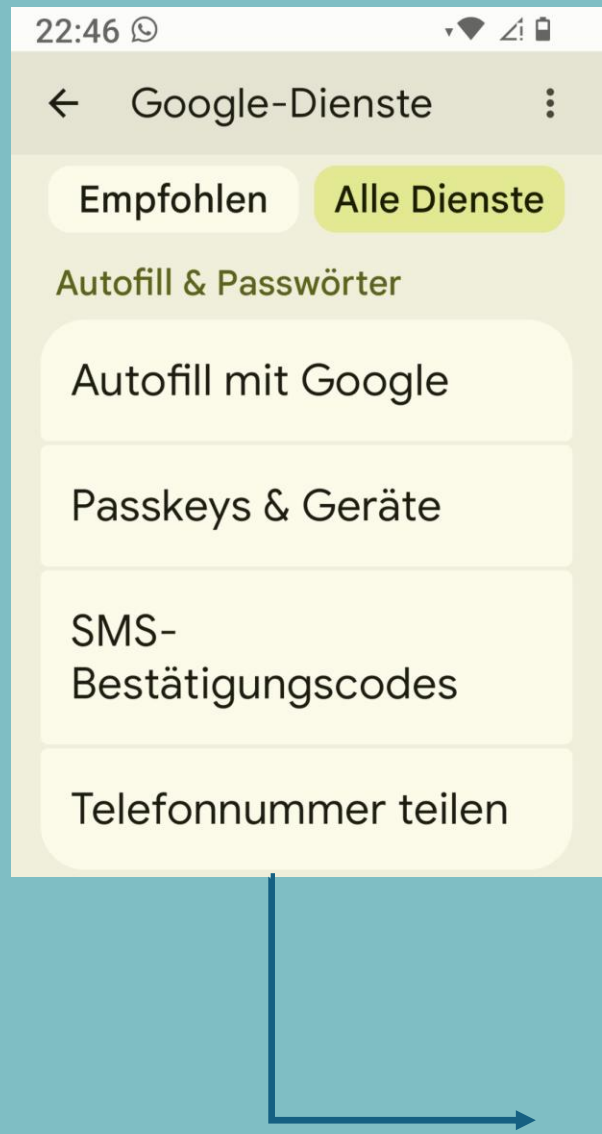
Konten welche nichtmehr verwendet werden einfach löschen.

Android - Einstellungen

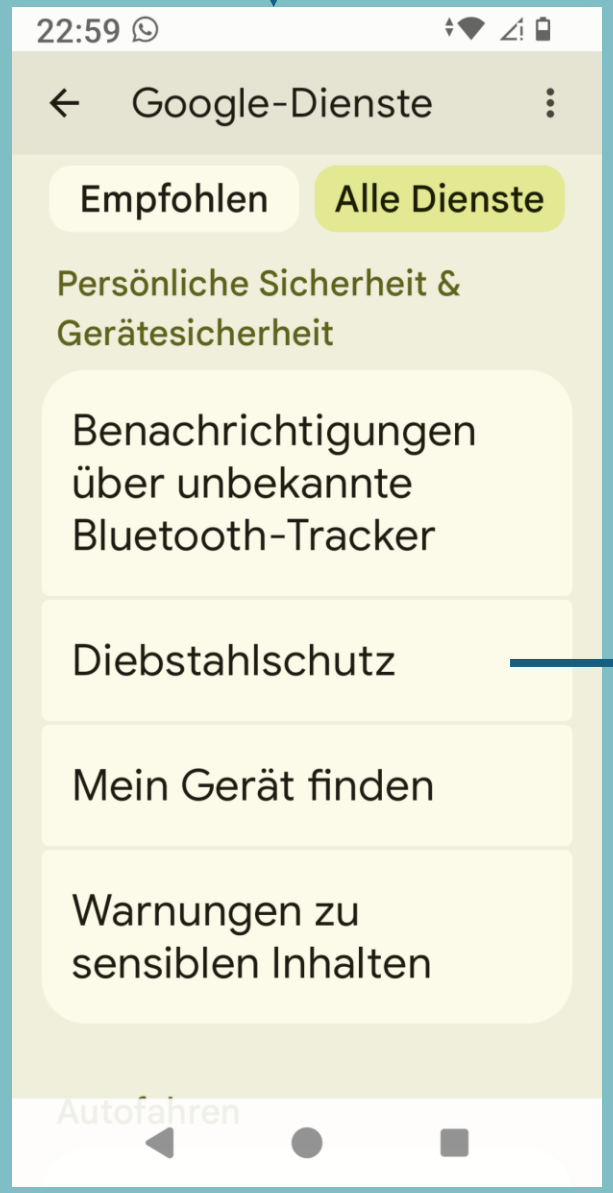


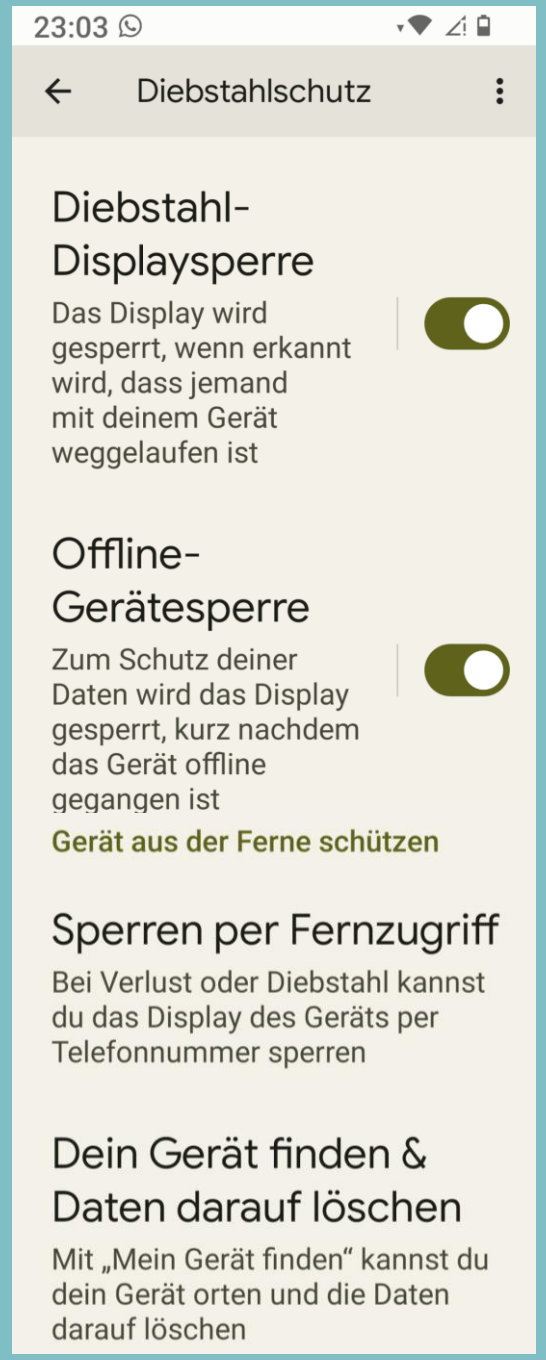






Android - Einstellungen





Und Nun? Wo Fang ich an?

1. Welche Funktionen sind mir wichtig?
   - **Navigation:** Maps, „Mein Gerät finden“, Notfall
   - **Bewegungs-/Aktivitäts-Erkennung :** Fitness- oder Gesundheits-Apps
   - **Notfall-Daten:** Notfall-Apps
   - **Kontakt-Daten:** Kontakte in allen Messenger-Apps (verweigern falls man in einem Messenger anonym bleiben will
   - **Fotos & Medien-Daten:** Zugriff zum versenden von Bildern und Dateien
2. Google-Konto Datenschutz anpassen
   - Im Internet über Browser
   - Auf dem Gerät
3. Was will ich mit welcher App machen
   - App-Berechtigungen überprüfen und ggf. unnötige Freigaben entziehen
   - Freigaben nur bei Verwendung der App

Oder einfach im Mediencafé für Senioren vorbeischauen und sich beraten Lassen

Und Nun? Wo Fang ich an?

1. Welche Funktionen sind mir wichtig?
   - **Navigation:** Maps, „Mein Gerät finden“, Notfall
   - **Bewegungs-/Aktivitäts-Erkennung :** Fitness- oder Gesundheits-Apps
   - **Notfall-Daten:** Notfall-Apps
   - **Kontakt-Daten:** Kontakte in allen Messenger-Apps (verweigern falls man in einem Messenger anonym bleiben will
   - **Fotos & Medien-Daten:** Zugriff zum versenden von Bildern und Dateien
2. Google-Konto Datenschutz anpassen
   - Im Internet über Browser
   - Auf dem Gerät
3. Was will ich mit welcher App machen
   - App-Berechtigungen überprüfen und ggf. unnötige Freigaben entziehen
   - Freigaben nur bei Verwendung der App

Oder einfach im Mediencafé für Senioren vorbeischauen und sich beraten Lassen

Sonstiges

Was man noch tun kann:

- Vorinstallierte Apps deinstallieren oder deaktivieren
- Europäische Cloud-Anbieter wählen (siehe: https://european-alternatives.eu/de
- Messanger und E-Mail Alternativen suchen
- Alternativen App-Store verwenden (https://f-droid.org/de/)
- Immer informieren und dazu lernen
    - https://digitalcourage.de/swarm-support
    - https://digitale-senioren-weimar.de/
    - https://european-alternatives.eu/de
    - https://digital-botschafter.silver-tipps.de/

Danke!