Edno Chovak

PRAKTISCHES HANDBUCH DER GEGENMASSNAHMEN

TACTICAL BRIEFING | I-BF-06-01

Digitaler Selbstschutz auf Android und Samsung

Die Komplettanleitung

Version 1.0

Impressum

Praktisches Handbuch der Gegenmaßnahmen -
Tactical Briefing BF-06-01: Digitaler Selbstschutz auf Android und Samsung: Die Komplettanleitung
Version 1.0 - Erste deutschsprachige Ausgabe 2026

c/o IP-Management #8444
Ludwig-Erhard-Straße 18
20459 Hamburg
E-Mail: contact@edno-chovak.com
Web: edno-chovak.com

Dateiname: TB-I-BF-06-01-v1_de_DigitalerSelbstschutzaufAndroidundSamsung.pdf
~~Prüfsummenverifizierungsdatei: TB-I-BF-06-01-v1_de_CHKSUM.txt~~

Ich habe bei der Recherche und Ersterstellung dieses Tactical Briefings KI-Assistenzsysteme eingesetzt. Alle Inhalte wurden von mir inhaltlich verantwortet, auf Richtigkeit geprüft und redaktionell bearbeitet.

Inhaltsverzeichnis

Digitaler Selbstschutz auf Android und Samsung – Die Komplettanleitung

Zielgruppe: Nutzer eines Samsung Galaxy-Smartphones (oder eines anderen Android-Geräts) mit Google-Konto, YouTube-Nutzung, Google-Logins auf Drittanbieter-Websites und - bei Samsung-Geräten - einem Samsung-Konto.

Gesamtaufwand: ca. 2-3 Stunden für alle Maßnahmen; die wichtigsten Sofortmaßnahmen sind in 30 Minuten erledigt.

Gliederung: Das Kapitel folgt einer Logik von außen nach innen - von der Kontoebene über das Betriebssystem bis zur Hardware - und schließt mit einem vollständigen Überblick über alle Maßnahmen.

Vorbemerkung: Wer ein Samsung-Smartphone mit Google-Konto nutzt, hat es mit mindestens zwei parallelen Datensammlern zu tun: Google erfasst Aktivitäten über das Betriebssystem und seine Apps, Samsung erfasst Nutzungsdaten über One UI, das Samsung-Konto und eigene Dienste. Beide Akteure sind legitime Unternehmen, die im Rahmen ihrer Datenschutzrichtlinien handeln - aber diese Richtlinien erlauben erheblich mehr Datensammlung, als den meisten Nutzern bewusst ist. Die folgenden Maßnahmen reduzieren diese Datensammlung systematisch, ohne die grundlegende Funktionsfähigkeit des Geräts zu beeinträchtigen.

1 Lagebild

Digitale Bedrohungen beginnen nicht mit einem Angriff. Sie beginnen mit Datenerfassung. Suchverläufe, Standortdaten, Klickmuster und Metadaten werden zu Verhaltensprofilen aggregiert, aus denen Systeme Rückschlüsse ziehen, die Sie nie preisgegeben haben - über Einkommen, Gesundheit, politische Überzeugungen. Die eigentliche Angriffsfläche ist nicht Ihr Gerät. Es ist das Vorhersagemodell Ihres Verhaltens.

Überwachung schadet, auch wenn nichts passiert. Der Chilling Effect, erlernte Hilflosigkeit und chronischer Hintergrundstress sind messbare psychologische Folgen - lange bevor ein konkreter Schaden eintritt. Und: Digitale Spuren überdauern Regierungen. Was heute legal ist, kann morgen gegen Sie verwendet werden.

Ihre Geräte und Dienste sind in der Standardkonfiguration nicht auf Datenschutz ausgelegt. Der Abfluss persönlicher Informationen ist der Normalzustand - nicht die Ausnahme.

Konsequenz: Sie müssen selbst aktiv werden. Jede Schutzmaßnahme reduziert Ihre Angriffsfläche, stärkt Ihre digitale Selbstbestimmung und hat eine nachweislich positive Wirkung auf Ihr psychisches Wohlbefinden. Wer sich schützt, schützt zudem auch andere - Datenschutz ist ein gesellschaftliches Gut.

Dieses Tactical Briefing zeigt Ihnen ganz konkret, wie das geht.

1.1 FOKUS DIESES TACTICAL BRIEFINGS

SB-I-4	Schutz der Privatsphäre
BF-06	Mobile Nutzung
SOFORT	Minimierung der Datenbasis für Metadatenanalyse

Smartphones sind die persönlichsten und gleichzeitig am stärksten überwachten Geräte im digitalen Alltag. Sie kennen Ihren Standort, Ihre Kontakte, Ihre Gewohnheiten, Ihre Gesundheitsdaten und Ihre Kommunikation. Die Standardkonfiguration von Android und iOS ist auf Datenerfassung optimiert.

Operative Leitlinie

Das Smartphone ist das umfassendste Überwachungsgerät, das je existiert hat - und Sie tragen es freiwillig bei sich. Jede Einschränkung der Datenerfassung ist ein Gewinn an persönlicher Souveränität.

2 Das Google-Konto - Aktivitäten, Verlauf und Werbung

Das Google-Konto ist der wichtigste Ausgangspunkt, weil hier die meisten Daten zentral gespeichert und verwaltet werden. Alle Einstellungen in diesem Abschnitt sind über myaccount.google.com erreichbar - am besten am Desktop-Browser, da die Übersicht dort vollständiger ist. Auf dem Android-Handy alternativ über **Einstellungen → Google → Google-Konto verwalten**.

2.1 AKTIVITÄTSSTEUERUNG: WAS GOOGLE ÜBER SIE SPEICHERT

Der Bereich „Aktivitätssteuerung" unter myaccount.google.com/activitycontrols ist die umfangreichste Datenquelle im Google-Konto. Hier entscheiden Sie, welche Aktivitätsdaten Google dauerhaft mit Ihrem Konto verknüpft.

Web- und App-Aktivitäten ist standardmäßig aktiviert und erfasst jede Suchanfrage, jeden Besuch einer Website mit Google-Diensten, jeden Klick in Google-Apps sowie alle Aktivitäten in Apps, die Google Analytics oder Firebase nutzen - einschließlich Sprachsuchen via Google Assistant. Klicken Sie auf diesen Eintrag und deaktivieren Sie den Schalter. Bestätigen Sie mit „Pausieren". Klicken Sie anschließend auf „Aktivitäten verwalten", wählen Sie „Löschen → Gesamten Zeitraum → Alle Kategorien → Löschen". Deaktivieren Sie innerhalb dieser Einstellung auch die Unteroption „Auch Chrome-Verlauf und Aktivitäten auf Websites und in Apps einschließen, die Google-Dienste nutzen" - diese erlaubt Google, Ihren Browser-Verlauf auch außerhalb von Google-eigenen Seiten zu erfassen.

Standortverlauf speichert eine präzise Zeitleiste Ihrer Bewegungen auf Basis von GPS, WLAN-Netzwerken und Mobilfunkmasten. Diese Daten werden in „Google Maps Zeitleiste" visualisiert und sind oft erschreckend detailliert: Wann Sie wo waren, wie lange, welche Route Sie genommen haben. Deaktivieren Sie den Schalter und löschen Sie alle gespeicherten Standortdaten über „Gesamten Standortverlauf löschen".

YouTube-Verlauf wird separat gespeichert und umfasst Such- und Wiedergabeverlauf. Diese Daten werden genutzt, um ein detailliertes Profil Ihrer Interessen, politischen Neigungen und Gewohnheiten zu erstellen. Deaktivieren Sie beide Unteroptionen - „YouTube-Suchverlauf" und „YouTube-Wiedergabeverlauf" - separat und löschen Sie die bisherigen Daten. Als Kompromiss, wenn Sie die Empfehlungsfunktion teilweise nutzen möchten: Richten Sie unter „Automatische Löschung" einen Zeitraum von 3 Monaten ein.

Für alle verbleibenden Aktivitätsbereiche empfiehlt sich die Einrichtung einer **automatischen Löschfrist**: Öffnen Sie jeden Bereich und wählen Sie „Automatische Löschung aktivieren → Älter als 3 Monate". So werden Daten, die trotz Deaktivierung anfallen könnten, regelmäßig bereinigt.

2.2 WERBEPERSONALISIERUNG ABSCHALTEN

Öffnen Sie adssettings.google.com. Google erstellt auf Basis Ihrer Aktivitäten ein Werbeprofil mit geschätztem Alter, Geschlecht, Interessen, Beruf und Kaufabsichten. Dieses Profil wird nicht nur für Google-eigene Dienste genutzt, sondern auch für das gesamte Google Display-Netzwerk - also Werbung auf Millionen von Websites. Klicken Sie auf „Personalisierte Werbung" und deaktivieren Sie den Schalter. Scrollen Sie anschließend nach unten und löschen Sie alle gespeicherten Interessen-Kategorien manuell, da diese sonst gespeichert bleiben.

Auf dem Android-Handy gibt es zusätzlich eine separate Werbe-ID (Android Advertising ID), die Apps zur Verfolgung Ihres Verhaltens über verschiedene Apps hinweg nutzen. Öffnen Sie **Einstellungen → Google → Werbung** (oder bei neueren Android-Versionen: **Einstellungen → Datenschutz → Werbung**) und wählen Sie „Werbe-ID löschen". Bei Android 12 und neuer können Sie die Werbe-ID vollständig deaktivieren.

2.3 DRITTANBIETER-ZUGRIFFE BEREINIGEN

Öffnen Sie myaccount.google.com/permissions. Hier sehen Sie alle Apps, Websites und Dienste, bei denen Sie sich mit Ihrem Google-Konto angemeldet haben oder denen Sie Zugriff auf Ihr Konto gewährt haben. Dieser Bereich ist häufig erschreckend umfangreich - viele Nutzer finden hier Dienste, die sie seit Jahren nicht mehr genutzt haben. Gehen Sie jeden Eintrag durch und entfernen Sie den Zugriff für alle Dienste, die Sie nicht innerhalb der letzten sechs Monate aktiv genutzt haben. Achten Sie besonders auf Einträge mit weitreichenden Berechtigungen wie „Alle Google-Kontodaten anzeigen" oder „E-Mails senden".

2.4 SICHERHEIT: ANMELDUNGEN, SICHERHEITSCHECK UND ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Öffnen Sie myaccount.google.com/security. Im Abschnitt „Ihre Geräte" sehen Sie alle Geräte, auf denen Sie aktuell mit Ihrem Google-Konto angemeldet sind. Prüfen Sie jeden Eintrag und melden Sie sich von Geräten ab, die Sie nicht mehr besitzen oder nicht erkennen.

Führen Sie den integrierten Sicherheitscheck unter myaccount.google.com/security-checkup durch. Er zeigt kompromittierte Passwörter, unsichere Drittanbieter-Zugriffe und veraltete Wiederherstellungsoptionen an.

Falls noch nicht geschehen: Aktivieren Sie die **Zwei-Faktor-Authentifizierung** unter **Sicherheit → Wie Sie sich bei Google anmelden → Bestätigung in zwei Schritten**. Wählen Sie als zweiten Faktor ausdrücklich *nicht* die SMS-Option - SMS ist anfällig für SIM-Swapping-Angriffe, bei denen ein Angreifer Ihre Telefonnummer auf eine neue SIM-Karte überträgt und damit Ihre 2FA-Codes abfängt. Nutzen Sie stattdessen eine Authenticator-App wie Proton Authenticator, Google Authenticator oder das quelloffene Aegis auf Android.

2.5 PERSÖNLICHE DATEN, GOOGLE-SUCHE UND CHROME

Öffnen Sie myaccount.google.com/personal-info und entfernen Sie alle Angaben, die für die Kontonutzung nicht zwingend erforderlich sind - insbesondere Geburtsdatum, Geschlecht und Adresse. Die Telefonnummer ist für die 2FA-Wiederherstellung nützlich, sollte aber nicht für Werbezwecke genutzt werden: Prüfen Sie unter **Persönliche Daten → Telefon → Wozu wird diese Nummer verwendet**, ob die Option „Für personalisierte Werbung" deaktiviert ist.

Falls Sie Google Chrome nutzen: Öffnen Sie **Chrome → Einstellungen → Synchronisierung und Google-Dienste** und deaktivieren Sie die Synchronisierung für alle nicht benötigten Kategorien - insbesondere „Browserverlauf" und „Offene Tabs". Deaktivieren Sie außerdem unter „Weitere Google-Dienste" die Optionen „Suchanfragen und Browsing verbessern" sowie „Autofill-Daten an Google senden". Mittelfristig empfiehlt sich der Wechsel zu einem datenschutzfreundlicheren Browser.

2.6 YOUTUBE-DATENSCHUTZ UND GOOGLE ASSISTANT

Öffnen Sie YouTube und navigieren Sie zu **Ihr Konto → Einstellungen → Datenschutz**. Deaktivieren Sie alle drei Optionen: „Abonnierte Kanäle öffentlich machen", „Gespeicherte Playlists öffentlich machen" und „Bewertungen öffentlich machen". Diese Einstellungen geben Informationen über Ihre Interessen und Gewohnheiten preis.

Für den Google Assistant: Öffnen Sie die **Google-App → Profilbild → Einstellungen → Google Assistant**. Deaktivieren Sie unter „Allgemein" den Google Assistant vollständig, oder schränken Sie unter „Daten & Datenschutz" alle Datenzugriffe ein: Deaktivieren Sie „Web- und App-Aktivitäten", „Sprachmodell auf diesem Gerät verbessern" und alle personalisierten Ergebnisse. Für Google Gemini: Öffnen Sie **Google-App → Profilbild → Google-Konto verwalten → Daten & Datenschutz → Gemini-Apps-Aktivität**, deaktivieren Sie diese und löschen Sie alle gespeicherten Aktivitäten.

3 Das Android-Betriebssystem - Netzwerk, Berechtigungen und Systemdienste

Dieser Abschnitt behandelt Einstellungen, die direkt im Android-Betriebssystem vorgenommen werden - unabhängig vom Google-Konto. Alle Einstellungen befinden sich in der App **Einstellungen** auf dem Gerät. Die genauen Bezeichnungen können je nach Hersteller und Android-Version leicht abweichen, die Struktur ist jedoch vergleichbar.

3.1 NETZWERK UND VERBINDUNGEN ABSICHERN

Privates DNS ist eine der wirkungsvollsten und am wenigsten bekannten Schutzmaßnahmen. Jede DNS-Anfrage - also jedes Mal, wenn Ihr Handy einen Domainnamen auflöst - wird standardmäßig unverschlüsselt an den DNS-Server Ihres Mobilfunkanbieters gesendet. Dieser kann damit ein vollständiges Protokoll aller von Ihnen besuchten Domains erstellen, auch wenn die eigentlichen Inhalte verschlüsselt übertragen werden. Öffnen Sie **Einstellungen → Netzwerk & Internet → Privates DNS**, wählen Sie „Hostname des privaten DNS-Anbieters" und tragen Sie dns.quad9.net (Quad9, Schweiz, blockiert bekannte Malware-Domains) oder dns.adguard.com (blockiert zusätzlich Tracking- und Werbedomains) ein. Ab diesem Moment werden alle DNS-Anfragen verschlüsselt über DNS-over-TLS übertragen.

IMSI-Catcher-Schutz: IMSI-Catcher sind Geräte, die vorgeben, eine Mobilfunkbasisstation zu sein, und Mobiltelefone dazu bringen, sich mit ihnen zu verbinden. Sie werden von Strafverfolgungsbehörden, aber auch von privaten Akteuren eingesetzt, um Standortdaten und Kommunikation abzufangen. Sie nutzen häufig das veraltete 2G-Protokoll, da es keine gegenseitige Authentifizierung kennt. Öffnen Sie **Einstellungen → Netzwerk & Internet → SIM-Karten → Sicherheit des Mobilfunknetzes** und aktivieren Sie „Nur verschlüsselte Verbindungen zulassen" und „Schutz vor 2G-Netzen" (auf Pixel-Geräten ab Android 12 verfügbar; bei anderen Herstellern unter abweichendem Namen).

MAC-Adress-Randomisierung: Jedes WLAN-Gerät sendet beim Suchen nach bekannten Netzwerken seine MAC-Adresse aus - eine eindeutige Hardware-Kennung. Betreiber von WLAN-Netzwerken können diese Adresse nutzen, um Ihre Bewegungen über verschiedene Standorte hinweg zu verfolgen. Öffnen Sie **Einstellungen → WLAN**, tippen Sie auf jedes gespeicherte Netzwerk und prüfen Sie unter „Datenschutz", ob „Zufällige MAC-Adresse" aktiviert ist. Ab Android 10 ist diese Funktion standardmäßig aktiviert - prüfen Sie dennoch alle gespeicherten Netzwerke.

WLAN- und Bluetooth-Hintergrundscan deaktivieren: Android erlaubt Apps und dem System standardmäßig, auch bei ausgeschaltetem WLAN und Bluetooth nach Netzwerken und Geräten zu scannen - für die Standortbestimmung. Öffnen Sie **Einstellungen → Standort → Standortdienste** und deaktivieren Sie sowohl „WLAN-Suche" als auch „Bluetooth-Suche".

Bluetooth und NFC sollten deaktiviert werden, wenn sie nicht aktiv genutzt werden. Bluetooth ermöglicht Tracking über Beacons in Geschäften und öffentlichen Räumen; NFC kann bei bestimmten Angriffen für ungewollte Datenübertragungen genutzt werden. Nutzen Sie die Schnelleinstellungsleiste für das schnelle Ein- und Ausschalten; für NFC: **Einstellungen → Verbundene Geräte → Verbindungseinstellungen → NFC**.

3.2 APP-BERECHTIGUNGEN SYSTEMATISCH PRÜFEN

Der **Berechtigungsmanager** unter **Einstellungen → Datenschutz → Berechtigungsmanager** zeigt alle Berechtigungen kategorisiert an und listet auf, welche Apps jeweils Zugriff haben. Dies ist effizienter als jede App einzeln zu öffnen. Die folgende Tabelle gibt eine Orientierung für die Vergabe:

Berechtigung	Exposition	Empfehlung
Standort	Sehr hoch	Nur bei Nutzung; nie „Immer" außer für Navigation
Mikrofon	Sehr hoch	Nur bei Nutzung; für die meisten Apps deaktivieren
Kamera	Hoch	Nur bei Nutzung; für Nicht-Kamera-Apps deaktivieren
Kontakte	Hoch	Nur für Telefon/Messenger; alle anderen deaktivieren
Anrufprotokolle	Hoch	Nur für Telefon-App
SMS	Hoch	Nur für Standard-SMS-App
Körpersensoren	Mittel	Nur für Fitness-Apps
Kalender	Mittel	Nur für Kalender-Apps
Dateien & Medien	Mittel	Restriktiv vergeben
Nahe gelegene Geräte	Mittel	Nur für Bluetooth-Apps
Benachrichtigungen	Niedrig	Selektiv; viele Apps brauchen keine Push-Benachrichtigungen

Neben den Standardberechtigungen gibt es den **speziellen App-Zugriff** unter **Einstellungen → Apps → Spezieller App-Zugriff**, der besonders weitreichende Berechtigungen enthält und häufig übersehen wird. Prüfen Sie insbesondere: „Zugriff auf alle Dateien" (nur Dateimanager und Backup-Apps), „Apps zur Geräteverwaltung" (nur legitime MDM-Lösungen), „Über anderen Apps einblenden" (ein bekannter Angriffsvektor für Clickjacking - beschränken Sie diese auf wenige vertrauenswürdige Apps), „Unbekannte Apps installieren" (sollte für alle Apps deaktiviert sein) und „Zugriff auf Premium-SMS" (sollte für keine App aktiviert sein).

Ab Android 12 gibt es bei einigen Geräten einen **globalen Kamera- und Mikrofonschalter** in der Schnelleinstellungsleiste (zweimal von oben wischen). Deaktivieren Sie beide und aktivieren Sie sie nur temporär, wenn eine App sie benötigt. Alternativ: **Einstellungen → Datenschutz → Kamerazugriff / Mikrofonzugriff**.

3.3 DATENSCHUTZ-DASHBOARD, DIAGNOSEDATEN UND SYSTEMDIENSTE

Das **Datenschutz-Dashboard** unter **Einstellungen → Datenschutz → Datenschutz-Dashboard** (ab Android 12) zeigt, welche Apps in den letzten 24 Stunden auf sensible Berechtigungen zugegriffen haben. Prüfen Sie es regelmäßig - insbesondere Zugriffe auf Standort, Mikrofon und Kamera. Wenn eine App auf eine Berechtigung zugegriffen hat, die Sie nicht erwartet hätten, entziehen Sie die Berechtigung sofort.

Android sendet standardmäßig **Nutzungsstatistiken und Diagnosedaten** an Google. Öffnen Sie **Einstellungen → Datenschutz → Nutzung & Diagnose** und deaktivieren Sie alle Optionen.

Öffnen Sie zusätzlich **Einstellungen → Google → Weitere Einstellungen → Nutzung & Diagnose** - dieser zweite Kanal wird häufig übersehen.

Android System Intelligence - der Dienst hinter Tastaturvorschlägen, Smart Reply und automatischer Texterkennung - analysiert Ihre Kommunikationsinhalte und sendet Daten an Google. Öffnen Sie **Einstellungen → Datenschutz → Erweitert** und deaktivieren Sie „Personalisieren anhand von App-Daten". Tippen Sie auf „Android System Intelligence" und deaktivieren Sie „Mithilfe der Google-Kontodaten die Nutzung anpassen".

Der **AutoFill-Dienst** unter **Einstellungen → Datenschutz → AutoFill-Dienst** füllt Passwörter und Kreditkartendaten aus. Wenn dieser Dienst auf Google eingestellt ist, werden Ihre Zugangsdaten mit Google synchronisiert. Wechseln Sie zu einem datenschutzfreundlichen Passwortmanager wie **Proton Pass** oder **Bitwarden** - installieren Sie zunächst die App, dann erscheint sie als Option.

Health Connect unter **Einstellungen → Datenschutz → Health Connect** ist Googles zentrale Schnittstelle für Gesundheits- und Fitnessdaten. Prüfen Sie unter „App-Berechtigungen", welche Apps Lese- und Schreibzugriff auf welche Datenkategorien haben, und entziehen Sie nicht benötigten Apps den Zugriff.

3.4 GERÄTESICHERHEIT

Die **Displaysperre** ist die wichtigste physische Sicherheitsmaßnahme. Verwenden Sie eine PIN mit mindestens 6 Ziffern oder ein alphanumerisches Passwort. Wenn Sie Fingerabdruck oder Gesichtserkennung nutzen, beachten Sie: In manchen Jurisdiktionen können Behörden Sie zwingen, biometrische Entsperrung zu nutzen, nicht aber eine PIN einzugeben. Aktivieren Sie zusätzlich die Option „Biometrie bei Neustart deaktivieren", sodass nach jedem Neustart zunächst die PIN eingegeben werden muss.

Aktivieren Sie die **SIM-Karten-PIN** unter **Einstellungen → Sicherheit → SIM-Kartensperre**. Die Standard-PIN (meist 0000 oder 1234) sollte auf eine individuelle, mindestens 6-stellige PIN geändert werden. Diese verhindert, dass eine gestohlene SIM-Karte in einem anderen Gerät genutzt werden kann.

Stellen Sie sicher, dass **automatische Sicherheitsupdates** aktiviert sind: **Einstellungen → System → Systemupdate**. Geräte, die seit mehr als sechs Monaten kein Sicherheitspatch erhalten haben, sind erheblich anfälliger für bekannte Angriffe.

3.5 STANDARD-APPS ERSETZEN

Chrome ersetzen: Google Chrome ist trotz Inkognito-Modus ein umfangreiches Tracking-Werkzeug. Im Jahr 2024 einigte sich Google in einem Vergleich auf die Vernichtung von Milliarden von Datensätzen, die im Inkognito-Modus gesammelt worden waren. Empfehlenswerte Alternative: **Brave Browser** (blockiert Tracker und Werbung standardmäßig, unterstützt alle Chrome-Erweiterungen). Standard-Browser setzen: **Einstellungen → Apps → Standard-Apps → Browser-App**.

Suchmaschine ersetzen: Die Google-Suche ist auch ohne angemeldetes Konto ein Tracking-Instrument. Wechseln Sie zu **Brave Search** (eigener Index, kein Google-Tracking) oder **DuckDuckGo**. Die Suchmaschine wird direkt im Browser als Standard eingestellt.

Gboard ersetzen: Googles Standard-Tastatur sendet Tipp-Muster und Wörter an Google-Server. Installieren Sie **OpenBoard** (Open Source, vollständig offline) oder **FlorisBoard**. Standard-Tastatur setzen: **Einstellungen → Allgemeine Verwaltung → Tastatur → Standard-Tastatur**.

Benachrichtigungsvorschau auf dem Sperrbildschirm einschränken: Öffnen Sie **Einstellungen → Benachrichtigungen → Benachrichtigungen auf Sperrbildschirm** und wählen Sie

„Sensible Benachrichtigungen ausblenden". So werden 2FA-Codes, Nachrichten und E-Mails nicht auf dem gesperrten Bildschirm angezeigt.

Google-Backup einschränken: Das Android-Backup sichert standardmäßig App-Daten, WLAN-Passwörter und Geräteeinstellungen in Google Drive. Öffnen Sie **Einstellungen → System → Backup** und prüfen Sie, was gesichert wird. Wenn Sie kein Google-Backup wünschen, deaktivieren Sie „Auf Google Drive sichern". Beachten Sie: Ohne Backup gehen bei einem Geräteverlust alle App-Daten verloren - erwägen Sie **Proton Drive** als Alternative.

4 Samsung One UI - Das zweite Ökosystem

Samsung-Nutzer haben es mit einem zweiten, oft übersehenen Datensammler zu tun: One UI ist keine neutrale Android-Oberfläche, sondern ein eigenständiges Ökosystem mit eigenen Diensten, eigener Dateninfrastruktur und eigenen KI-Funktionen. Das Samsung-Konto unterliegt südkoreanischem Recht (PIPA - Personal Information Protection Act), das in einigen Bereichen weniger streng ist als die europäische DSGVO.

4.1 DAS SAMSUNG-KONTO BEREINIGEN

Das Samsung-Konto verknüpft Gerätenutzung, App-Käufe im Galaxy Store, Samsung Health-Daten, Standortdaten über „Mein Gerät finden" und KI-Aktivitäten über Galaxy AI. Samsung gibt in seiner Datenschutzrichtlinie an, Daten mit „Geschäftspartnern" zu teilen - darunter Werbepartner und Analysedienstleister.

Synchronisation einschränken: Öffnen Sie **Einstellungen → Samsung-Konto → [Ihr Konto] → Synchronisierung** und deaktivieren Sie alle Kategorien, die Sie nicht aktiv benötigen: Samsung Cloud Backup, Samsung Internet-Lesezeichen, Samsung Notes, Samsung Health-Daten und Kalender - sofern Sie jeweils alternative Dienste nutzen.

Datenschutzeinstellungen im Konto: Öffnen Sie **Einstellungen → Samsung-Konto → Datenschutz** und deaktivieren Sie „Personalisierte Dienste" (Samsung nutzt diese Einstellung für geräteübergreifende Werbeauswertung), „Diagnosedaten senden" und „Marketingmitteilungen". Öffnen Sie zusätzlich account.samsung.com in einem Browser und prüfen Sie unter „Datenschutz" die gespeicherten Daten. Samsung bietet dort die Möglichkeit, Daten einzusehen, herunterzuladen und zu löschen.

4.2 SAMSUNG-EIGENE DATENSAMMLUNG IM BETRIEBSSYSTEM

Samsung betreibt mehrere Hintergrunddienste zur Datensammlung, die über die normalen Einstellungen nicht immer sichtbar sind.

Der **Samsung Customization Service** (com.samsung.android.rubin.app) sammelt Nutzungsdaten und sendet sie an Samsung für „personalisierte Empfehlungen". Öffnen Sie **Einstellungen → Apps → Alle Apps anzeigen** und suchen Sie nach „Anpassungsdienst" - tippen Sie darauf und wählen Sie „Deaktivieren". Alternativ: **Einstellungen → Datenschutz → Erweiterte Datenschutzeinstellungen → Anpassungsdienst**.

Der **Samsung Push Service** (com.sec.spp.push) wird nicht nur für legitime Benachrichtigungen genutzt, sondern auch für Werbeanzeigen in Samsung-eigenen Apps und Benachrichtigungen. Öffnen Sie **Einstellungen → Apps → Alle Apps anzeigen → Samsung Push Service → Deaktivieren** (sofern Sie Galaxy Store und Samsung Pay nicht nutzen).

Samsung sendet Diagnosedaten über **drei parallele Kanäle**, zusätzlich zu den Google-Diagnosedaten. Deaktivieren Sie alle drei: **Einstellungen → Datenschutz → Diagnosedaten senden**, **Einstellungen → Allgemeine Verwaltung → Diagnose** und **Einstellungen → Samsung-Konto → Datenschutz → Diagnosedaten**.

Samsung blendet in mehreren vorinstallierten Apps **Werbung** ein: im Sperrbildschirm (Samsung Free), in der Galerie und in der Wetter-App. Öffnen Sie **Einstellungen → Datenschutz → Marketing-Informationen** und deaktivieren Sie alle Optionen. Für den Sperrbildschirm: Wischen Sie nach rechts zu Samsung Free, tippen Sie auf das Drei-Punkte-Menü und wählen Sie „Einstellungen → Seite deaktivieren".

4.3 BIXBY – SAMSUNGS SPRACHASSISTENT

Bixby hat Zugriff auf Mikrofon, Kontakte, Kalender, Nachrichten, Anrufprotokolle, Standort und - bei aktivierter Bixby Vision - auf die Kamera. Sprachaufnahmen werden laut Samsung-Datenschutzrichtlinie „verschlüsselt an Server gesendet" und für die Verbesserung des Sprachmodells genutzt. Die Aufbewahrungsdauer ist in der öffentlichen Dokumentation nicht vollständig transparent.

Bixby deaktivieren: Öffnen Sie die **Bixby-App → Drei-Punkte-Menü → Einstellungen → Bixby Voice → Bixby deaktivieren**. Für die Seitentaste: **Einstellungen → Erweiterte Funktionen → Seitentaste** und ändern Sie die Belegung. Deaktivieren Sie außerdem **Bixby Routines** unter **Einstellungen → Erweiterte Funktionen → Bixby Routines**.

Bixby-Sprachdaten löschen: Öffnen Sie account.samsung.com → **Datenschutz → Meine Daten verwalten → Bixby-Daten** und löschen Sie alle gespeicherten Sprachaufnahmen und Aktivitätsdaten.

4.4 GALAXY AI – ON-DEVICE ODER CLOUD?

Galaxy AI nutzt ein hybrides Verarbeitungsmodell. Die folgende Tabelle zeigt, welche Funktionen lokal laufen und welche Daten in die Cloud senden:

Funktion	Verarbeitung	Datenschutzrisiko
Live Translate (Anrufe)	On-Device	Niedrig
Chat-Übersetzung	On-Device	Niedrig
Schreibstil & Grammatik	On-Device	Niedrig
Transcript Assist (Basis)	On-Device	Niedrig
Foto-Remaster (einfach)	On-Device	Niedrig
Generative Bearbeitung (Fotos)	Cloud (Samsung)	**Hoch**
Sketch to Image	Cloud (Samsung)	**Hoch**
Note Assist (Zusammenfassung)	Cloud (Samsung)	**Hoch**
Browsing Assist	Cloud (Samsung)	**Hoch**
Circle to Search	Cloud (Google)	**Sehr hoch**
Portrait Studio	Cloud (Samsung)	**Hoch**

Galaxy AI auf On-Device beschränken: Öffnen Sie **Einstellungen → Galaxy AI** (oder **Einstellungen → Erweiterte Funktionen → Erweiterte Intelligenz**) und aktivieren Sie „Daten nur auf

Gerät verarbeiten". Damit werden alle cloud-basierten KI-Funktionen deaktiviert, während die On-Device-Funktionen verfügbar bleiben.

Circle to Search separat deaktivieren: Diese Google-Integration kann nicht über die Galaxy-AI-Einstellungen deaktiviert werden. Öffnen Sie **Einstellungen → Erweiterte Funktionen → Circle to Search** und deaktivieren Sie den Schalter.

4.5 VORINSTALLIERTE APPS UND BLOATWARE

Samsung-Geräte werden mit einer erheblichen Anzahl vorinstallierter Apps ausgeliefert, die nicht deinstalliert, sondern nur deaktiviert werden können. Öffnen Sie **Einstellungen → Apps → Alle Apps anzeigen**, tippen Sie auf die jeweilige App und wählen Sie „Deaktivieren". Die folgende Tabelle listet Apps auf, die für die meisten Nutzer sicher deaktiviert werden können:

App	Datenschutzproblem
Samsung Free	Nutzungsprofilierung, Werbeanzeigen im Sperrbildschirm
Samsung TV Plus	Nutzungsdaten, Werbung
Samsung Global Goals	Werbeanzeigen im Hintergrund
Bixby Voice	Sprachdaten an Samsung-Server
Bixby Routines	Zugriff auf umfangreiche Gerätedaten
Samsung Push Service	Werbeanzeigen in Benachrichtigungen
Samsung Customization Service	Nutzungsprofilierung
Samsung Location SDK	Standortdaten für Samsung-Apps
Game Launcher	Nutzungsstatistiken
AR Zone	Kameradaten

Für Apps, die nicht über die normalen Einstellungen deaktiviert werden können, ist das **Android Debug Bridge (ADB)**-Tool erforderlich. Verbinden Sie das Gerät mit einem Computer (USB-Debugging muss aktiviert sein: **Einstellungen → Entwickleroptionen → USB-Debugging**) und führen Sie aus:

```
adb shell pm disable-user --user 0 <Paketname>
```

Häufig deaktivierte Pakete: com.samsung.android.rubin.app (Customization Service), com.sec.spp.push (Push Service), com.samsung.android.app.spage (Samsung Free). Mit adb shell pm enable <Paketname> kann jede Deaktivierung rückgängig gemacht werden.

Wichtiger Hinweis: Deaktivieren Sie **niemals** Knox-bezogene Pakete (com.samsung.android.knox.*) oder den Secure Folder. Diese sind sicherheitskritisch und können bei Deaktivierung das Gerät in einen nicht startfähigen Zustand versetzen.

4.6 SAMSUNG INTERNET BROWSER

Samsung Internet bietet im Vergleich zu Google Chrome bessere Datenschutzoptionen - vorausgesetzt, diese werden manuell aktiviert. Öffnen Sie **Samsung Internet → Drei-Striche-Menü → Einstellungen → Datenschutz und Sicherheit** und aktivieren Sie: „Smart Anti-Tracking", einen Werbeblocker (z. B. AdGuard), „Nicht verfolgen senden" und „Verdächtige Websites blockieren". Deaktivieren Sie: „Surfverlauf für personalisierte Empfehlungen nutzen" und „Samsung Browsing-Daten für Verbesserungen teilen".

Ich empfehle aber ohnehin, statt des Samsung-Browsers den Brave-Browser einzusetzen.

4.7 SAMSUNG HEALTH UND WEARABLES

Samsung Health sammelt Schrittzähler-Daten, Herzfrequenz, Schlafmuster, Gewicht, Ernährungsdaten und - bei Galaxy Watch oder Galaxy Ring - kontinuierliche biometrische Messungen. Gesundheitsdaten gehören zu den sensibelsten Datenkategorien: Sie können von Versicherungen, Arbeitgebern oder Behörden genutzt werden und sind nach einem Datenleck nicht rückgängig zu machen.

Öffnen Sie **Samsung Health → Profilbild → Einstellungen → Datenschutz** und deaktivieren Sie „Daten mit Samsung teilen" und „Forschungsdaten teilen". Prüfen Sie unter „Verbundene Dienste", welche Drittanbieter-Apps Zugriff auf Ihre Gesundheitsdaten haben. Für Galaxy Watch und Ring: Öffnen Sie **Galaxy Wearable → Einstellungen → Datenschutz** und deaktivieren Sie „Diagnosedaten senden".

4.8 KNOX UND SECURE FOLDER

Samsung Knox ist Samsungs proprietäres Sicherheits-Framework, das auf Hardwareebene eine sichere Enklave für sensible Daten bereitstellt. Knox ist grundsätzlich ein Sicherheitsgewinn - es verhindert, dass Schadsoftware auf sensible Daten zugreift. Gleichzeitig ist Knox ein proprietäres, nicht auditierbares System.

Öffnen Sie **Einstellungen → Sicherheit und Datenschutz → Knox-Einstellungen** und prüfen Sie, ob „Knox Matrix" aktiviert ist - diese Funktion synchronisiert Sicherheitsstatus zwischen mehreren Samsung-Geräten im selben Samsung-Konto. Wenn Sie nur ein Gerät nutzen, können Sie Knox Matrix deaktivieren.

Wenn Sie den Secure Folder nutzen: Stellen Sie sicher, dass die Synchronisation mit Samsung Cloud deaktiviert ist: **Secure Folder → Einstellungen → Sicherung und Wiederherstellung → Samsung Cloud-Synchronisation → Deaktivieren**.

5 Gesamtübersicht – Alle Maßnahmen nach Priorität

Die folgende Tabelle fasst alle Maßnahmen aus den drei Abschnitten zusammen und ordnet sie nach Priorität. Die SOFORT-Maßnahmen sind in ca. 30 Minuten erledigt und haben die größte Wirkung.

5.1 SOFORT-MAßNAHMEN (CA. 30 MINUTEN)

Maßnahme	Pfad	Aufwand
Web- & App-Aktivitäten deaktivieren + löschen	myaccount.google.com/activitycontrols	5 Min.
YouTube-Verlauf deaktivieren + löschen	myaccount.google.com/activitycontrols	3 Min.
Standortverlauf deaktivieren + löschen	myaccount.google.com/activitycontrols	3 Min.
Drittanbieter-Zugriffe bereinigen	myaccount.google.com/permissions	10 Min.
Werbe-ID auf Android löschen	Einstellungen → Google → Werbung	2 Min.
2FA mit Authenticator-App aktivieren	myaccount.google.com/security	5 Min.
Galaxy AI auf On-Device beschränken *(Samsung)*	Einstellungen → Galaxy AI	2 Min.
Circle to Search deaktivieren *(Samsung)*	Einstellungen → Erweiterte Funktionen	1 Min.
Bixby deaktivieren *(Samsung)*	Bixby-App → Einstellungen	3 Min.
Samsung-Diagnosedaten (alle 3 Kanäle) deaktivieren *(Samsung)*	Einstellungen → Datenschutz / Samsung-Konto / Allg. Verwaltung	5 Min.

5.2 HOCH-MAßNAHMEN (CA. 45 MINUTEN)

Maßnahme	Pfad	Aufwand
Personalisierte Werbung deaktivieren	adssettings.google.com	3 Min.
App-Berechtigungen systematisch prüfen	Einstellungen → Datenschutz → Berechtigungsmanager	15 Min.

Maßnahme	Pfad	Aufwand
Privates DNS einrichten	Einstellungen → Netzwerk & Internet → Privates DNS	2 Min.
WLAN/Bluetooth-Hintergrundscan deaktivieren	Einstellungen → Standort → Standortdienste	2 Min.
Globale Kamera/Mikrofon-Sperre aktivieren	Schnelleinstellungen	1 Min.
AutoFill-Dienst auf Passwortmanager umstellen	Einstellungen → Datenschutz → AutoFill-Dienst	5 Min.
Nutzungs- & Diagnosedaten (Android) deaktivieren	Einstellungen → Datenschutz → Nutzung & Diagnose	3 Min.
Samsung-Konto-Synchronisation einschränken *(Samsung)*	Einstellungen → Samsung-Konto → Synchronisierung	5 Min.
Samsung Customization Service deaktivieren *(Samsung)*	Einstellungen → Apps → Anpassungsdienst	2 Min.
Samsung Push Service deaktivieren *(Samsung)*	Einstellungen → Apps → Samsung Push Service	2 Min.
Samsung Free deaktivieren *(Samsung)*	Sperrbildschirm → Wischen → Einstellungen	2 Min.
Werbung in Samsung-Apps deaktivieren *(Samsung)*	Einstellungen → Datenschutz → Marketing-Informationen	2 Min.
Samsung Health Datenweitergabe einschränken *(Samsung)*	Samsung Health → Datenschutz	3 Min.
SIM-Karten-PIN aktivieren	Einstellungen → Sicherheit → SIM-Kartensperre	2 Min.
Benachrichtigungsvorschau auf Sperrbildschirm einschränken	Einstellungen → Benachrichtigungen	2 Min.

5.3 MITTEL-MAßNAHMEN (CA. 45 MINUTEN)

Maßnahme	Pfad	Aufwand
Automatische Löschung (3 Monate) einrichten	myaccount.google.com/activitycontrols	5 Min.
Chrome-Synchronisation einschränken	Chrome → Einstellungen	5 Min.
Persönliche Daten im Google-Konto bereinigen	myaccount.google.com/personal-info	5 Min.

Maßnahme	Pfad	Aufwand
Speziellen App-Zugriff prüfen	Einstellungen → Apps → Spezieller App-Zugriff	10 Min.
Health Connect prüfen	Einstellungen → Datenschutz → Health Connect	5 Min.
Google-Backup einschränken	Einstellungen → System → Backup	3 Min.
Kontaktsynchronisation prüfen	Einstellungen → Konten → Google → Synchronisierung	3 Min.
Google Fotos Backup konfigurieren	Google Fotos → Fotospeicher-Einstellungen	3 Min.
Samsung-Konto-Datenschutz auf account.samsung.com *(Samsung)*	account.samsung.com	10 Min.
Bixby-Sprachdaten löschen *(Samsung)*	account.samsung.com → Datenschutz → Bixby-Daten	5 Min.
Knox Matrix deaktivieren *(Samsung)*	Einstellungen → Knox-Einstellungen	2 Min.
Secure Folder Cloud-Sync deaktivieren *(Samsung)*	Secure Folder → Einstellungen → Sicherung	2 Min.
Samsung Internet Datenschutz aktivieren *(Samsung)*	Samsung Internet → Einstellungen → Datenschutz	5 Min.
MAC-Adress-Randomisierung prüfen	Einstellungen → WLAN → [Netzwerk] → Datenschutz	5 Min.
Gboard durch OpenBoard ersetzen	Einstellungen → Allg. Verwaltung → Tastatur	5 Min.

5.4 WAS DIESE ANLEITUNG LEISTET - UND WAS NICHT

Diese Maßnahmen reduzieren die Datensammlung durch Google und Samsung erheblich. Sie eliminieren sie nicht vollständig. Beide Unternehmen erfassen weiterhin IP-Adressen, aggregierte Nutzungsdaten und Gerätekennungen, auch ohne Konto-Verknüpfung und auch bei deaktivierten Einstellungen, da Google Play Services und Samsung-Systemdienste privilegierten Systemzugriff haben, der durch normale Einstellungen nicht vollständig eingeschränkt werden kann.

Für weitergehenden Schutz sind strukturelle Maßnahmen erforderlich, die über diese Anleitung hinausgehen:

Der **Wechsel zu datenschutzfreundlichen Diensten** - Proton-Mail statt Gmail, Proton VPN statt ungeschützter Verbindung, Brave Search statt Google Search - reduziert die Datenmenge, die Google überhaupt erfassen kann, weil weniger Aktivitäten über Google-Infrastruktur laufen.

Die **Nutzung eines VPN** verschleiert die IP-Adresse gegenüber Websites und dem Mobilfunkanbieter, schützt aber nicht vor Tracking durch eingeloggte Google- oder Samsung-Konten.

Der **Wechsel zu einem Custom ROM** wie GrapheneOS (für Google Pixel-Geräte) oder iodé OS ist die konsequenteste Lösung: Es enthält keine Google-Dienste und bietet deutlich mehr Kontrolle über alle Systemfunktionen. Der Aufwand ist erheblich und setzt technisches Verständnis voraus. Für die meisten Nutzer ist dies kein realistischer erster Schritt, aber ein möglicher zweiter.

Die vorliegende Anleitung ist als **erster und wichtigster Schritt** zu verstehen: Sie bietet innerhalb des bestehenden Ökosystems den größtmöglichen Schutz, ohne einen vollständigen Systemwechsel vorauszusetzen. Wer alle SOFORT-Maßnahmen umsetzt, hat in 30 Minuten mehr für seine digitale Privatsphäre getan als die überwiegende Mehrheit der Smartphone-Nutzer.

6 Praxishandbuch und Tactical Briefings

6.1 ÜBER DAS „PRAKTISCHE HANDBUCH DER GEGENMAßNAHMEN“

Das „Praktische Handbuch der Gegenmaßnahmen“ ist ein mehrbändiges, praxisorientiertes Gesamtwerk. Grundlage sind mehrjährige Recherche sowie Austausch mit Fachleuten unterschiedlicher Disziplinen.

Zielgruppe sind Menschen, die in einer komplexen, krisenanfälligen und zunehmend digitalisierten Umwelt ihre Selbstverantwortung, Handlungsfähigkeit und Autonomie sichern wollen.

Der Ansatz ist operativ, nicht theoretisch.

Der Fokus liegt auf umsetzbaren Strategien für den Alltag, ohne ideologische Ausschweifungen.

Das Werk erscheint ab 2026 in vier unabhängig nutzbaren Bänden:

- Bd. 1: Digitaler Widerstand (April 2026)
- Bd. 2: Resilienz und Vorsorge (Oktober 2026)
- Bd. 3: Manipulationsabwehr (Frühjahr 2027)
- Bd. 4: Zeitgemäße Männlichkeit (Herbst 2027)

Jeder Band behandelt einen eigenständigen Handlungsraum.

Gemeinsame Leitlinie:

- Analyse der Lage
- Definition von Gegenmaßnahmen
- Umsetzung im Alltag

Dieses Tactical Briefing gehört zu „Band 1: Digitaler Widerstand - So schützen Sie Ihre Privatsphäre, Ihre Daten und Ihre Familie vor digitaler Ausbeutung, digitalen Angriffen und totaler Kontrolle “

Das Buch richtet sich nicht an Hacker oder IT-Experten, sondern an ganz normale Nutzer von Android-Smartphones und Windows-Computern.

In einer digital vernetzten Welt aus sozialen Medien, Cloud-Diensten und Künstlicher Intelligenz wachsen Datensammlung und -analyse rasant und mit ihnen die Risiken von Datenmissbrauch, Identitätsdiebstahl, Datenlecks und gezielter Manipulation. Durch Profiling und Scoring entsteht aus Ihrer Internet-, E-Mail- und Social-Media-Nutzung automatisch ein digitales Nutzerprofil, das erfasst und ausgewertet wird und dazu dient, Ihr Verhalten vorherzusagen und zu beeinflussen. Für Konzerne wie Google oder Meta sind Sie dabei nicht Kunde, sondern Datenquelle.

Ihr digitales Profil kann darüber entscheiden, welche Job-, Wohnungs- oder Kreditchancen Sie haben, welche Preise Ihnen angezeigt werden oder was Sie für Flüge und Versicherungen bezahlen. Umso wichtiger ist es, digitale Spuren zu minimieren und die Kontrolle über die eigenen Daten zu behalten.

Darüber hinaus plädiert das Buch für eine verantwortungsvolle, respektvolle und rechtlich bewusste Nutzung sozialer Medien. Es zeigt, wie Sie Ihre Meinungsfreiheit ausüben können, ohne unnötige persönliche oder strafrechtliche Risiken einzugehen und wie Sie bei einer Hausdurchsuchung die Ruhe bewahren und Ihre Freiheitsrechte schützen können.

Ergänzend zeigt das Buch, wie aktuelle Gesetzesvorhaben der EU und der Bundesregierung Privatsphäre, Freiheitsrechte und Meinungsfreiheit gefährden können.

6.2 ÜBER DIE „TACTICAL BRIEFINGS“

Die Reihe „Tactical Briefings“ ist eine Serie kleiner eBooks, die jeweils ein einziges Thema aus dem „Praktischen Handbuch der Gegenmaßnahmen“ komprimiert und praxisgerecht im Stil professioneller Einsatzdokumente aufbereiten.

Dabei stehen der praktische Nutzen und die sofortige Umsetzbarkeit im Vordergrund.

Weitere Infos und Bücher finden Sie auf meiner Website:

https://edno-chovak.com

6.3 HAFTUNGSAUSSCHLUß

- Alle Informationen in diesem Practical Briefing sind sorgfältig recherchiert, die Anleitungen praxiserprobt. Ich übernehme jedoch keine Gewähr für Aktualität, Korrektheit, Vollständigkeit und Qualität der bereitgestellten Informationen oder die Eignung für einen bestimmten Zweck. Insbesondere, weil ich nicht weiß, wie Ihr individuelles Gerät konfiguriert ist und wie Sie es benutzen. Das Practical Briefing kann eine individuelle Beratung durch einen professionellen Spezialisten für IT-Sicherheit nicht ersetzen. Die Verwendung des Buches und der darin enthaltenen Informationen erfolgt daher auf Ihr eigenes Risiko.