Coordinated Privacy Disclosure, Final Report

BILLA Android (at.billa.service)

BILLA AG / REWE International AG, Wiener Neudorf, Austria

SUBSTANTIVE FIRST REPLY, THEN SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO

Target	BILLA – Lebensmittel & Angebote, a grocery loyalty, ordering, and home-delivery Android app
Package	at.billa.service
Operator	BILLA AG / REWE International AG, Wiener Neudorf, Austria (app built by digital.riag.appsolution)
Initial Disclosure	2026-06-21
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	Austrian DSB (lead SA), CERT.at
Total Outbound Messages	4, across 73 days, to datenschutz@billa.at, cc'ing security@rewe-group.com.
Inbound Replies	1, on 25 June 2026: a named BILLA data protection contact acknowledged the report and stated the findings would be reviewed in detail with a follow-up to come. No follow-up was ever received; 91 days of silence followed.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS disclosed to BILLA AG that its grocery loyalty and home-delivery Android app embeds three separate Google API keys in plaintext, a Firebase key, a Google Maps key, and a Google Places key, all extractable from the public Play Store APK in seconds. The same disclosure named an integrated Adobe Experience Cloud stack, including Adobe Audience Manager, a behavioral data broker, receiving grocery purchase history capable of supporting inferences about dietary restrictions, religious practice, pregnancy status, and other Art. 9-adjacent categories, without this relationship being clearly disclosed.

On 25 June 2026, four days after disclosure, a named BILLA data protection contact replied, thanking RFI-IRFOS for the report and stating the findings would be reviewed in detail with a follow-up. No further reply of any kind was received across the following 91 days, despite one further message on 2 September 2026 explicitly referencing that promise. That 2 September message also incorporated a fresh, independent re-pull of the live APK: it confirmed the original findings unchanged, corrected the Crashlytics finding to note collection is in fact disabled by default (the original report's wording had overstated this as active), and surfaced a new finding, FirebaseInitProvider itself initializing before any consent screen, absent from the original review.

Four messages were sent across 73 days, cc'ing security@rewe-group.com and, on later rounds, the Austrian DSB. One substantive reply was received, on 25 June 2026, promising a follow-up that never came. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days 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 BILLA Android application (at.billa.service), reviewed initially on 21 June 2026 and independently re-verified against a fresh APK pull (version 26.31.0-926845) on 2 September 2026. No dynamic instrumentation, live traffic capture, or interaction with BILLA's or Adobe's backend infrastructure was performed.

Disposition

Six findings were disclosed on 21 June 2026, re-scored under CVSS v4.0. All six correct to MEDIUM on their computed bands, with one exception: a re-verification pass conducted 2 September 2026 found that Firebase Crashlytics collection is disabled by default, contradicting the original report's overstated description of it as actively transmitting device data, and that finding is corrected here to OBSERVATIONAL. The same re-verification pass also surfaced a finding absent from the original report: FirebaseInitProvider itself initializes before any consent screen. A named contact at BILLA acknowledged the report substantively four days after disclosure and promised a follow-up review; none was ever received across the following 91 days.

ID	Severity	Title
C1	MEDIUM	Three Google API Keys Hardcoded in Production

ID	Severity	Title
H1	MEDIUM	Adobe Audience Manager Receives Grocery Purchase Data Capable of Sensitive Inference
H2	MEDIUM	Debug-Override Trust Anchors and No Certificate Pinning on Checkout and Delivery Traffic
C2	MEDIUM	Firebase Initializes Before Any Consent Screen
M1	MEDIUM	Fine-Precision Location Disproportionate to a Store-Locator Purpose
H3	OBSERVATIONAL	Firebase Crashlytics — Collection Confirmed Disabled by Default, Correcting the Original Report

Subject & Operator Analysis

BILLA is a major Austrian grocery chain operated by BILLA AG, part of REWE International AG, headquartered in Wiener Neudorf. The app handles loyalty program membership, purchase history, shopping lists, home-delivery orders including residential address and payment method, and precise location.

Several genuine positives are worth naming. allowBackup is correctly set to false, blocking ADB backup extraction. A OneTrust consent management platform is present, indicating consent infrastructure exists, though whether it correctly gates every tracking SDK was outside the scope of this static review. Klarna's payment SDK is a standard, non-concerning checkout integration in isolation.

One Substantive Reply, a Promised Follow-Up That Never Came

This case's correspondence record includes a genuine, named, substantive first reply, not silence from the outset. On 25 June 2026, four days after disclosure, a BILLA data protection contact thanked RFI-IRFOS for the report and stated the findings would be reviewed in detail, with a follow-up to come. That follow-up never arrived. A further message on 2 September 2026, referencing the promise directly and incorporating a fresh, independent re-verification of the live APK, drew no response either. Four messages were sent in total across 73 days, cc'ing security@rewe-group.com and the Austrian DSB. No reply beyond the single 25 June acknowledgment was ever received.

Findings

C1: Three Google API Keys Hardcoded in Production

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9. Confirmed unchanged on independent re-verification, 2 September 2026.

A Firebase API key, a Google Maps API key, and a Google Places API key are all embedded in plaintext in the production APK, extractable by anyone who decompiles the app, a 30-second operation. Any party could consume Google Maps/Places API quota billed to REWE's GCP account, attempt Firebase database access against the named project, or access Firebase Cloud Storage if bucket rules are misconfigured.

```
Firebase API key: AIzaSyAGEzUo4kcMw-_45vqoACXRlNtQL2zAvDE (project billa-austria---as)
Google Maps API key: AIzaSyBwXe0LPHEERiyzBZFmvk69EliKv9vY4s0
Google Places API key: AIzaSyDgmW4ZMvNblSXqMOgsbY8uRrTnfR3E7pY
```

Impact: All three keys are trivially extractable, and depending on the security-rule and quota configuration behind each, could enable unauthorized access, unbudgeted API billing, or denial of service against legitimate users.

Fix: Restrict all three keys by package name and SHA-256 certificate fingerprint in the GCP console. No confirmation that this has occurred was ever received.

H1: Adobe Audience Manager Receives Grocery Purchase Data Capable of Sensitive Inference

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. Confirmed unchanged on independent re-verification, 2 September 2026.

The Adobe Experience Cloud Mobile SDK is integrated with Analytics, Identity, UserProfile, AudienceManager, Target, and Assurance modules all confirmed active in smali. Adobe Audience Manager is a behavioral data broker; its integration links BILLA purchase history, dietary choices, purchase frequency, basket value, to Adobe's cross-publisher identity graph, without this specific relationship being clearly disclosed.

```
com.adobe.marketing.mobile: Analytics, Identity, UserProfile, AudienceManager, Target,
     Assurance (all confirmed active)
```

Impact: Grocery purchase history, capable of supporting inferences about religious practice (kosher/halal products), reproductive status (baby formula, pregnancy tests), health conditions (medications, supplements), and lifestyle (alcohol, tobacco), flows into a third-party behavioral data broker without clear disclosure of that specific relationship.

Fix: Conduct an Art. 35 DPIA for the AudienceManager integration and implement explicit opt-in consent for any inferred special-category processing, or disable AudienceManager pending that review. No confirmation that this has occurred was ever received.

H2: Debug-Override Trust Anchors and No Certificate Pinning on Checkout and Delivery Traffic

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.3. Confirmed unchanged on independent re-verification, 2 September 2026.

The network security config declares a debug-overrides block trusting user-installed CA certificates, present without any accompanying production base-config or domain-config, and no certificate pinning exists for any BILLA backend endpoint. On a rooted device, or in the presence of a user-installed or corporate MDM CA, this permits interception of checkout flows, home-delivery addresses, and payment-method selection.

```
<network-security-config>
  <debug-overrides>
    <trust-anchors><certificates src="user" /></trust-anchors>
  </debug-overrides>
</network-security-config>
(no production base-config, no pin-set)
```

Impact: A system-CA compromise or a corporate MDM-installed CA can intercept loyalty, purchase, and checkout data, including home-delivery addresses and payment method selection, in transit.

Fix: Add a production base-config with cleartextTrafficPermitted=false and a pin-set for critical endpoints, and scope debug-overrides strictly to debug build types in Gradle. No confirmation that this has occurred was ever received.

C2: Firebase 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. First identified on independent re-verification, 2 September 2026, absent from the original 21 June review.

FirebaseInitProvider is declared with android:initOrder=100, executing before any Activity and therefore before any consent screen, a finding not identified in the original static review and surfaced only on independent re-verification against the live production build.

```
com.google.firebase.provider.FirebaseInitProvider  android:initOrder=100 (confirmed
    2026-09-02, absent from original 2026-06-21 review)
```

Impact: Firebase begins initializing before a user has seen a single consent notice, a gap not caught in the original review and surfaced only through re-verification against the live build.

Fix: Defer FirebaseInitProvider initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

M1: Fine-Precision Location Disproportionate to a Store-Locator Purpose

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. Confirmed unchanged on independent re-verification, 2 September 2026.

ACCESS_FINE_LOCATION (GPS-precision, roughly 10m accuracy) is declared for a store-locator function that coarse location (roughly 50-100m accuracy) would adequately serve. Combined with purchase history and the Adobe AudienceManager integration, precise GPS traces support home/work location inference and travel-pattern profiling well beyond the stated store-locator purpose.

Impact: Precise location data, combined with purchase and behavioral-profiling data already flowing to Adobe, creates a detailed movement and location profile disproportionate to finding nearby stores.

Fix: Downgrade to ACCESS_COARSE_LOCATION for the store-locator function, or gate fine location behind an explicit, separately justified permission request. No confirmation that this has occurred was ever received.

H3: Firebase Crashlytics — Collection Confirmed Disabled by Default, Correcting the Original Report

OBSERVATIONAL — CVSS v4.0 computes to 0.0/None with collection disabled by default; this finding corrects an overstated claim in the original 21 June report and is not independently scored.

The original report described Crashlytics as actively transmitting device data to Google upon any crash. Independent re-verification on 2 September 2026 found that Crashlytics collection is in fact disabled by default in the reviewed build, contradicting that original, overstated wording. This correction is made here in the interest of accuracy; the Crashlytics SDK's mere presence in the binary, with collection off by default, carries no independently scoreable technical impact.

```
com.google.firebase.crashlytics -- SDK present, collection confirmed DISABLED by
    default on re-verification (corrects original overstated 'active' claim)
```

Impact: No default-state data transmission occurs via Crashlytics; if collection is ever enabled, whether by a future update or a runtime toggle, the original Art. 13/Art. 46 disclosure concerns would apply at that point.

Fix: Document Crashlytics' default-off state and any conditions under which it can be enabled, under Art. 13(1)(e), should that state ever change. No confirmation that this has occurred was ever received.

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. 32	C1	Three hardcoded, trivially extractable Google API keys.
Art. 9 (inference risk), Art. 35	H1	Grocery purchase data flowing to a third-party behavioral data broker.
Art. 32	H2	Debug-override trust anchors and no certificate pinning on checkout/delivery traffic.
Art. 7, Art. 25	C2	Pre-consent Firebase initialization, identified on re-verification.
Art. 5(1)(c)	M1	Disproportionate precise-location access for a store-locator function.

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, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, C1, H1, H2, C2, and M1 correct to MEDIUM to match their own computed bands; H3 is corrected to OBSERVATIONAL, reflecting a self-corrected overstatement in the original 21 June report, confirmed on independent re-verification that Crashlytics collection is disabled by default. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: BILLA-2026-R1.