Coordinated Privacy Disclosure, Final Report

Babbel Android (com.babbel.mobile.android.en)

Babbel GmbH, Berlin, Germany

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, TWO DAYS AFTER THE EMBARGO, ELEVEN MESSAGES, ONE AUTOMATED ACKNOWLEDGMENT, ZERO SUBSTANTIVE REPLY

Target	Babbel, a language-learning subscription Android app with approximately 10 million subscribers
Package	com.babbel.mobile.android.en
Operator	Babbel GmbH, Berliner Freiheit 18, 10785 Berlin, Germany
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators	Berlin data protection authority BlnBDI (lead SA), Austrian DSB, CERT.at
Total Outbound Messages	11, across 84 days, to privacy@babbel.com, cc'ing press@babbel.com, the Austrian DSB, and, on later rounds, BlnBDI and CERT.at.
Inbound Replies	1, on 25 June 2026, a pure automated acknowledgment confirming receipt only. No substantive human reply 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 25 June 2026, RFI-IRFOS disclosed to Babbel GmbH that its language-learning app initializes both FirebaseInitProvider (initOrder=100, directBootAware) and Facebook's PlatformProvider as ContentProviders, both firing before MainActivity, before SplashActivity, and before any consent screen. This finding sits alongside a genuinely positive practice: Babbel's own in-app voice-AI feature does implement an explicit, correctly worded consent dialog for voice recording, confirming the company's engineering team is capable of doing this correctly when it chooses to.

A second finding names the app's advertising infrastructure, not a single tracking flow: all four Privacy Sandbox permissions are declared, including ACCESS_ADSERVICES_CUSTOM_AUDIENCE, present in relatively few apps in this audit series, enabling Babbel to define behavioral cohorts of its own subscribers and serve ads to those cohorts inside other, unrelated apps, a use exceeding what a paid, ad-free-model subscription app's users would reasonably expect. Separately, all seven Adjust fingerprinting modules are compiled in, including IMEI collection (a permanent, non-resettable identifier) and dedicated Samsung, Huawei, Vivo, Xiaomi, and Meta device-fingerprint modules, and two hardcoded staging API endpoints remain reachable from the production binary.

Eleven messages were sent to privacy@babbel.com across 84 days, cc'ing press@babbel.com, the Austrian DSB, and, from August onward, the Berlin data protection authority (BlnBDI) and CERT.at. Only one reply was ever received, a pure automated acknowledgment on 25 June 2026 confirming receipt only. Not one substantive, human-authored reply addressing any specific finding followed across four further deadline-restating follow-ups. The 90-day embargo, set at first contact, elapsed on 23 September 2026. This report and the accompanying closure notice publish two 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 Babbel Android application (com.babbel.mobile.android.en, version 22.2.2, 62.4 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Babbel's, Google's, Facebook's, or Adjust's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All seven correct to MEDIUM, LOW, or OBSERVATIONAL on their computed bands. Pre-consent Firebase and Facebook initialization, all four Privacy Sandbox permissions including Custom Audience cohort targeting, a full seven-module Adjust fingerprinting stack, and hardcoded staging API endpoints all correct to MEDIUM. allowBackup left at true corrects to LOW, and duplicate boot-time auto-start corrects to OBSERVATIONAL. Eleven messages were sent across 84 days; only one reply was ever received, a pure automated acknowledgment on the day of disclosure, and no substantive human reply followed.

ID	Severity	Title
C1	MEDIUM	Firebase and Facebook Both Initialize Before Any Consent Screen
H1	MEDIUM	All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting
H2	MEDIUM	Full Seven-Module Adjust Fingerprinting Stack, Including IMEI and Multi-OEM Modules
H3	MEDIUM	Media Projection (Screen-Capture) Permission With No Corresponding Registered Service
M1	MEDIUM	Staging API Endpoints Hardcoded in the Production Binary
M2	LOW	allowBackup Left at True: Learning Progress and Subscription Status Eligible for Cloud Backup
M3	OBSERVATIONAL	Duplicate Boot-Time Auto-Start

Subject & Operator Analysis

Babbel is a language-learning subscription platform with approximately 10 million subscribers, operated by Babbel GmbH, Berlin, placing the Berlin data protection authority (BlnBDI) as lead supervisory authority.

Several genuine positives are worth naming. usesCleartextTraffic is correctly set to false. A network security configuration is present. Babbel's in-app voice-AI feature implements a correctly worded, explicit consent dialog for voice recording, a real, working example of Art. 7-compliant consent gating already present in the codebase. CAMERA is correctly declared as not required, so the app does not force camera access on devices without one, and RECORD_AUDIO is contextually justified by the pronunciation feature.

Eleven Messages, One Automated Acknowledgment, Zero Substantive Reply

This case's correspondence record involved a working contact channel from the first message; no address bounced. Eleven messages were sent to privacy@babbel.com across 84 days, cc'ing press@babbel.com, the Austrian DSB, and, from August 2026 onward, BlnBDI and CERT.at. Only one reply was ever received, a pure automated acknowledgment on 25 June 2026, the day of disclosure, confirming receipt only. Not one substantive, human-authored reply addressing any of the seven findings or the three original technical questions was ever received across four further deadline-restating follow-ups.

Findings

C1: Firebase and Facebook Both 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 is declared with initOrder=100 and directBootAware="true", and Facebook's PlatformProvider is registered as a ContentProvider, both firing at process creation, before any Activity and therefore before any consent screen. Babbel's own in-app voice-AI feature, by contrast, does implement an explicit, correctly worded Art. 7 consent dialog for voice recording, confirming the underlying engineering capability to do this correctly already exists inside the company.

```
com.google.firebase.provider.FirebaseInitProvider   initOrder=100, directBootAware=
    true
com.facebook.katana.provider.PlatformProvider (registered ContentProvider)
```

Impact: Two separate SDK bootstraps begin before a user has seen a single consent notice, even though the app's own voice-AI feature demonstrates correct consent-gating is already implemented elsewhere in the same codebase.

Fix: Apply the same consent-gating pattern already used for the voice-AI feature to Firebase and Facebook initialization. No confirmation that this has occurred was ever received.

H1: All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting

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.

AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS, and ACCESS_ADSERVICES_CUSTOM_AUDIENCE are all declared. Custom Audience, present in relatively few apps in this audit series, enables Babbel to define behavioral cohorts of its own subscribers, such as language and streak-length segments, and serve ads to those cohorts inside other, unrelated apps.

```
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

Impact: A subscriber's language-learning behavior can be turned into a cross-app advertising targeting cohort, an advertising-network-style use exceeding what a subscription app's users would reasonably expect.

Fix: Document an individual Art. 6(1) legal basis for Custom Audience targeting or remove the permission. No confirmation that this has occurred was ever received.

H2: Full Seven-Module Adjust Fingerprinting Stack, Including IMEI and Multi-OEM Modules

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.

All seven Adjust fingerprinting modules are compiled in: IMEI collection, OAID (Chinese ad-tracking identifier), and dedicated Samsung, Huawei, Vivo, Xiaomi, and Meta device-fingerprint modules. IMEI is a permanent, non-resettable device identifier, and the multi-OEM modules build cross-app and cross-device profiles that survive app reinstallation.

```
com.adjust.sdk.imei.Util, oaid.Util, samsung.Util, huawei.Util, vivo.Util, xiaomi.Util
    , meta.Util (all 7 compiled)
```

Impact: A permanent, non-resettable hardware identifier and multiple OEM-specific fingerprinting modules are all active, building a device profile that survives even a full app reinstall.

Fix: Remove IMEI and multi-OEM fingerprinting modules unless independently required and documented, and rely on resettable identifiers only. No confirmation that this has occurred was ever received.

H3: Media Projection (Screen-Capture) Permission With No Corresponding Registered Service

MEDIUM, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 4.1.

FOREGROUND_SERVICE_MEDIA_PROJECTION, required to run a screen-capturing foreground service via MediaProjectionManager, is declared, but all registered foreground services use foregroundServiceType=mediaPlayback only, with no service registered at foregroundServiceType=mediaProjection. Either a library dependency is pulling the permission silently, or the capability exists without a documented, disclosed feature.

```
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION (declared)
All registered foreground services: foregroundServiceType=mediaPlayback only, none at
    mediaProjection
```

Impact: A screen-capture-capable permission is present with no corresponding, documented feature, an undisclosed capability gap; the practical trigger conditions require local investigation the static review could not perform, which keeps the computed score moderate.

Fix: Identify the source of this permission (likely a support-chat library's screen-sharing module) and either register and disclose the corresponding service, or remove the permission if unused. No confirmation that this has occurred was ever received.

M1: Staging API Endpoints Hardcoded in the Production Binary

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.

Two staging API endpoints are hardcoded in the production binary, environments that typically carry relaxed authentication and less comprehensive logging than production infrastructure.

```
https://api.babbel-staging.io/gamma/
https://api.babbel-staging.io/gamma/v1/service-discovery
```

Impact: A permanent, publicly extractable reference to staging infrastructure not designed for public access ships in the production build.

Fix: Strip all staging environment references from production release builds. No confirmation that this has occurred was ever received.

M2: allowBackup Left at True: Learning Progress and Subscription Status Eligible for Cloud Backup

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

android:allowBackup is left at its true default, with no selective exclusion visible in the manifest, meaning language-learning progress, vocabulary history, streak data, and subscription status are all eligible for automatic backup via Android Backup Service to Google Cloud.

Impact: Learning and subscription data can end up in a user's Google Cloud backup; the practical exposure depends on the backup destination's own security and is not directly network-reachable, which keeps the computed score low.

Fix: Set allowBackup to false, or define explicit backup exclusion rules for sensitive learning and subscription data. No confirmation that this has occurred was ever received.

M3: Duplicate Boot-Time Auto-Start

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

Two receivers are registered for BOOT_COMPLETED, meaning the app starts automatically at device boot before any user interaction.

Impact: The app begins running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove the duplicate declaration if not load-bearing. 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. 7, Art. 25	C1	Pre-consent SDK initialization via direct-BootAware ContentProviders.
Art. 5(1)(b), Art. 6(1), Art. 13(1)(c)	H1	Undisclosed cross-app advertising cohort targeting.
Art. 5(1)(a), Art. 6(1)	H2	A permanent, non-resettable hardware identifier collected without documented explicit consent.
Art. 5(1)(c), Art. 13(1)(c)	H3	An undocumented screen-capture-capable permission.
Art. 32	M1	Staging infrastructure endpoints hardcoded in a production binary.

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, H1, H2, H3, and M1 correct to MEDIUM to match their own computed bands; M2 corrects to LOW on its own computed band; M3 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. Disclosure conducted

under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: BABBEL-2026-R1.