Coordinated Privacy Disclosure, Final Report

Audible Android (com.audible.application)

Audible, Inc. (Amazon subsidiary), Newark, New Jersey, USA

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO, THIRTEEN MESSAGES, ONE BOUNCE, ZERO REPLY OF ANY KIND

Target	Audible, a paid audiobook subscription Android app
Package	com.audible.application
Operator	Audible, Inc. (Amazon subsidiary), Newark, New Jersey, USA; EU establishment Amazon Services Europe S.à r.l., Luxembourg
Initial Disclosure	2026-06-25
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	Luxembourg CNPD (lead SA for Amazon Services Europe), Austrian DSB, EDPS
Total Outbound Messages	13, across 79 days, to audibleprivacy@audible.com and mediarelations@audible.com. The first attempt bounced; twelve further messages were delivered successfully.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

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 Audible, Inc. that its Android app, a paid audiobook subscription service with no advertising, ships PryonLite, Amazon's on-device Alexa wake-word detection engine, whose ContentProvider is declared directBootAware="true", meaning it can initialize before the device is unlocked, loading a wake-word model into memory before any user authentication and before any consent dialog. The same app declares ACCESS_BACKGROUND_LOCATION alongside Braze's SINGLE_LOCATION_UPDATE receiver, indicating geofence-based engagement campaigns, continuous background location collection in a paid subscription product with no advertising purpose to justify it.

A second finding names Amazon's own cross-platform ecosystem, not a third-party tracker: the Google Advertising ID is declared despite the app serving no advertising of any kind, no AdMob, no third-party ad network SDK found anywhere in the binary, meaning its only plausible purpose is linking Audible listening behavior to Kindle, Prime Video, Alexa, and Amazon shopping activity within Amazon's own ecosystem. Separately, a full Meta wearable-connectivity SDK, including ACDC protocol configuration and secure IPC classes designed for Meta Quest and Ray-Ban Stories hardware, is compiled into this paid Amazon product with no disclosure to subscribers that Meta technology is embedded.

Thirteen messages were sent to audibleprivacy@audible.com and mediarelations@audible.com across 79 days, cc'ing the Austrian DSB and the EDPS on later rounds. The first message bounced; the twelve that followed were all delivered successfully. Not one reply, automated or human, was ever received on any address at any point. 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 Audible Android application (com.audible.application, version 26.23.03, 160 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Audible's, Amazon's, Braze's, or Meta's backend infrastructure was performed.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All five correct to MEDIUM or LOW on their computed bands. A directBootAware wake-word engine capable of initializing microphone-adjacent infrastructure before device unlock, background location paired with a geofence-capable CRM platform, an advertising identifier in an app that serves no advertising, and an embedded Meta wearable-connectivity SDK all correct to MEDIUM. An undocumented camera permission and screenshot-detection capability correct to LOW. Thirteen messages were sent across 79 days, one bouncing before delivery began succeeding. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Alexa Wake-Word Engine Declared directBootAware, Initializing Before Device Unlock

ID	Severity	Title
C2	MEDIUM	Background Location Paired With a Geofence-Capable CRM Platform in a Paid, Ad-Free App
H1	MEDIUM	Advertising Identifier Declared in an App That Serves No Advertising
H2	MEDIUM	A Full Meta Wearable-Connectivity SDK Embedded in a Paid Amazon Product
H3	LOW	Camera and Screenshot-Detection Permissions With No Disclosed Purpose

Subject & Operator Analysis

Audible is a paid audiobook subscription service, an Amazon subsidiary headquartered in Newark, New Jersey, with an EU establishment in Luxembourg placing the CNPD as lead supervisory authority.

Several genuine positives are worth naming. allowBackup is correctly set to false. No AdMob or third-party ad network SDKs were found, consistent with the paid subscription model. No Firebase integration was found; Amazon uses its own AWS analytics infrastructure instead. FOREGROUND_SERVICE_MEDIA_PLAYBACK, Bluetooth permissions, and Android Auto integration are all correctly justified by the app's core audiobook-playback and car-listening functions.

Thirteen Messages, One Bounce, Zero Reply

This case's correspondence record involved one address failure before delivery began succeeding. The first message, on 25 June 2026, bounced outright; the twelve messages that followed across the next 79 days were all delivered successfully, cc'ing the Austrian DSB and the EDPS on later rounds. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Alexa Wake-Word Engine Declared directBootAware, Initializing Before Device Unlock

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.

PryonLite, Amazon's on-device Alexa wake-word detection engine, is compiled in (native libraries for all four architectures, com.amazon.alexa.wakeword.pryon and com.amazon.alexa.wakeword.davs.DavsClient classes confirmed), with its ContentProvider declared directBootAware="true". This means the wake-word model, a 300-400 KB native model requiring audio input to function, can load into device memory before the device is unlocked, before any user authentication, and before any consent dialog can appear.

```
com.audible.application.pryon.wakeword.model  directBootAware=true
lib/arm64-v8a/libpryon-lite-jni.so, libpryon_lite-PRL2000.so (wake word model)
com.amazon.alexa.wakeword.pryon.R$integer, com.amazon.alexa.wakeword.davs.DavsClient
AlexaListeningState
```

Impact: Microphone-adjacent wake-word infrastructure can initialize before a user has unlocked their device or seen any consent mechanism, in an app whose only stated function is playing audiobooks.

Fix: Remove directBootAware from the wake-word ContentProvider, or gate its initialization behind explicit, post-unlock user consent. No confirmation that this has occurred was ever received.

C2: Background Location Paired With a Geofence-Capable CRM Platform in a Paid, Ad-Free App

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.

ACCESS_BACKGROUND_LOCATION is declared alongside Braze's SINGLE_LOCATION_UPDATE receiver and a fully embedded Braze engagement SDK, indicating geofence-based engagement campaigns triggered by physical location, in a paid subscription app that shows no advertising.

```
android.permission.ACCESS_BACKGROUND_LOCATION
com.braze.action.receiver.SINGLE_LOCATION_UPDATE
assets/braze-html-bridge.js, braze-html-in-app-message-bridge.js
```

Impact: Subscribers paying a monthly fee for audiobooks have their background physical location collected and made available to a CRM platform capable of geofence-triggered targeting, with no advertising purpose to explain the need.

Fix: Remove ACCESS_BACKGROUND_LOCATION or document the specific, disclosed feature it serves, and disclose Braze's geofencing capability explicitly. No confirmation that this has occurred was ever received.

H1: Advertising Identifier Declared in an App That Serves No Advertising

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.

The Google Advertising ID permission is declared despite no AdMob or third-party ad network SDK being found anywhere in the binary. Audible is a paid subscription service showing no advertising; the identifier's only plausible purpose is linking listening behavior to other Amazon services.

```
com.google.android.gms.permission.AD_ID  (no AdMob, no third-party ad SDK found in
    binary)
```

Impact: Listening behavior can be linked across Amazon's ecosystem, Kindle, Prime Video, Alexa, and shopping activity, via a persistent cross-app identifier, with no advertising purpose to explain its presence and no disclosure of this internal cross-service linkage located.

Fix: Remove the AD_ID permission if no advertising use exists, or disclose the specific internal ecosystem-linkage purpose under Art. 13(1)(c). No confirmation that this has occurred was ever received.

H2: A Full Meta Wearable-Connectivity SDK Embedded in a Paid Amazon Product

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.

Meta's wearable connectivity SDK, designed for Meta Quest headsets and Ray-Ban Stories smart glasses, is fully embedded, confirmed via com.facebook.wearable.* classes, a wearables_acdc.json configuration file confirming Meta's ACDC connectivity protocol is active, and dedicated data-framing and secure-IPC classes.

```
com.facebook.wearable.* (wearable connectivity, GATT, WiFi, Bluetooth)
xplat/mobileconfigschemas/wearables_acdc/wearables_acdc.json
com.facebook.wearable.airshield.stream.Framing, com.facebook.secure.aidl.AccessScope
```

Impact: Meta connectivity technology is compiled into a paid Amazon subscription product with no disclosure to subscribers that this integration exists or what data it can access.

Fix: Disclose the Meta wearable SDK integration explicitly under Art. 13(1)(e), or remove it if unused. No confirmation that this has occurred was ever received.

H3: Camera and Screenshot-Detection Permissions With No Disclosed Purpose

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.

CAMERA and DETECT_SCREEN_CAPTURE are both declared with no documented use case, such as a profile picture or barcode scan, disclosed at install time. An audiobook service has no self-evident need for either.

```
android.permission.CAMERA
android.permission.DETECT_SCREEN_CAPTURE
```

Impact: Camera access and screenshot-monitoring capability are present with no disclosed purpose; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low.

Fix: Document the specific feature requiring camera access and screenshot detection, or remove both. 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. 5(1)(b), Art. 7, Art. 25	C1	Microphone-adjacent infrastructure capable of initializing before device unlock and consent.
Art. 5(1)(b), Art. 6(1), Art. 13(1)(c)	C2	Undisclosed background location paired with geofence-capable CRM.
Art. 13(1)(c), Art. 5(1)(b)	H1	An advertising identifier with no advertising use, linking cross-ecosystem behavior.
Art. 13(1)(e), Art. 5(1)(b)	H2	An undisclosed Meta wearable-connectivity SDK embedded in a paid product.
Art. 5(1)(c), Art. 13(1)(c)	H3	Undocumented camera and screenshot-detection permissions.

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, C2, H1, and H2 correct to MEDIUM to match their own computed bands; H3 corrects to LOW on its own computed band. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: AUDIBLE-2026-R1.