Coordinated Privacy Disclosure, Final Report

Geizhals Android (at.geizhals.pv)

Preisvergleich Internet Services AG, Austria

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE STATED 24 SEPTEMBER EMBARGO, SEVEN MESSAGES, ZERO REPLY OF ANY KIND

Target	Geizhals, Austria's largest price comparison platform
Package	at.geizhals.pv, version 3.13.0
Operator	Preisvergleich Internet Services AG, Austria
Initial Disclosure	2026-06-26
Stated Embargo	2026-09-24, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, one day after the stated date
Regulators	Austrian DSB, EDPS
Total Outbound Messages	7, across 78 days, all delivered to info@geizhals.at, presse@geizhals.at, and webmaster@geizhals.at.
Inbound Replies	0. No reply, automated or human, was ever received.

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 26 June 2026, RFI-IRFOS disclosed to Preisvergleich Internet Services AG that its Geizhals Android app registers com.facebook.internal.FacebookInitProvider as an Android ContentProvider, meaning the Facebook SDK initializes at process start, before any Activity, Fragment, or consent screen exists. Facebook's own SDK documentation states that AutoInitEnabled should be set to false until consent is received; that flag was not set. The same pattern repeats for Firebase: two separate ContentProviders, one directBootAware and initOrder=100, initialize before consent, generating and transmitting a Firebase Installation ID even though Firebase Analytics event collection itself is correctly disabled, a partial mitigation that does not reach the underlying initialization.

A second structural finding concerns Settings.Secure.ANDROID_ID, a permanent, cross-session device identifier that resets only on factory reset. Confirmed in decompiled smali bytecode, it is read and transmitted as device_id and request_fingerprint to the app's own backend, with no legal basis established before collection and no mention in the app's privacy policy. Even a user who later declines optional analytics consent cannot retroactively un-transmit an identifier already read.

Four further findings round out the disclosure: four Google API keys hardcoded and extractable from the production binary; RECEIVE_BOOT_COMPLETED registered alongside WorkManager background tasks that run before the user has opened the app in a given session, meaning consent from a prior session cannot cover new processing that begins on reboot; all four Google Privacy Sandbox advertising APIs (Topics, Custom Audience/FLEDGE, AD_ID, Attribution) declared with no disclosure in the privacy policy; and ACCESS_FINE_LOCATION with a foreground location service, disproportionate for what the app itself describes as a store-locator feature. Genuine positives are worth naming: firebase_analytics_collection_enabled is correctly set to false, the camera permission ties cleanly to a legitimate barcode-scanner feature, and no cleartext traffic exceptions were found anywhere in the network security configuration.

Seven messages were sent across 78 days, all delivered to info@geizhals.at, presse@geizhals.at, and webmaster@geizhals.at, cc'ing the Austrian DSB throughout. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the initial disclosure, elapsed on 24 September 2026. This report and the accompanying closure notice publish one day later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Geizhals Android application (at.geizhals.pv, version 3.13.0, versionCode 31285, targetSdk 35), pulled from Google Play and reviewed on 26 June 2026. No account was created and no interaction with api.geizhals.net, Facebook's, or Google's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 26 June 2026, re-scored under CVSS v4.0. All six re-scored findings correct to MEDIUM on their own computed bands: pre-consent Facebook SDK initialization, dual pre-consent Firebase ContentProviders, an ANDROID_ID permanent identifier read with no established legal basis, four hardcoded Google API keys, boot-triggered background WorkManager tasks before the app is opened, and all four undisclosed Privacy Sandbox advertising APIs. Disproportionate fine-location access for a store-locator feature corrects to LOW. Seven messages were sent across 78 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Facebook SDK Initializes Before Any Consent Screen
C2	MEDIUM	Two Firebase ContentProviders Initialize Before Any Consent Screen
C3	MEDIUM	Permanent Device Identifier Read With No Established Legal Basis
C4	MEDIUM	Four Google API Credentials Hardcoded in the Production Binary
C5	MEDIUM	Background Tasks Run at Device Boot Before the App Is Opened
M1	MEDIUM	All Four Privacy Sandbox Advertising APIs Declared, Undisclosed
M2	LOW	Fine-Grained Location Access Disproportionate for a Store-Locator Feature

Subject & Operator Analysis

Geizhals is operated by Preisvergleich Internet Services AG and positions itself as Austria's most trusted price comparison platform, used by millions of Austrian and German consumers to make purchasing decisions.

Genuine positives are worth naming. firebase_analytics_collection_enabled is correctly set to false, disabling Firebase Analytics event collection and showing awareness of the underlying issue, even though it does not reach Firebase's own initialization. The camera permission ties cleanly to a legitimate barcode-scanner feature (ZXing CaptureActivity). No cleartext traffic exceptions were found in the network security configuration, and all API calls target HTTPS endpoints.

Seven Messages, Zero Reply

All seven messages in this case's correspondence record were delivered successfully to info@geizhals.at, presse@geizhals.at, and webmaster@geizhals.at across 78 days, cc'ing the Austrian DSB throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Facebook SDK Initializes Before Any Consent Screen

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

com.facebook.internal.FacebookInitProvider is registered as an Android ContentProvider, meaning its onCreate() fires at application process start, before any Activity or consent screen. No meta-data for com.facebook.sdk.AutoInitEnabled=false was found; Facebook's own documentation requires setting that flag before collecting consent. The Facebook SDK is not named as a data processor in the app's privacy policy.

```
<provider android:name="com.facebook.internal.FacebookInitProvider" android:exported="
    false"/>
Facebook App ID: 1443340215984423
Facebook Client Token: fa9e4e777ccad3506f4a3be176698210
```

Impact: Facebook's SDK initializes unconditionally on every app launch, with no disclosed processor relationship, meaning users cannot have given informed consent for a processing activity they were never told about.

Fix: Set AutoInitEnabled to false until app-native consent is obtained, and name Meta as a data processor in the privacy policy. No confirmation that this has occurred was ever received.

C2: Two Firebase ContentProviders Initialize Before Any Consent Screen

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

FirebaseInitProvider (directBootAware=true, initOrder=100) and FlutterFirebaseMessagingInitProvider (initOrder=99) both fire before any user-facing screen. firebase_analytics_collection_enabled is correctly set to false, disabling event logging, but this does not prevent Firebase from generating and transmitting a Firebase Installation ID on first launch, before consent, and Google is not listed as a data processor in the privacy policy.

```
FirebaseInitProvider: directBootAware=true, initOrder=100
FlutterFirebaseMessagingInitProvider: initOrder=99
google_api_key: AIzaSyBLIUf66NBSCq4tB-_pCz0HpuGA_NqsPUM
```

Impact: A unique Firebase Installation ID tied to the specific device-app pair reaches Google's infrastructure before any consent is given, a partial mitigation (disabled analytics events) that does not reach the underlying identifier generation.

Fix: Delay Firebase initialization until after consent, or gate FID generation specifically. No confirmation that this has occurred was ever received.

C3: Permanent Device Identifier Read With No Established Legal Basis

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

Settings.Secure.ANDROID_ID, a permanent identifier that persists across reinstalls and resets only on factory reset, is read and transmitted as device_id and request_fingerprint to api.geizhals.net, confirmed in decompiled smali bytecode. No legal basis is established before this collection, and it is not mentioned in the privacy policy.

```
Settings.Secure.getString(ContentResolver, "android_id")
Transmitted as device_id, request_fingerprint -> api.geizhals.net
```

Impact: Even a user who later declines optional analytics consent cannot retroactively undo the ANDROID_ID read that already occurred, since it happens before any consent mechanism is presented.

Fix: Establish a documented legal basis before reading ANDROID_ID, or remove the collection. No confirmation that this has occurred was ever received.

C4: Four Google API Credentials Hardcoded in the Production Binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9.

Four Google API credentials, a Firebase API key, a crash-reporting key, a Google app ID, and a Google Maps API key, are all hardcoded and extractable from the production binary with a standard decompiler.

```
google_api_key, google_crash_reporting_api_key: AIzaSyBLIUf66NBSCq4tB-
    _pCz0HpuGA_NqsPUM
google_app_id: 1:274620206527:android:0cc851fbf58c56bf45a50a
google_maps_api_key: AIzaSyA5CzkibJ6lWQl7yh09b9oLdQNvBy9WCdc
```

Impact: Any actor with a standard decompiler can extract these keys and exhaust the associated project's API quotas anonymously, taking the service offline for real users, a genuine Art. 32(1)(b) availability concern even though the keys themselves are not secrets by design.

Fix: Restrict all four keys by package name and certificate fingerprint, and monitor for anomalous quota consumption. No confirmation that this has occurred was ever received.

C5: Background Tasks Run at Device Boot Before the App Is Opened

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

RECEIVE_BOOT_COMPLETED is declared, with three WorkManager system receivers registered against it. Scheduled tasks include FCM token refresh and Play Install Referrer queries, both of which can run before the user has opened the app for the first time in a given session.

```
RECEIVE_BOOT_COMPLETED
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
```

Impact: Consent is not a one-time past event, it must be freely given before each new processing operation; a user who reboots their device without opening the app has not consented to any processing that begins in that new session.

Fix: Gate boot-triggered background tasks behind a check that consent has already been given in the current session. No confirmation that this has occurred was ever received.

M1: All Four Privacy Sandbox Advertising APIs Declared, Undisclosed

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

TOPICS, CUSTOM_AUDIENCE (FLEDGE), AD_ID, and ATTRIBUTION are all declared, the full set of Google's Privacy Sandbox advertising permissions, with no mention of any of them in the privacy policy.

Impact: Behavioral advertising infrastructure spanning cohort assignment, cross-app audience targeting, advertising identification, and attribution is present with no user-facing disclosure of any of it.

Fix: Document each Privacy Sandbox API's specific purpose in the privacy policy, or remove any not actively used. No confirmation that this has occurred was ever received.

M2: Fine-Grained Location Access Disproportionate for a Store-Locator Feature

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

ACCESS_FINE_LOCATION (GPS-precision location) is declared alongside a foreground location service. A price comparison platform's store-locator function does not typically require GPS-precision accuracy over coarse location.

Impact: Precise, continuous location access is a broader data category than a store-locator feature needs, a data-minimisation gap, not an active exploitation path.

Fix: Evaluate whether ACCESS_COARSE_LOCATION satisfies the store-locator use case, and downgrade if so. No confirmation that this has occurred was ever received.

Article	Finding	Basis

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 7, Art. 6(1)(a), Art. 13(1)(e)	C1	Pre-consent Facebook SDK initialization.
Art. 7, Art. 6(1)(a), Art. 28	C2	Pre-consent Firebase initialization and undisclosed Installation ID transmission.
Art. 6(1), Art. 25, Art. 5(1)(c)	C3	Permanent device identifier read with no legal basis.
Art. 32(1)(b)	C4	Hardcoded, unrestricted Google API keys.
Art. 7(1)	C5	Boot-triggered background processing before app is opened.
Art. 5(1)(a), Art. 13(1)(c)	M1	Undisclosed Privacy Sandbox advertising APIs.
Art. 5(1)(c)	M2	Disproportionate fine-location access.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1-C5 and M1 correct to MEDIUM on their own computed bands. M2 corrects to LOW. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: #GEI-2026-001.