Coordinated Privacy Disclosure, Final Report

Headspace Android (com.getsomeheadspace.android)

Headspace Health, Inc., United States, global mental health platform

CS-DEFLECT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE STATED 24 SEPTEMBER EMBARGO, EIGHT MESSAGES, ONE BUG-BOUNTY REDIRECT, ZERO SUBSTANTIVE REPLY

Target	Headspace, a global meditation, live therapy, and mental health app
Package	com.getsomeheadspace.android
Operator	Headspace Health, Inc., United States
Initial Disclosure	2026-06-22
Stated Embargo	2026-09-24, as restated directly to the target in later correspondence, superseding the 2026-09-19 date given in the initial disclosure
Report Published	2026-09-25, one day after the stated date
Regulators	Austrian DSB, CERT.at
Total Outbound Messages	8, across 70 days, to bugbounty@, privacy@, legal@, and security@headspace.com.
Inbound Replies	1 automated bug-bounty redirect to HackerOne, minutes after the initial disclosure. No further reply of any kind, 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 22 June 2026, RFI-IRFOS disclosed to Headspace Health that its Android app's production binary contains Sentry's RRWeb session-replay SDK, 72 active classes performing continuous screen recording, not error-triggered screenshots, active on the same screens where users conduct live video and audio therapy sessions with licensed therapists over WebRTC, and speak to Ebb, an AI voice journaling assistant, about their mental state, emotions, and trauma. The recording is streamed to Sentry's US servers. RFI-IRFOS holds this finding at CRITICAL under an explicit blast-radius escalation beyond its computed HIGH/8.7 CVSS band: it is the single most sensitive finding across this entire audit campaign, a continuous screen recorder capturing the content of live therapy conversations, transmitted to a third country with no confirmed transfer mechanism.

Within minutes, bugbounty@headspace.com replied with a standard HackerOne submission link. RFI-IRFOS declined to use it and explained why the same day: a bug-bounty triage team has no authority to evaluate whether special-category mental health data processing is lawful, assess a data processing agreement with Sentry, or determine an Art. 44 transfer basis, decisions that require a DPO, legal counsel, and executive leadership, not a vulnerability-triage queue. RFI-IRFOS named this explicitly as Pattern 7, Scope Deflect / Bug Bounty Redirect, and escalated directly to privacy@ and legal@headspace.com six days later. No further reply of any kind was ever received on any address across the following eight weeks.

A second finding compounds the first: Amplitude (517 classes), Braze (1,059 classes), Facebook's install-referrer attribution, and Google's advertising ID process the same therapy-engagement behavioral data, how often a user opens the app, which therapy features they use, how long sessions last, simultaneously across four separate marketing systems, alongside a per-user cumulative revenue metric layered on top of the mental health behavioral data. Four further findings round out the disclosure: an enterprise Zebra barcode-scanner SDK shipped in the consumer APK with no functional purpose for consumer users, WRITE_MINDFULNESS writes to Android Health Connect alongside an active marketing SDK stack with no verifiable architectural boundary between the two, a hardcoded Firebase API key, and a permission surface (foreground microphone, screen overlay, calendar read/write, phone calls) that is individually explicable but disproportionate in combination with the rest of the findings.

Eight messages were sent across 70 days, to bugbounty@, privacy@, legal@, and security@headspace.com, cc'ing the Austrian DSB and CERT.at throughout. The embargo, initially stated as 19 September 2026, was restated as 24 September 2026 in later correspondence without further comment; the later date governs. This report and the accompanying closure notice publish one day after that date.

Scope: Root-level static analysis of the production Headspace Android application (com.getsomeheadspace.android), pulled from Google Play and reviewed on 22 June 2026. No account was created, no network traffic was captured, and no interaction with Sentry's, Amplitude's, Braze's, or Facebook's backend infrastructure was performed.

Disposition

Six findings were disclosed on 22 June 2026, re-scored under CVSS v4.0. Continuous Sentry session-replay screen recording active during live WebRTC therapy sessions and AI voice journaling reaches HIGH/8.7 on its own computed band, and RFI-IRFOS holds it at CRITICAL under an explicit blast-radius escalation, given that it is the single most sensitive finding in this entire audit campaign: a continuous screen recorder running during live therapy conversations about mental health crises. Behavioral data from therapy engagement shared across four simultaneous marketing platforms reaches HIGH on its own computed band without escalation. Health Connect boundary risk and a hardcoded Firebase key correct to MEDIUM. Enterprise SDK bloat and a broad but individually-explicable permission surface both correct to LOW. Eight messages were sent across 70 days. The only inbound reply was an automated bug-bounty redirect minutes after the first message, which RFI-IRFOS explicitly declined to use and named as a GDPR-inappropriate deflection channel the same day. No further reply, automated or human, was ever received.

ID	Severity	Title
C1	CRITICAL	Continuous Screen Recording Active During Live Therapy Sessions
C2	HIGH	Therapy Engagement Behavioral Data Shared Across Four Marketing Platforms
H1	MEDIUM	Health Connect Mindfulness Writes With No Verified Boundary From the Marketing Stack
H2	MEDIUM	Hardcoded Firebase API Key in the Production Binary
H3	LOW	Enterprise Barcode-Scanner SDK Shipped in the Consumer APK
H4	LOW	Broad Permission Surface Disproportionate in Combination

Subject & Operator Analysis

Headspace Health, Inc. is a US-based global mental health platform offering meditation content, live therapy sessions with licensed therapists over WebRTC, and Ebb, an AI voice journaling assistant. The Austrian DSB and CERT.at have jurisdiction over EU users.

A Bug-Bounty Redirect on a Mental Health Data Finding

Within minutes of the initial disclosure, bugbounty@headspace.com replied with a standard HackerOne submission link. RFI-IRFOS declined to use it and explained the same day, in writing, why a security triage queue is the wrong venue: it has no authority to evaluate the lawfulness of special-category mental health data processing, assess a data processing agreement with a third-party vendor, or determine an Art. 44 transfer basis. Those decisions require a DPO, legal counsel, and executive leadership. RFI-IRFOS named this response explicitly as Pattern 7, Scope Deflect / Bug Bounty Redirect, and escalated directly to privacy@ and legal@headspace.com six days later, copying the Austrian DSB. No reply of any kind, automated or human, was received on any address across the following eight messages and ten weeks.

Findings

C1: Continuous Screen Recording Active During Live Therapy Sessions

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.

Sentry RRWeb Session Replay, 72 active compiled classes, is a continuous screen-recording system, not an error-triggered screenshot tool. WindowManagerSpy monitors the active window state; RRWebIncrementalSnapshotEvent records incremental UI changes continuously; ReplayRecorderCallbacks streams the recording to Sentry's US infrastructure. This runs on the same screens where users conduct live WebRTC video and audio therapy sessions with licensed therapists and speak to Ebb, an AI voice journaling assistant, about their mental state, emotions, anxiety, depression, and trauma. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because this is the single most sensitive finding across the entire audit campaign, continuous screen recording active during live therapy sessions about mental health crises, transmitted to a third country with no confirmed transfer mechanism.

```
io/sentry/android/replay/WindowManagerSpy
io/sentry/rrweb/RRWebIncrementalSnapshotEvent
io/sentry/flutter/ReplayRecorderCallbacks
Sentry Session Replay class count: 72, io.sentry.attach-screenshot: enabled
```

Impact: The screen of a person speaking to their therapist about the worst period of their life is continuously captured and transmitted to a US third party, on a platform whose entire value proposition depends on users believing the session is private.

Fix: Disable session replay on all screens rendering therapy or voice-journaling content,

or restrict capture to error-triggered snapshots with sensitive views explicitly masked. No confirmation that this has occurred was ever received.

C2: Therapy Engagement Behavioral Data Shared Across Four Marketing Platforms

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.

Amplitude (517 classes), Braze (1,059 classes), Facebook's install-referrer attribution provider, and Google's advertising ID process therapy-engagement behavioral data, how often a user opens the app, which therapy features they use, how long sessions last, simultaneously across four separate systems. A per-user cumulative revenue metric (p ly_user_cumulated_revenues_in_usd) is layered on top of this same behavioral profile.

```
Amplitude: 517 classes -> api2.amplitude.com/2/httpapi
Braze: 1059 classes
content://com.facebook.katana.provider.InstallReferrerProvider
ply_user_cumulated_revenues_in_usd (per-user financial profile)
```

Impact: Mental health engagement behavior, how often and how long a user engages with therapy features, is processed across four simultaneous marketing systems and layered with a per-user financial profile, with no documented Art. 9(2) basis specific to this combination.

Fix: Separate therapy-engagement telemetry from the general marketing SDK stack, and document a specific Art. 9(2) legal basis for any processing that remains combined. No confirmation that this has occurred was ever received.

H1: Health Connect Mindfulness Writes With No Verified Boundary From the Marketing Stack

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 app writes mindfulness and meditation session data to Android Health Connect via WRITE_MINDFULNESS. The same APK simultaneously runs Amplitude, Braze, Facebook attribution, and Sentry session replay. The architectural boundary between Health Connect writes and the active marketing SDK stack is not verifiable from static analysis, and any leakage between them involves Art. 9 special-category health data.

Impact: Health Connect positions itself as a secure health-data store, but its actual isolation from an active marketing SDK stack in the same binary cannot be confirmed from the outside.

Fix: Publish or make independently verifiable the technical isolation between Health Connect writes and the marketing SDK stack. No confirmation that this has occurred was ever received.

H2: Hardcoded Firebase API Key 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.

A Firebase API key, database URL, and app ID are hardcoded and extractable from the production binary.

```
AIzaSyCH8JfZk8Kbw6SKvzFeGsrWLA-x0SHJDX4
firebase_database_url: https://api-8729136757784200493-667569.firebaseio.com
```

Impact: The key is trivially extractable; depending on the security-rule configuration behind it, this could enable unauthorized access or quota-exhaustion denial of service.

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

H3: Enterprise Barcode-Scanner SDK Shipped in the Consumer APK

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.

Zebra Technologies' Enterprise Mobility Development Kit (EMDK), a hardware SDK for enterprise barcode scanners, is present in the consumer APK, confirmed by com.symbol.emdk.permission.EMDK and B2B-specific assets in the binary. This supports Headspace's B2B enterprise access-provisioning feature but ships to every consumer install regardless of whether an employer is involved.

Impact: Every consumer who downloads Headspace from the Play Store receives enterprise barcode-scanner permissions with no functional reason, a data-protection-by-design gap, not an active exploitation path.

Fix: Split the B2B enterprise-provisioning SDK into a separate build target from the consumer app. No confirmation that this has occurred was ever received.

H4: Broad Permission Surface Disproportionate in Combination

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.

FOREGROUND_SERVICE_MICROPHONE, SYSTEM_ALERT_WINDOW, READ_CALENDAR, WRITE_CALENDAR, and CALL_PHONE are all present. Each has an individually plausible functional explanation, but combined with active continuous session replay and four marketing SDKs, the aggregate permission surface is disproportionate for a meditation application.

Impact: No single permission here is individually alarming, but the aggregate surface, considered alongside the session-replay and marketing-SDK findings above, exceeds what data minimisation under Art. 5(1)(c) calls for.

Fix: Review each permission against a documented, specific feature justification and remove any without one. 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. 9(1), Art. 5(1)(f), Art. 32, Art. 44	C1	Continuous screen recording during live therapy sessions, transmitted to a US third party.
Art. 9(1), Art. 5(1)(b), Art. 26	C2	Therapy-engagement behavioral data shared across four marketing platforms.
Art. 9(1), Art. 5(1)(b)	H1	Health Connect mindfulness writes with no verified boundary from the marketing stack.
Art. 32(1)(b)	H2	Hardcoded Firebase API key.
Art. 25, Art. 5(1)(c)	H3	Enterprise barcode-scanner SDK shipped to every consumer install.
Art. 5(1)(c)	H4	Broad permission surface disproportionate in combination.

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 is held at CRITICAL under an explicit, stated blast-radius escalation beyond its computed HIGH/8.7 band. C2 corrects to HIGH on its own computed band. H1 and H2 correct to MEDIUM, and H3 and H4 correct to LOW, all on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: com.getsomeheadspace.android.