Edno Chovak

PRACTICAL HANDBOOK OF COUNTERMEASURES

TACTICAL BRIEFING | I-TB-06-01

Digital Self-Defense on Android and Samsung

The Complete Privacy Guide

Version 1.0

Imprint

Practical Handbook of Countermeasures –
Tactical Briefing BF-06-01: Digital Self-Defense on Android and Samsung - The Complete Privacy Guide
Version 1.0 – First Edition in English language 2026

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

Filename: TB-I-BF-06-01-v1_en_DigitalSelfDefenseonAndroidandSamsung.pdf
Prüfsummenverifizierungsdatei: TB-I-BF-06-01-v1_de_CHKSUM.txt

Table of Contents

Digital Self-Defense on Android and Samsung – The Complete Privacy Guide

Audience: Users of a Samsung Galaxy smartphone (or any other Android device) with a Google account, YouTube usage, Google sign-in on third-party websites, and - for Samsung device owners - a Samsung account.

Time required: Approximately 2–3 hours for all measures; the most critical immediate steps can be completed in under 30 minutes.

Structure: This guide works from the outside in - starting at the account level, moving through the operating system, and then covering Samsung-specific services - closing with a complete prioritized action list.

A note on the data landscape: Anyone using a Samsung smartphone with a Google account is dealing with at least two parallel data collectors. Google captures activity through the operating system and its apps; Samsung captures usage data through One UI, the Samsung account, and its own services. Both are legitimate companies operating within the terms of their privacy policies, but those policies permit substantially more data collection than most users realize. The measures below systematically reduce that collection without compromising the core functionality of your device**.**

1 Situational Overview

Digital threats don't start with an attack. They start with data collection. Search histories, location data, click patterns, and metadata are aggregated into behavioral profiles from which systems draw conclusions that you never disclosed-about your income, health, political beliefs. The real target is not your device. It's the predictive model of your behavior.

Surveillance is harmful, even if nothing happens. The chilling effect, learned helplessness, and chronic background stress are measurable psychological consequences, long before any concrete damage occurs. And: Digital traces outlive governments. What is legal today can be used against you tomorrow.

Your devices and services are not designed for data protection in their default configuration. The leakage of personal information is the norm, not the exception.

Consequence: You need to take action yourself. Every protective measure reduces your vulnerability, strengthens your digital self-determination, and has a proven positive effect on your mental well-being. Those who protect themselves also protect others-data protection is a social good**.**

This tactical briefing shows you exactly how to do this.

1.1 FOCUS OF THIS TACTICAL BRIEFING

PA-I-4	Privacy protection
TF-06	Mobile Usage
IMME-DI-ATELY	Minimizing the database for metadata analysis

Smartphones are the most personal and, at the same time, the most closely monitored devices in our digital everyday lives. They know your location, your contacts, your habits, your health data, and your communications. The default configuration of Android and iOS is optimized for data collection.

Operational guideline
The smartphone is the most comprehensive surveillance device that has ever existed-and you carry it around with you voluntarily. Any restriction on data collection is a gain in personal sovereignty.

2 Your Google Account – Activity, History, and Advertising

Your Google account is the most important starting point because it is where the largest volume of data is centrally stored and managed. All settings in this section are accessible at myaccount.google.com - best accessed from a desktop browser, where the interface is more complete. On your Android phone, you can also reach these settings via **Settings → Google → Manage your Google Account**.

2.1 ACTIVITY CONTROLS: WHAT GOOGLE STORES ABOUT YOU

The "Data & privacy" section at myaccount.google.com/activitycontrols is the most comprehensive data source in your Google account. This is where you decide which activity data Google permanently associates with your account.

Web & App Activity is enabled by default and captures every search query, every visit to a website that uses Google services, every tap within Google apps, and all activity in apps that use Google Analytics or Firebase - including voice searches via Google Assistant. Click on this entry and turn off the toggle. Confirm by selecting "Pause." Then click "Manage all Web & App Activity," select "Delete → All time → All products → Delete." Within this setting, also uncheck the sub-option "Include Chrome history and activity from sites, apps, and devices that use Google services" - this option allows Google to capture your browsing history even outside of Google-owned properties.

Location History stores a precise timeline of your movements based on GPS, Wi-Fi networks, and cell towers. This data is visualized in "Google Maps Timeline" and is often startlingly detailed: where you were, when, for how long, and which route you took. Turn off the toggle and delete all stored location data by selecting "Delete all Location History."

YouTube History is stored separately and includes both search history and watch history. This data is used to build a detailed profile of your interests, political leanings, and daily habits. Turn off both sub-options - "YouTube Search History" and "YouTube Watch History" - separately, and delete the existing data. As a middle ground if you want to keep some recommendation functionality: set up "Auto-delete" with a three-month window so data is regularly purged.

For all remaining activity categories, set up **auto-delete**: open each category and select "Auto-delete → Delete activity older than 3 months." This ensures that any data collected despite your other settings is periodically cleared.

2.2 TURN OFF AD PERSONALIZATION

Open adssettings.google.com. Google builds an advertising profile based on your activity that includes estimated age, gender, interests, profession, and purchase intent. This profile is used not only within Google's own services but across the entire Google Display Network - meaning ads on millions of third-party websites. Click on "Ad personalization" and turn off the toggle. Scroll down and manually delete all stored interest categories, as they persist even after personalization is disabled.

On your Android phone, there is an additional advertising identifier, the Android Advertising ID, that apps use to track your behavior across different apps. Open **Settings** → **Google** → **Ads** (or on newer Android versions: **Settings** → **Privacy** → **Ads**) and select "Delete advertising ID." On Android 12 and later, you can disable the advertising ID entirely.

2.3 CLEAN UP THIRD-PARTY APP ACCESS

Open myaccount.google.com/permissions. This page shows every app, website, and service that has been granted access to your Google account. This section is often surprisingly extensive - many users find services here they haven't used in years. Go through every entry and remove access for any service you haven't actively used within the past six months. Pay particular attention to entries with broad permissions such as "View all your Google Account data" or "Send email on your behalf."

2.4 SECURITY: ACTIVE SIGN-INS, SECURITY CHECKUP, AND TWO-FACTOR AUTHENTICATION

Open myaccount.google.com/security. Under "Your devices," you'll see every device currently signed in to your Google account. Review each entry and sign out of any device you no longer own or don't recognize.

Run the built-in Security Checkup at myaccount.google.com/security-checkup. It surfaces compromised passwords, insecure third-party access, and outdated recovery options.

If you haven't already: **enable** two-factor authentication at **Security** → **How you sign in to Google** → **2-Step Verification**. Critically, do not choose SMS as your second factor - SMS is vulnerable to SIM-swapping attacks, where an attacker convinces your carrier to transfer your phone number to a new SIM card and then intercepts your 2FA codes. This attack has been used to drain cryptocurrency wallets, hijack social media accounts, and bypass banking security across the US. Use an authenticator app instead: **Proton Authenticator**, **Google Authenticator**, or the open-source **Aegis Authenticator** (Android only) are all solid choices.

2.5 PERSONAL INFO, GOOGLE SEARCH, AND CHROME

Open myaccount.google.com/personal-info and remove any information not strictly required for account functionality - particularly date of birth, gender, and home address. Your phone number is useful for 2FA recovery but should not be used for advertising: check under **Personal info** → **Phone** → **What this number is used for** and make sure "Personalized ads" is not checked.

If you use Google Chrome: open **Chrome** → **Settings** → **Sync and Google services** and turn off sync for any categories you don't need - particularly "History" and "Open tabs." Under "Other Google services," disable "Help improve Chrome's features and performance" and "Make searches and browsing better." For the long term, switching to a more privacy-respecting browser like Brave is recommended (see Section 4.1).

2.6 YOUTUBE PRIVACY AND GOOGLE ASSISTANT

Open YouTube and navigate to **Your account** → **Settings** → **Privacy**. Disable all three options: "Keep all my subscriptions private," "Keep all my saved playlists private," and "Keep all my liked videos and saved playlists private." These settings expose information about your interests and habits to anyone who visits your profile.

For Google Assistant: open the **Google app** → **your profile picture** → **Settings** → **Google Assistant**. Either disable Google Assistant entirely under "General," or restrict all data access under "Data & privacy": turn off "Web & App Activity," "Improve voice models for everyone," and all personalized results. For Google Gemini: open **Google app** → **profile picture** → **Manage your Google Account** → **Data & privacy** → **Gemini Apps Activity**, turn it off, and delete all stored activity.

3 The Android Operating System – Network, Permissions, and System Services

This section covers settings made directly within the Android operating system - independent of your Google account. All settings are in the Settings app on your device. Exact menu names may vary slightly by manufacturer and Android version, but the structure is consistent.

3.1 SECURE YOUR NETWORK CONNECTIONS

Private DNS is one of the most effective and least-known privacy measures available. Every DNS query - meaning every time your phone resolves a domain name - is sent unencrypted to your carrier's DNS server by default. Your carrier can use this to build a complete log of every domain you visit, even when the actual content is transmitted over an encrypted HTTPS connection. Open **Settings** → **Network & internet** → **Private DNS**, select "Private DNS provider hostname," and enter dns.quad9.net (Quad9, based in Switzerland, blocks known malware domains) or dns.adguard.com (additionally blocks tracking and advertising domains). From this point forward, all DNS queries are transmitted encrypted via DNS-over-TLS.

IMSI-catcher protection: IMSI-catchers (also called "Stingrays") are devices that impersonate cell towers and trick nearby phones into connecting to them. They are used by law enforcement agencies and, in some cases, by private actors to intercept location data and communications. They frequently exploit the outdated 2G protocol, which lacks mutual authentication. Open **Settings** → **Network & internet** → **SIMs** → **Require encryption** and enable "Require encrypted connections" and "2G protection" (available on Pixel devices running Android 12 and later; on other manufacturers, look for similar options under network security settings).

MAC address randomization: Every Wi-Fi device broadcasts its MAC address, a unique hardware identifier, when scanning for known networks. Wi-Fi network operators can use this address to track your movements across different locations. Open **Settings** → **Wi-Fi**, tap each saved network, and verify that "Privacy" is set to "Use randomized MAC." This feature is enabled by default from Android 10 onward, but it's worth checking all saved networks, especially older ones.

Disable Wi-Fi and Bluetooth background scanning: Android allows apps and the system to scan for networks and devices even when Wi-Fi and Bluetooth are turned off, for location determination purposes. Open **Settings** → **Location** → **Location services** and disable both "Wi-Fi scanning" and "Bluetooth scanning."

Bluetooth and NFC should be turned off when not actively in use. Bluetooth enables tracking through beacons deployed in retail stores, airports, and public spaces; NFC can be exploited in certain proximity attacks. Use the Quick Settings panel for fast toggling; for NFC: **Settings** → **Connected devices** → **Connection preferences** → **NFC**.

3.2 SYSTEMATICALLY REVIEW APP PERMISSIONS

The **Permission Manager** at **Settings** → **Privacy** → **Permission manager** displays all permissions by category and lists which apps have access to each. This is more efficient than opening each app individually. The following table provides guidance:

Permission	Risk Level	Recommendation
Location	Very high	"While using the app" only; never "Always" except for navigation
Microphone	Very high	"While using the app" only; disable for most apps
Camera	High	"While using the app" only; disable for non-camera apps
Contacts	High	Phone and messaging apps only; deny all others
Call logs	High	Phone app only
SMS	High	Default SMS app only
Body sensors	Medium	Fitness apps only
Calendar	Medium	Calendar apps only
Files and media	Medium	Grant restrictively
Nearby devices	Medium	Bluetooth-dependent apps only

Beyond standard permissions, there is **Special app access** at **Settings** → **Apps** → **Special app access**, which contains particularly far-reaching permissions that are frequently overlooked. Review in particular: "All files access" (file managers and backup apps only), "Device admin apps" (legitimate MDM solutions only), "Display over other apps" (a known attack vector for clickjacking - restrict to a small number of trusted apps), "Install unknown apps" (should be disabled for all apps), and "Access to premium SMS" (should not be granted to any app).

Starting with Android 12, in most devices there is a **global camera and microphone toggle** in the Quick Settings panel (swipe down twice from the top). Disable both and enable them only temporarily when an app needs them. Alternatively: **Settings** → **Privacy** → **Camera access / Microphone access**.

3.3 PRIVACY DASHBOARD, DIAGNOSTICS, AND SYSTEM SERVICES

The Privacy Dashboard at **Settings** → **Privacy** → **Privacy dashboard** (Android 12 and later) shows which apps accessed sensitive permissions within the last 24 hours. Check it regularly, particularly for location, microphone, and camera access. If an app accessed a permission you didn't expect, revoke it immediately.

Android sends usage statistics and diagnostic data to Google by default. Open **Settings** → **Privacy** → **Usage & diagnostics** and turn off all options. Also open **Settings** → **Google** → **More settings** → **Usage & diagnostics**: this second channel is frequently overlooked and operates independently.

Android System Intelligence - the service behind keyboard suggestions, Smart Reply, and automatic text recognition - analyzes your communication content and sends data to Google. Open Settings → Privacy → Advanced and disable "Personalize using app data." Tap on "Android System Intelligence" and disable "Customize using Google account data."

The Autofill service at Settings → Privacy → Autofill service fills in passwords and credit card information. If this service is set to Google, your credentials are synchronized with Google's servers. Switch to a privacy-respecting password manager such as Proton Pass or Bitwarden. Install the app first, then it will appear as an option in the Autofill service setting.

Health Connect at Settings → Privacy → Health Connect is Google's central interface for health and fitness data. Under "App permissions," review which apps have read and write access to which data categories, and revoke access for any that don't need it.

3.4 DEVICE SECURITY

Your screen lock is the most important physical security measure. Use a PIN with at least six digits or an alphanumeric password. If you use fingerprint or face unlock, be aware: in some US jurisdictions, courts have ruled that law enforcement can compel biometric unlocking but cannot compel you to reveal a PIN or password. Enable the option to require your PIN after every restart, so biometric unlock is not available immediately after a reboot.

Activate the SIM card PIN at **Settings** → **Security** → **SIM card lock**. Change the default PIN (typically 0000 or 1234) to a unique PIN of at least six digits. This prevents a stolen SIM card from being used in another device: a critical defense against SIM-swapping attacks.

Make sure automatic security updates are enabled: **Settings** → **System** → **System update**. Devices that haven't received a security patch in more than six months are significantly more vulnerable to known exploits. If your device manufacturer has stopped issuing security updates, this is a strong signal to consider upgrading your hardware.

3.5 REPLACE DEFAULT APPS

Replace Chrome: Google Chrome, even in Incognito mode, is a comprehensive tracking tool. In 2024, Google settled a class-action lawsuit and agreed to destroy billions of data records collected in Incognito mode, confirming that Incognito does not mean private. Recommended alternatives: Brave Browser (blocks trackers and ads by default, supports all Chrome extensions) or Firefox with the uBlock Origin and Privacy Badger extensions. To set your default browser: **Settings** → **Apps** → **Default apps** → **Browser app**.

Replace your search engine: Google Search is a tracking instrument even without a signed-in account. Switch to Brave Search (independent index, no Google tracking) or DuckDuckGo. The default search engine is set directly within your browser settings.

Replace Gboard: Google's default keyboard sends typing patterns and words to Google's servers for model improvement. Install OpenBoard (open source, fully offline) or FlorisBoard as a replacement. To set your default keyboard: **Settings** → **General management** → **Keyboard list and default** → **Default keyboard**.

Restrict lock screen notification previews: Open **Settings** → **Notifications** → **Lock screen notifications** and select "Hide sensitive content." This prevents 2FA codes, messages, and emails from being displayed on your locked screen, a simple but effective defense against shoulder surfing.

Restrict Google Backup: Android's backup feature syncs app data, Wi-Fi passwords, and device settings to Google Drive by default. Open **Settings** → **System** → **Backup** and review what is being backed up. If you don't want Google to hold your backup, disable "Back up to Google Drive." Note that without a backup, all app data will be lost if your device is lost or reset. Consider Proton Drive as an alternative for document and photo backup.

4 Samsung One UI - The Second Ecosystem

Samsung users are dealing with a second, often overlooked data collector. One UI is not a neutral Android skin - it is a full ecosystem with its own services, its own data infrastructure, and its own AI features. The Samsung account is governed by South Korean law (PIPA - Personal Information Protection Act), which in some respects provides less stringent protections than US state privacy laws such as the California Consumer Privacy Act (CCPA).

4.1 CLEAN UP YOUR SAMSUNG ACCOUNT

The Samsung account links device usage, app purchases from the Galaxy Store, Samsung Health data, location data through Find My Mobile, and AI activity through Galaxy AI. Samsung's privacy policy states that data is shared with "business partners" - including advertising partners and analytics providers.

Restrict sync: Open **Settings** → **Samsung account** → **[your account]** → **Sync account** and disable all categories you don't actively need: Samsung Cloud backup, Samsung Internet bookmarks, Samsung Notes, Samsung Health data, and Calendar, particularly if you're using alternative services for any of these.

Account privacy settings: Open **Settings** → **Samsung account** → **Privacy** and disable "Personalized service" (Samsung uses this for cross-device advertising analysis), "Send diagnostic data," and "Receive marketing information." Also open account.samsung.com in a browser and check under "Privacy" what data Samsung has stored. Samsung provides options to view, download, and delete your data there.

4.2 SAMSUNG'S BUILT-IN DATA COLLECTION

Samsung operates several background data collection services that are not always visible through standard settings menus.

The Samsung Customization Service (com.samsung.android.rubin.app) collects usage data and sends it to Samsung for "personalized recommendations." Open **Settings** → **Apps** → **See all apps** and search for "Customization Service". Tap it and select "Disable." Alternatively: **Settings** → **Privacy** → **Advanced privacy** → **Customization service**.

The Samsung Push Service (com.sec.spp.push) is used not only for legitimate notifications but also for displaying advertisements in Samsung-owned apps and push notifications. Open **Settings** → **Apps** → **See all apps** → **Samsung Push Service** → **Disable** (only if you don't use the Galaxy Store or Samsung Pay, as those depend on this service).

Samsung sends diagnostic data through three separate channels, in addition to Google's diagnostic data. Disable all three: **Settings** → **Privacy** → **Send diagnostic data**, **Settings** → **General management** → **Diagnostics**, and **Settings** → **Samsung account** → **Privacy** → **Send diagnostic data**.

Samsung displays advertising in several pre-installed apps: on the lock screen (Samsung Free), in the Gallery app, and in the Weather app. Open **Settings** → **Privacy** → **Marketing information** and disable all options. For the lock screen: swipe right to Samsung Free, tap the three-dot menu, and select **Settings** → **Turn off page**.

4.3 BIXBY - SAMSUNG'S VOICE ASSISTANT

Bixby has access to your microphone, contacts, calendar, messages, call logs, location, and - with Bixby Vision enabled - your camera. According to Samsung's privacy policy, voice recordings are "encrypted and sent to servers" and used to improve the speech model. The retention period is not fully transparent in Samsung's public documentation.

Disable Bixby: Open the **Bixby app** → **three-dot menu** → **Settings** → **Bixby Voice** → **Turn off Bixby**. For the side button: Settings → **Advanced features** → **Side button** and change the assignment. Also disable Bixby Routines at **Settings** → **Advanced features** → **Bixby Routines**.

Delete Bixby voice data: Open account.samsung.com → Privacy → Manage my data → Bixby data and delete all stored voice recordings and activity data.

4.4 GALAXY AI - ON-DEVICE OR CLOUD?

Galaxy AI uses a hybrid processing model. The following table shows which features run locally on your device and which send data to external servers:

Feature	Processing	Privacy Risk
Live Translate (calls)	On-device	Low
Chat translation	On-device	Low
Writing style & grammar	On-device	Low
Transcript Assist (basic)	On-device	Low
Photo Remaster (basic)	On-device	Low
Generative Edit (photos)	Cloud (Samsung)	High
Sketch to Image	Cloud (Samsung)	High
Note Assist (summarization)	Cloud (Samsung)	High
Browsing Assist	Cloud (Samsung)	High
Circle to Search	Cloud (Google)	Very high
Portrait Studio	Cloud (Samsung)	High

Restrict Galaxy AI to on-device processing: Open **Settings** → **Galaxy AI** (or **Settings** → **Advanced features** → **Advanced intelligence**) and enable "Process data only on device." This disables all cloud-based AI features while keeping on-device features available.

Disable Circle to Search separately: This Google integration cannot be disabled through the Galaxy AI settings. Open **Settings** → **Advanced features** → **Circle to Search** and turn off the toggle.

4.5 PRE-INSTALLED APPS AND BLOATWARE

Samsung devices ship with a significant number of pre-installed apps that cannot be uninstalled but can be disabled. Open Settings → Apps → See all apps, tap the relevant app, and select "Disable." The following table lists apps that are safe to disable for most users:

App	Privacy Concern
Samsung Free	Usage profiling, lock screen ads
Samsung TV Plus	Usage data, advertising
Samsung Global Goals	Background advertising
Bixby Voice	Voice data sent to Samsung servers
Bixby Routines	Access to extensive device data
Samsung Push Service	Ads in notifications
Samsung Customization Service	Usage profiling
Samsung Location SDK	Location data for Samsung apps
Game Launcher	Usage statistics
AR Zone	Camera data

For apps that cannot be disabled through the standard settings, the Android Debug Bridge (ADB) tool is required. Connect your device to a computer (USB debugging must be enabled: Settings → Developer options → USB debugging) and run:

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

Commonly disabled packages: com.samsung.android.rubin.app (Customization Service), com.sec.spp.push (Push Service), com.samsung.android.app.spage (Samsung Free). Any deactivation can be reversed with adb shell pm enable <package_name>.

Important: Never disable Knox-related packages (com.samsung.android.knox.*) or the Secure Folder. These are security-critical components and disabling them can render the device unbootable.

4.6 SAMSUNG INTERNET BROWSER

Samsung Internet offers better privacy options than Google Chrome - provided they are manually enabled. Open **Samsung Internet → three-line menu → Settings → Privacy and security** and enable: "Smart anti-tracking," an ad blocker (such as AdGuard), "Send 'Do Not Track' requests," and "Block malicious sites." Disable: "Use browsing data for personalized recommendations" and "Share Samsung browsing data for improvements."

For the Incognito mode: enable a PIN or biometric lock for Secret Mode under **Settings → Privacy and security → Use Secret mode lock**. This prevents others from accessing your private browsing sessions if they pick up your phone.

4.7 SAMSUNG HEALTH AND WEARABLES

Samsung Health collects step count data, heart rate, sleep patterns, weight, nutrition data, and - with a Galaxy Watch or Galaxy Ring - continuous biometric measurements. Health data is among the most sensitive data categories: it can be used by insurers, employers, or government agencies, and once exposed in a data breach, it cannot be changed.

Open **Samsung Health → your profile picture → Settings → Privacy** and disable "Share data with Samsung" and "Share research data." Under "Connected services," review which third-party apps have access to your health data. For Galaxy Watch and Ring: open **Galaxy Wearable → Settings → Privacy** and disable "Send diagnostic data."

4.8 KNOX AND SECURE FOLDER

Samsung Knox is Samsung's proprietary security framework that provides a hardware-level secure enclave for sensitive data. Knox is generally a security benefit, it prevents malware from accessing sensitive data. At the same time, Knox is a proprietary, non-auditable system.

Open **Settings → Security and privacy → Knox settings** and check whether "Knox Matrix" is enabled. This feature synchronizes security status across multiple Samsung devices on the same Samsung account. If you only use one device, you can disable Knox Matrix.

If you use Secure Folder: make sure sync with Samsung Cloud is disabled: **Secure Folder → Settings → Backup and restore → Samsung Cloud sync** → Disable.

5 Complete Action List by Priority

The following tables consolidate all measures from the three sections above, organized by priority. The Immediate Actions can be completed in approximately 30 minutes and have the greatest impact.

5.1 IMMEDIATE ACTIONS (APPROXIMATELY 30 MINUTES)

Action	Path	Time
Disable + delete Web & App Activity	myaccount.google.com/activitycontrols	5 min.
Disable + delete YouTube History	myaccount.google.com/activitycontrols	3 min.
Disable + delete Location History	myaccount.google.com/activitycontrols	3 min.
Clean up third-party app access	myaccount.google.com/permissions	10 min.
Delete Android Advertising ID	Settings → Google → Ads	2 min.
Enable 2FA with authenticator app	myaccount.google.com/security	5 min.
Restrict Galaxy AI to on-device (Samsung)	Settings → Galaxy AI	2 min.
Disable Circle to Search (Samsung)	Settings → Advanced features → Circle to Search	1 min.
Disable Bixby (Samsung)	Bixby app → Settings	3 min.
Disable Samsung diagnostics (all 3 channels) (Samsung)	Settings → Privacy / Samsung account / General management	5 min.

5.2 HIGH-PRIORITY ACTIONS (APPROXIMATELY 45 MINUTES)

Action	Path	Time
Turn off personalized ads	adssettings.google.com	3 min.

Action	Path	Time
Systematically review app permissions	Settings → Privacy → Permission manager	15 min.
Set up Private DNS	Settings → Network & internet → Private DNS	2 min.
Disable Wi-Fi/Bluetooth background scanning	Settings → Location → Location services	2 min.
Enable global camera/mic toggle	Quick Settings panel	1 min.
Switch Autofill to a password manager	Settings → Privacy → Autofill service	5 min.
Disable Android usage & diagnostics	Settings → Privacy → Usage & diagnostics	3 min.
Restrict Samsung account sync (Samsung)	Settings → Samsung account → Sync account	5 min.
Disable Samsung Customization Service (Samsung)	Settings → Apps → Customization Service	2 min.
Disable Samsung Push Service (Samsung)	Settings → Apps → Samsung Push Service	2 min.
Disable Samsung Free (Samsung)	Lock screen → swipe right → Settings	2 min.
Disable ads in Samsung apps (Samsung)	Settings → Privacy → Marketing information	2 min.
Restrict Samsung Health data sharing (Samsung)	Samsung Health → Privacy	3 min.
Activate SIM card PIN	Settings → Security → SIM card lock	2 min.
Restrict lock screen notification previews	Settings → Notifications → Lock screen	2 min.

5.3 MEDIUM-PRIORITY ACTIONS (APPROXIMATELY 45 MINUTES)

Action	Path	Time
Set up auto-delete (3 months)	myaccount.google.com/activitycontrols	5 min.

Action	Path	Time
Restrict Chrome sync	Chrome → Settings → Sync	5 min.
Clean up personal info in Google account	myaccount.google.com/personal-info	5 min.
Review Special app access	Settings → Apps → Special app access	10 min.
Review Health Connect	Settings → Privacy → Health Connect	5 min.
Restrict Google Backup	Settings → System → Backup	3 min.
Review contact sync	Settings → Accounts → Google → Sync	3 min.
Configure Google Photos backup	Google Photos → Photo storage settings	3 min.
Review Samsung account privacy at account.samsung.com (Samsung)	account.samsung.com	10 min.
Delete Bixby voice data (Samsung)	account.samsung.com → Privacy → Bixby data	5 min.
Disable Knox Matrix (Samsung)	Settings → Knox settings	2 min.
Disable Secure Folder cloud sync (Samsung)	Secure Folder → Settings → Backup	2 min.
Enable Samsung Internet privacy settings (Samsung)	Samsung Internet → Settings → Privacy	5 min.
Verify MAC address randomization	Settings → Wi-Fi → [network] → Privacy	5 min.
Replace Gboard with OpenBoard	Settings → General management → Keyboard	5 min.

5.4 WHAT THIS GUIDE ACHIEVES — AND WHAT IT DOESN'T

The measures in this guide substantially reduce data collection by Google and Samsung. They do not eliminate it entirely. Both companies continue to capture IP addresses, aggregated usage data, and device identifiers — even without account linkage and even with the settings above configured — because Google Play Services and Samsung system services operate with privileged system access that normal user-facing settings cannot fully restrict.

For deeper protection, structural changes are necessary that go beyond what this guide covers.

Switching to privacy-respecting services - Proton Mail instead of Gmail, Proton VPN instead of an unprotected connection, Brave Search instead of Google Search - reduces the amount of data Google can collect in the first place, because fewer activities run through Google infrastructure.

Using a VPN conceals your IP address from websites and your carrier, but does not protect against tracking through signed-in Google or Samsung accounts.

Switching to a custom ROM such as iodé, GrapheneOS (available for Google Pixel devices) is the most thorough solution: it contains no Google services and provides significantly more control over all system functions. The setup process is substantial and requires technical knowledge. For most users it is not a realistic first step, but it is a viable second step for those who want to go further.

This guide should be understood as the first and most important step: it provides the maximum available protection within the existing ecosystem, without requiring a complete platform migration. **Anyone who completes the Immediate Actions list has done more for their digital privacy in 30 minutes than the vast majority of smartphone users ever will.**

6 Practical Handbook and Tactical Briefings

6.1 ABOUT THE "PRACTICAL HANDBOOK OF COUNTER-MEASURES"

The "Practical Handbook of Countermeasures" is a multi-volume, practice-oriented complete work. It is based on several years of research and exchange with experts from various disciplines.

The target group is people who want to secure their self-responsibility, ability to act, and autonomy in a complex, crisis-prone, and increasingly digitized environment.

The approach is operational, not theoretical.

The focus is on implementable strategies for everyday life, without ideological digressions.

The work will be published from 2026 in four independently usable volumes:

- Vol. 1: Digital Resistance (April 2026)
- Vol. 2: Resilience and Preparedness (October 2026)
- Vol. 3: Manipulation Defense (Spring 2027)
- Vol. 4: Contemporary Masculinity (Fall 2027)

Each volume deals with an independent area of action.

Common Guideline:

- Analysis of the situation.
- Definition of countermeasures.
- Implementation in everyday life.

This Tactical Briefing belongs to "Volume 1: Digital Resistance"

The book is not aimed at hackers or IT experts, but at ordinary users of smartphones and Windows computers.

In a digitally connected world of social media, cloud services, and artificial intelligence, data collection and analysis are growing rapidly, and with them the risks of data misuse, identity theft, data leaks, and targeted manipulation. Profiling and scoring automatically create a digital user profile from your internet, email, and social media usage, which is recorded and evaluated and used to predict and influence your behavior. For corporations such as Google or Meta, you are not a customer, but a source of data.

Your digital profile can determine what job, housing, or credit opportunities you have, what prices you are shown, or what you pay for flights and insurance. This makes it all the more important to minimize your digital footprint and maintain control over your own data.

In addition, the book advocates for responsible, respectful, and legally conscious use of social media. It shows how you can exercise your freedom of expression without taking unnecessary personal or criminal risks, and how you can remain calm during a search and seizure and protect your civil rights.

In addition, the book shows how current legislative proposals by the EU and the German government could jeopardize privacy, civil rights, and freedom of expression.

6.2 ABOUT THE "TACTICAL BRIEFINGS"

The "Tactical Briefings" series is a series of small eBooks, each of which condenses and prepares a single topic from the "Practical Handbook of Countermeasures" in a practical way in the style of professional operational documents.

The focus is on practical use and immediate implementability.

More information and books can be found on my website:

https://edno-chovak.com

6.3 DISCLAIMER

- All information in this Practical Briefing has been carefully researched, and the instructions have been tested in practice. However, I make no warranty regarding the timeliness, accuracy, completeness, or quality of the information provided, nor its suitability for any particular purpose. This is especially true because I do not know how your specific device is configured or how you use it. This Practical Briefing cannot replace individual consultation with a professional IT security specialist. Use of this book and the information contained herein is therefore at your own risk.