



Coordinated Privacy Disclosure, Final Report

Easy Voice Recorder Android
(com.coffeebeanventures.easyvoicerecorder)

Digipom, United States

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, TWELVE MESSAGES, ONE AUTOMATED TICKET CONFIRMATION, ZERO HUMAN REPLY

Target	Easy Voice Recorder, a voice-recording Android app
Package	com.coffeebeanventures.easyvoicerecorder, version 2.10.2.1
Operator	Digipom, United States
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Austrian DSB, CERT.at, EDPS
Total Outbound Messages	12, across 79 days, all to support@digipom.com and privacy@digipom.com.
Inbound Replies	1 automated support-ticket confirmation on the day of disclosure. No human reply of any kind was ever received.

Contents

1	Executive Summary	4
2	Subject & Operator Analysis	5
3	Twelve Messages, One Auto-Reply, Zero Human Engagement	5
4	Findings	5
4.1	H1: Voice Recordings Eligible for Google Cloud Backup, No Exclusion Rules . .	6
4.2	C1: AdMob and Firebase Both Initialize Before Device Unlock in a Microphone App	6
4.3	H2: Hardcoded Firebase API Key	7
4.4	M1: Behavioral Topic Inference From Recording Patterns	7
4.5	H3: Undocumented WRITE_SETTINGS and READ_PHONE_STATE Permissions	7
5	Data Protection, Article by Article	8

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Digipom that its Easy Voice Recorder Android app leaves `android:allowBackup` set to `true` with no exclusion rules, meaning every recorded audio file, potentially including medical dictations, confidential conversations, or professional memos, is eligible for Android's default Google Cloud Backup mechanism. This is the single most sensitive finding in this report: a voice recorder's own recordings, its core product data, can leave the device to Google's infrastructure with no disclosed opt-out and no indication in the privacy policy presented to EU users at install time.

A second finding names the app's advertising initialization sequence: both the AdMob and Firebase content providers are declared with `initOrder=100` and `directBootAware=true`, meaning both can activate before the device is even unlocked, well before any consent screen renders, in an app whose entire function is capturing audio through the microphone. A hard-coded Firebase API key and `ACCESS_AD SERVICES TOPICS`, which can infer behavioral patterns from recording frequency, timing, and session length, round out the marketing-and-tracking findings. Two further permissions, `WRITE_SETTINGS` and `READ_PHONE_STATE`, have no documented purpose in a voice-recording context.

Twelve messages were sent across 79 days, all to `support@digipom.com` and `privacy@digipom.com`, cc'ing the Austrian DSB, CERT.at, and EDPS throughout. The only inbound reply, received the same day as the initial disclosure, was an automated support-ticket confirmation. Not one human reply of any kind was ever received across the following eleven messages and eleven weeks. The 90-day embargo, stated directly to the target in the initial disclosure, 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 Easy Voice Recorder Android application (`com.coffeebeanventures.easyvoicerecorder`, version 2.10.2.1, 23 MB), pulled from Google Play and reviewed on 25 June 2026. No account was created and no interaction with Digipom's, Google's, or Firebase's backend infrastructure was performed.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. `allowBackup` left enabled with no exclusion rules on a voice-recording app, meaning recorded audio is eligible for Google Cloud Backup, reaches HIGH/8.7 on its own computed band without escalation. Pre-consent AdMob and Firebase initialization at device boot, a hardcoded Firebase API key, and behavioral topic inference from recording patterns all correct to MEDIUM. Undocumented `WRITE_SETTINGS` and `READ_PHONE_STATE` permissions correct to LOW. Twelve messages were sent across 79 days. Not one human reply of any kind was ever received, only a single automated support-ticket confirmation on the day of the initial disclosure.

ID	Severity	Title
H1	HIGH	Voice Recordings Eligible for Google Cloud Backup, No Exclusion Rules

ID	Severity	Title
C1	MEDIUM	AdMob and Firebase Both Initialize Before Device Un-lock in a Microphone App
H2	MEDIUM	Hardcoded Firebase API Key
M1	MEDIUM	Behavioral Topic Inference From Recording Patterns
H3	LOW	Undocumented WRITE_SETTINGS and READ_PHONE_STATE Permissions

Subject & Operator Analysis

Easy Voice Recorder is a voice-recording app published by Digipom, a US company serving EU users under GDPR Art. 3(2).

Several genuine positives are worth naming. RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, BLUETOOTH, and MODIFY_AUDIO_SETTINGS are all justified for a voice recorder. There is no location or camera access. The APK is lean at 23 MB, with a single ad network, not a mediation stack, and no PRC-affiliated SDKs. MSAL for OneDrive integration is a legitimate, disclosed feature. These are signs of a focused, well-scoped app, the issues in this report are fixable without architectural changes.

Twelve Messages, One Auto-Reply, Zero Human Engagement

All twelve messages in this case's correspondence record were delivered successfully to support@digipom.com and privacy@digipom.com across 79 days, cc'ing the Austrian DSB, CERT.at, and the EDPS throughout. The only inbound reply, received the same day as the initial disclosure, was an automated support-ticket confirmation. Not one human reply, addressing any of the five findings, was ever received.

Findings

H1: Voice Recordings Eligible for Google Cloud Backup, No Exclusion Rules

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

android:allowBackup is set to true with no backup exclusion rules observed anywhere in the manifest or resources. Recorded audio files and their metadata, names, timestamps, durations, and file paths, are all eligible for Android's default Cloud Backup mechanism, which uploads to Google's infrastructure.

```
android:allowBackup="true"  
No backup exclusion rules present
```

Impact: Users recording medical dictations, confidential conversations, or professional memos on this app have not consented to Google storing copies of those recordings, and nothing in the app or its privacy policy discloses that this is the default behavior.

Fix: Set allowBackup to false, or define explicit backup exclusion rules covering all recorded audio files. No confirmation that this has occurred was ever received.

C1: AdMob and Firebase Both Initialize Before Device Unlock in a Microphone 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.

Both the app's own AdMob init provider and FirebaseInitProvider declare initOrder=100 and directBootAware=true, meaning both can activate before the device is unlocked, before any Activity, and before any consent screen renders, in an app whose core function is RECORD_AUDIO.

```
com.coffeebeanventures.easyvoicerecorder.mobileleadsinitprovider: initOrder=100,  
    directBootAware=true  
com.google.firebase.provider.FirebaseInitProvider: initOrder=100, directBootAware=true
```

Impact: A consent dialog shown after AdMob has already initialized is not a consent mechanism, it is a notification that processing has already begun, on the same device that stores the user's audio recordings.

Fix: Gate both providers' initialization behind an app-native consent flow. No confirmation that this has occurred was ever received.

H2: Hardcoded Firebase API Key

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.

A Firebase API key is hardcoded and extractable from the production binary.

Firebase API key: AIzaSyDrbcUjNC-eM0oqQnQqiWg5AwDI0ireFb8

Impact: The key is trivially extractable; unauthenticated calls against it can exhaust project quotas, a real availability risk.

Fix: Restrict the Firebase API key by package name and certificate fingerprint. No confirmation that this has occurred was ever received.

M1: Behavioral Topic Inference From Recording Patterns

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_AD SERVICES_TOPICS is declared, enabling behavioral topic inference from usage patterns, in this case recording frequency, timing, and session length, in an app whose core data is audio.

Impact: Advertising-topic inference built from the patterns of when and how often someone records audio adds a behavioral profiling layer on top of an app whose stated purpose is simple audio capture.

Fix: Remove ACCESS_AD SERVICES_TOPICS unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

H3: Undocumented WRITE_SETTINGS and READ_PHONE_STATE Permissions

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.

WRITE_SETTINGS, allowing system-level settings modification, and READ_PHONE_STATE, granting access to device identifiers and call state, are both declared with no documented purpose in a voice-recording context.

Impact: READ_PHONE_STATE combined with AdMob's identifier access is a device-fingerprinting vector, and WRITE_SETTINGS has no obvious justified purpose for a voice recorder.

Fix: Remove both permissions unless a specific, disclosed feature requires them. 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)(c), Art. 32, Art. 13(1)(e)	H1	Voice recordings eligible for cloud backup with no disclosed opt-out.
Art. 7, Art. 25	C1	Pre-consent ad and analytics SDK initialization before device unlock.
Art. 32	H2	Hardcoded Firebase API key.
Art. 5(1)(c)	M1	Behavioral topic inference from recording patterns.
Art. 5(1)(c), Art. 13(1)(c)	H3	Undocumented WRITE_SETTINGS and READ_PHONE_STATE permissions.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 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, H1 corrects to HIGH on its own computed band. C1, H2, and M1 correct to MEDIUM, and H3 corrects to LOW, all on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: #EASYVOICE-001.