Privacy Policy — Spy Apps Detector

Effective Date: *March 27, 2026*

Last Updated: *August 4, 2026*

1. Introduction

Spy Apps Detector ("the App," "we," "our," or "us") is a security tool that helps you identify potentially harmful or privacy-threatening applications installed on your Android device. We are committed to protecting your privacy.

This Privacy Policy explains what information the App accesses, how it is used, when limited network contact with Google Play occurs, and your rights as a user.

By downloading or using Spy Apps Detector, you agree to the practices described in this Privacy Policy.

2. At a Glance

- *All scanning and risk analysis happen **entirely on your device***
- *Scan, permission, and risk data are **never uploaded** to any server we operate — there is **no company backend***
- *The App has **no user accounts, no logins, and no cloud storage** we operate*
- *The App uses **no advertising or analytics SDKs***
- *The App **does** use the network for limited Google Play services only: optional Premium subscriptions (Play Billing), in-app updates, in-app review, and opening links you choose (privacy policy, support, Play Store subscription management)*

3. Information Accessed On Your Device

*To perform its security function, the App reads the following information **directly from your device** (primarily via Android's PackageManager and related system APIs during each scan you start). This scan and risk data is processed locally and is **never transmitted over the network**.*

3.1 Installed App Metadata

When you run a scan, the App reads basic information about apps installed on your device, including:

- *App names and icons*
- *Declared / granted sensitive permissions (e.g., whether an app can access your microphone or camera)*
- *Installation source and install date*

- *Whether an app is visible or hidden on your device (launchable vs. no launcher icon)*
- *Whether an app holds elevated system access (Device Administrator or Accessibility Service)*
- *Whether an app is a system app or user-installed*
- *Computed on-device risk signals and risk level for display in the App*

*This information is used solely to evaluate and display security risks to you within the App. The live scan view is session-based. Separately, the App may keep a **local, on-device history of past scan snapshots** (see Section 5) so you can compare changes over time. That history never leaves your device.*

3.2 Optional: App Usage Information (Usage Access)

*If you grant **Usage Access** permission (optional, manually granted in Android Settings), the App may also read:*

- *When each app was last used*
- *Each app's storage size (where supported by the device)*

This additional information improves on-device scan signals (including certain Premium Deep Scan signals). It is processed entirely on your device, is not included in stored Compare Snapshot records, and is never transmitted.

4. How We Use This Information

*The App uses the information described above **only** to:*

1. *Display a list of installed apps and their on-device security assessment*
2. *Help you identify apps that may pose a privacy risk*
3. *Allow you to take action (such as opening Android's uninstall screen for a flagged app)*
4. *Optionally keep a local history of past scan snapshots so you can compare what changed between scans (new apps, permission changes, sideload status, and risk-level changes)*
5. *Power Premium on-device tools (when subscribed): Scan PDF Report, Compare Snapshot, Device Security Checkup, Deep Scan, and Permission Manager*

*The App does **not** use this information for advertising, analytics, profiling, or any purpose other than the security features you initiate on your device.*

5. Local Storage

*The App stores data **only on your device** (not on any server we operate). This includes:*

- *Preference settings such as whether you have completed the first-launch introduction, theme preference, whether you have enabled daily security reminders, and a counter used to rotate daily reminder messages*

- *Optional risk-related preferences you choose in the App (for example, apps you mark as safe, or apps you choose to keep monitoring), plus a compact local map of last-seen risk scores used for in-app display*
- *A local cache of Premium subscription entitlement status (active / inactive and product id) used for smoother UX; entitlement is re-checked with Google Play Billing on launch and periodically on resume (see Sections 7 and 9)*
- *Deep Scan preference (on/off) when you are a Premium subscriber*
- *An optional **local history of past scan snapshots** used by the Compare Snapshot feature. Each snapshot may include app names/labels, package names, granted sensitive permissions, whether an app is launchable/hidden, install source category, and the risk level assessed at that scan. Snapshots are capped at **2** recent scans (previous + current) and are stored on-device only — they are **never transmitted** anywhere. This history exists purely so you can compare changes over time. You can clear all snapshot history at any time from Compare Snapshot in the App*

This local data contains no payment card details and never leaves your device as scan/permission/risk content. Uninstalling the App or clearing the App's data in Android Settings removes it.

6. Information We Do Not Collect

*We do **not** collect or store:*

- *Your name, email address, phone number, or account credentials inside the App (there is no App account)*
- *Your location (GPS or network-based)*
- *Your contacts, messages, or call history*
- *Your photos, videos, or any media files*
- *Device advertising identifiers for advertising*
- *Payment card numbers or bank details (payments, if any, are handled by Google Play — see Section 7)*
- *The contents of any other application on your device*
- *Usage patterns or in-app behaviour analytics sent to us*
- *Crash reports or diagnostic data sent to servers we operate*

7. Subscriptions & Billing

*The App offers an optional **Spy App Detector Pro (Premium)** subscription with **monthly** and **yearly** plans.*

What Premium unlocks

When entitled, Premium unlocks these on-device tools:

- ***Scan PDF Report*** *— export and share a PDF of your latest scan via the system share sheet*
- ***Compare Snapshot*** *— compare recent on-device scan snapshots*
- ***Device Security Checkup*** *— on-device device security posture checks*
- ***Deep Scan*** *— enhanced on-device scan signals (for example overlay permission and related signals; some signals work better with optional Usage Access)*
- ***Permission Manager*** *— browse sensitive permissions and open system settings to revoke them*

How billing works

- *Subscriptions are processed **entirely through Google Play Billing**. The App never sees or stores your payment card details.*
- *Subscription status (active / inactive) is checked with Google Play's on-device Billing APIs. That check is a data flow to a **third party (Google)** for purchase and entitlement verification only.*
- *There is **no company-operated backend server**. Entitlement verification relies on Google Play Billing's on-device APIs. This App is fully serverless from our side.*
- *Subscriptions **auto-renew until cancelled**. You can manage or cancel anytime in Google Play's subscription settings. From within the App, Settings includes **Manage Subscription** (when subscribed) or **Upgrade to Premium**, which can open Play's subscription management page.*
- *You can also use **Restore Purchases** on the paywall to re-query Play for an existing entitlement on your Google account.*

Google's own handling of your Google account and payment methods is governed by Google's privacy policy and Play terms.

8. Network / Internet Use

*The App declares and **uses** the **INTERNET** permission. Network use is limited to:*

6. ***Google Play Billing*** *— loading subscription product prices, purchasing, acknowledging purchases, restoring purchases, and checking active subscription entitlement*
7. ***Google Play in-app updates*** *— checking for and downloading app updates through Play's update API*
8. ***Google Play in-app review*** *— showing Play's review prompt when eligible*
9. ***Opening external links you choose*** *— for example the privacy policy, support email compose, Play Store listing / developer page, and Play Store subscription management, in your browser or the Play Store app*

Scan results, installed-app lists, permissions, risk scores, Usage Access data, snapshots, Device Security Checkup results, and Permission Manager data are never transmitted over the network. *Only the limited billing, update, review, and user-initiated link interactions above contact Google's (or your chosen browser's) services.*

9. Permissions

The App's AndroidManifest declares the following permissions:

QUERY_ALL_PACKAGES

Allows the App to see all apps installed on your device. This is required to perform the core security scan. Without this permission, the App cannot function as designed. ***No app scan data is transmitted off-device.***

PACKAGE_USAGE_STATS

Allows the App to read when apps were last used and their storage size. This is ***optional****, user-granted in Android Settings, and used solely within the App to enhance scan / Deep Scan signals.* ***This data is never transmitted remotely.***

POST_NOTIFICATIONS

Allows the App to send you daily security reminders and related notifications if you choose to enable them. Notifications are generated entirely on-device.

SCHEDULE_EXACT_ALARM

Allows the App to schedule daily notifications at a consistent time on supported Android versions (declared for API 31–32). On newer Android versions the App checks exact-alarm availability at runtime and falls back when needed.

RECEIVE_BOOT_COMPLETED

Allows the App to reschedule daily reminders after your device restarts or timezone changes. Android cancels scheduled alarms on reboot; this permission helps reminders continue working.

REQUEST_DELETE_PACKAGES

Allows the App to open Android's built-in system uninstall screen when you choose to remove a flagged app. ***The App cannot uninstall any app silently or without your explicit confirmation.***

INTERNET

Used for Google Play Billing, Play in-app updates, Play in-app review, and opening external links you initiate (see Section 8). ***Not used to upload scan or permission data.***

(Play Billing Library may also merge Google's* ***com.android.vending.BILLING* *permission into the installed app for subscription processing. That permission is for Play Billing only.)**

10. Data Sharing With Third Parties

Scan, permission, risk, snapshot, and related security-analysis data are not shared with any third party.

*The only third-party data flows are with **Google Play** for:*

- *Subscription / purchase processing and entitlement checks (Play Billing)*
- *In-app update checks / downloads*
- *In-app review prompts*

and with services you explicitly open (browser, email app, or Play Store) when you tap links such as Privacy Policy, Contact Us, or Manage Subscription.

The App contains no advertising SDKs, no analytics SDKs, no crash-reporting services we operate, and no social media tracking integrations.

11. Third-Party Services

*Aside from **Google Play** (Billing, updates, and review) as described above, the App uses open-source and platform libraries for user interface and local functionality. Those libraries are not used to send your scan or permission data to external servers. We do not operate a cloud platform or analytics backend for this App.*

12. Children's Privacy

Spy Apps Detector is not directed at children under the age of 13. We do not knowingly collect personal information from children through the App. The App does not create accounts or request personal information from users.

If you are a parent or guardian with concerns, please contact us using the information in Section 16.

13. Data Security

We have designed the App with privacy and security in mind:

- *Scanning and risk analysis run on-device; scan/permission/risk content is not uploaded to servers we operate*
- *The App holds no user credentials or payment card data*
- *The App does not modify, write to, or read the private content of other installed apps — it reads metadata and system signals provided by Android's operating system (and optional Usage Access when granted)*
- *Daily reminders use scheduled notifications; there is no continuous spyware-style monitoring service*
- *Any uninstall action requires your explicit confirmation in the Android system dialog*
- *Optional Premium PDF reports are generated on-device and leave the device only if **you** share them through the system share sheet*

This App helps you review risk signals; it does not guarantee complete detection of all spyware or harmful software.

14. Data Retention

- ***Live scan results** in the current session exist in memory during your active use and are cleared when you close or reset the scan*
- ***Scan snapshots** (if any) are retained locally on your device, limited to **2** recent scans, until you clear them via Compare Snapshot, uninstall the App, or clear the App's data in Android Settings*
- ***Local preferences**, risk whitelist / monitor entries, risk-score history, and Premium entitlement cache are retained on your device until you change them, uninstall the App, or clear its data*
- ***Google Play** retains subscription and purchase records according to Google's policies; we do not operate a separate remote store of that data*
- *There is no remote scan database of ours to delete, because scan data is never stored on servers we operate*

15. Your Rights and Controls

You have full control over the App's behaviour:

***Revoke any permission** at any time via: Android Settings → Apps → Spy Apps Detector → Permissions*

***Disable notifications** via: Android Settings → Apps → Spy Apps Detector → Notifications, or within the App itself*

***Clear scan snapshot history** at any time via Compare Snapshot in the App (clear snapshot history)*

***Manage or cancel your Premium subscription** via Google Play (Payments & subscriptions), including the Manage Subscription entry in the App's Settings when you are subscribed*

***Delete all App data** by uninstalling the App or via: Android Settings → Apps → Spy Apps Detector → Storage → Clear Data*

Uninstalling the App removes all local App data from your device. Cancelling a subscription is done through Google Play and does not by itself erase local preferences until you clear data or uninstall.

16. Contact Us

If you have questions or concerns about this Privacy Policy, please contact us:

***Email:** shahrozkhalid999@gmail.com*

***Developer:** Genzz*

We will respond to privacy-related enquiries within 30 days.

17. Changes to This Policy

We may update this Privacy Policy from time to time. The "Last Updated" date at the top of this page will reflect any changes. Continued use of the App after an update constitutes acceptance of the revised policy. We encourage you to review this policy periodically.

18. Regulatory Compliance

This Privacy Policy is designed to comply with applicable privacy laws and regulations, including:

- ***Google Play Developer Program Policies** (User Data policy, Permissions policy, Privacy and Security policy)*
- ***General Data Protection Regulation (GDPR)** — European Union / EEA*
- ***California Consumer Privacy Act (CCPA)** — California, USA*
- ***Children's Online Privacy Protection Act (COPPA)***

Accurate disclosure of on-device processing, local storage, and limited Google Play billing / update / review interactions is the primary compliance focus for this App.

19. Special Disclosure: Sensitive Permissions (Required by Google Play)

`QUERY_ALL_PACKAGES` Permission Justification:

*Spy Apps Detector uses the **QUERY_ALL_PACKAGES** permission for its **sole core purpose**: identifying potentially harmful, spy, or privacy-threatening applications installed on your Android device. The App must be able to enumerate all installed applications in order to perform a security assessment. This permission is essential to the App's primary function and cannot be replaced by a narrower alternative. All data accessed through this permission is processed locally on your device and is never transmitted to any external server. Compact scan snapshots may be stored **locally on your device only** (see Section 5) so you can compare changes over time; they are never transmitted and can be cleared at any time.*

`PACKAGE_USAGE_STATS` Permission Justification:

This permission is used optionally to retrieve the last-used date and storage size of installed applications, which enhances the accuracy of the security assessment by identifying apps that have been installed but never launched — a common characteristic of covert monitoring software — and supports certain Premium Deep Scan signals. This permission requires explicit user grant and is used solely to improve local scan results. No usage data is transmitted remotely.