Security & Privacy Disclosure, Final Report

SnoreLab for Android (com.snorelab.app)

A bedroom microphone that records the person next to you, and a Data Safety label that says nothing is shared.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. FIRST REPLY RECEIVED ON 20 NOVEMBER 2026, ASKING FOR CORRECTIONS. PUBLISHED ON THE EMBARGO DATE, NO EXTENSION REQUESTED.

Target	Reviva Softworks Ltd, 10c Printing House Yard, Hackney Road, London E2 7PR, United Kingdom
Versions Audited	2.32.1.7317 / versionCode 73170 (analysed 2026-08-23). Google Play listing showed an update on 2026-08-11.
Supervisory Authority	No EU establishment disclosed. Datenschutzbehörde (Austria) copied. ICO (United Kingdom) is the operator's domestic regulator.
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 2 High, 5 Medium, 4 Low (six from the first notice, re-assessed, and five added)
Status	FIRST REPLY ON 20 NOVEMBER 2026, 89 days after the notice, asking that the report be corrected before publication. The operator statements in it are stated by the operator, not verified by RFI-IRFOS. No extension was requested.
SHA-256 (base APK)	`f81694bc3560adc33993636f5abb938186b3ff35401e3fb9d21b4be8e3e563c7`

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 4

2 Finding Status at a Glance 7

3 Subject & Operator Analysis 8

4 Architecture & Data Flow 8

5 Findings 9

5.1 C1: Whole-room, all-night microphone capture with no isolation of the account holder from a bed partner, feeding on-device apnea-risk models 9

5.2 C2: Google Play Data Safety says "No data shared with third parties" while the operator's own policy names six recipient platforms and the package contains advertising SDKs 11

5.3 C3: Firebase and the Facebook SDK initialize at process start, before any consent screen, for free users and paying subscribers alike 12

5.4 H1: A class named EliLillyAnalytics tracks a pharmaceutical sleep-apnea marketing card that sits on the result screen of the in-app apnea-risk questionnaire 13

5.5 H2: The Segment analytics pipeline and the Google Mobile Ads SDK are compiled in and not named in the privacy policy's platform table 14

5.6 H3: Firebase, legacy Fabric and Facebook client keys are hardcoded in the distributed package 15

5.7 H4: PEGI 3 rating and a demographic profile with age on an app that records bedroom audio, with no age gate located 16

5.8 H5: UK-established controller, special-category health data of EU users at scale, and no Art. 27 EU representative disclosed 16

5.9 M1: SnoreLabContentProvider is exported with no permission guard 17

5.10 M2: network_security_config.xml permits cleartext traffic globally and sets no certificate pinning 18

5.11 M3: Firebase Remote Config is wired into the on-device audio DSP runtime . . 19

6 Impact Analysis 20

7 The Complete Chain 20

8 Health Data & Bystanders 21

9 Data Protection: Article by Article 21

10 Regulatory & Legal Landscape 22

11 Indicators of Compromise & Reproducible Evidence 23

12 Operator Response of 20 November 2026 24

13 Disclosure Timeline & Outcome 25

14 What SnoreLab Got Right 25

15 Residual Risk & Recommendations 26

Executive Summary

SnoreLab is a snoring and sleep recorder published on Google Play by Reviva Softworks Ltd of London, with more than 5 million installs. Its core function is to record the bedroom all night through the phone microphone. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF SNORELAB-2026-R1 after a root level code analysis of version 2.32.1.7317. It described three Critical and three High findings and asked three written questions.

Two findings carry the case. The first is the recording itself. The operator's own copy says the results may be affected by ambient noise and bed partners, so the microphone does not separate the account holder from the person next to them. That audio feeds on-device apnea-risk models and, for Premium subscribers with Cloud Backup, can be transferred to the operator's server. The second is a contradiction between two public statements: the Google Play Data Safety page says no data is shared with third parties, while the operator's privacy policy names six recipient platforms and describes cross-app tracking.

The package also contains a class named EliLillyAnalytics that counts views and taps of a pharmaceutical sleep-apnea campaign card next to the app's own apnea-risk questionnaire result. Further findings are ordinary but real: Firebase and the Facebook SDK start before any consent screen, advertising and analytics SDKs are missing from the recipient table, client keys are readable in the package, no EU representative is disclosed, and a ContentProvider is exported without a permission.

This report is stricter than the first notice. The six findings of the notice are all reassessed. The three Critical labels become High, High and Medium, and the three High labels become Medium, Medium and Medium, for the reasons given in each finding. Five further findings from the same analysis, namely client keys, the age gate, an exported provider, the cleartext setting and the remote-config surface, were not itemised in the notice and are added here at Medium, Low, Low, Low and Low. Where a data flow depends on control flow or a server that was not examined, the finding says UNVERIFIED.

The operator received the notice on 23 August 2026, a follow-up on 12 September, a reminder on 17 October and a further notice on 15 November. No acknowledgment, ticket number or reply arrived until 20 November 2026, when the SnoreLab Team answered seven points and asked that the report be corrected before publication. The operator's statements, among them that the Data Safety listing was updated, that the Facebook SDK is absent from the iOS app and that the code identified as Segment is the Customer.io SDK, are stated by the operator, not verified by RFI-IRFOS and are set out in the section Operator Response. The operator asked for no later date, so the report is published on 21 November 2026, 90 days after delivery.

Scope: Root level code analysis of SnoreLab 2.32.1.7317 (versionCode 73170): a 76.18 MB base.apk (79,878,879 bytes) with 5 dex files of about 39.9 MB, extracted from a split-APK bundle of 95,812,828 bytes. The analysis covers AndroidManifest.xml, decoded resources, the bundled model and asset files and the dex string pool (238,544 lines). A full bytecode disassembly was not run, so findings that depend on the order of calls inside a method are marked UNVERIFIED. Public web pages read by plain HTTP GET on 23 August 2026: the Google Play listing, the Google Play Data Safety page and the operator's privacy policy. No account was created, no SnoreLab server was called, no key was tested, no traffic was captured and no runtime instrumentation was used. The package was obtained from a public mirror (APKPure) because the audit device was not reachable that day, and the developer name Reviva Softworks Ltd was confirmed against the Google Play listing. Whether the audited build is the build Google Play served on the date of the notice was not confirmed. CVSS v4.0 measures exploitability. Most findings here are data-governance findings with no attacker, so the printed scores are low and four findings carry an explicit blast-radius escalation.

ID	Severity	Title
C1	HIGH	Whole-room, all-night microphone capture with no isolation of the account holder from a bed partner, feeding on-device apnea-risk models
C2	HIGH	Google Play Data Safety says ”No data shared with third parties” while the operator’s own policy names six recipient platforms and the package contains advertising SDKs
C3	MEDIUM	Firebase and the Facebook SDK initialize at process start, before any consent screen, for free users and paying subscribers alike
H1	MEDIUM	A class named EliLillyAnalytics tracks a pharmaceutical sleep-apnea marketing card that sits on the result screen of the in-app apnea-risk questionnaire
H2	MEDIUM	The Segment analytics pipeline and the Google Mobile Ads SDK are compiled in and not named in the privacy policy’s platform table
H3	MEDIUM	Firebase, legacy Fabric and Facebook client keys are hardcoded in the distributed package
H4	LOW	PEGI 3 rating and a demographic profile with age on an app that records bedroom audio, with no age gate located
H5	MEDIUM	UK-established controller, special-category health data of EU users at scale, and no Art. 27 EU representative disclosed
M1	LOW	SnoreLabContentProvider is exported with no permission guard
M2	LOW	network_security_config.xml permits cleartext traffic globally and sets no certificate pinning
M3	LOW	Firebase Remote Config is wired into the on-device audio DSP runtime

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Answered 20 November 2026. Operator states the policy covers other people in the room; no legal basis named for the bed partner. Not verified. Reassessed.
C2	CRITICAL	HIGH	Answered 20 November 2026. Operator states the Data Safety listing was updated. Not verified. Reassessed.
C3	CRITICAL	MEDIUM	Answered 20 November 2026. Operator states the iOS app has no Facebook SDK and the references are leftover configuration being removed. Not verified. Reassessed.
H1	HIGH	MEDIUM	Answered 20 November 2026. Operator denies any data sent to Eli Lilly. Not verified. Reassessed.
H2	HIGH	MEDIUM	Answered 20 November 2026. Operator states the code is the Customer.io SDK. Not verified. Reassessed.
H3	Not itemised	MEDIUM	Added in this report. Client keys.
H4	Not itemised	LOW	Added in this report. Age gate.
H5	HIGH	MEDIUM	Operator states on 20 November 2026 that it is reviewing the Art. 27(2) exemption. Reassessed.
M1	Not itemised	LOW	Added in this report. Exported provider.
M2	Not itemised	LOW	Added in this report. Cleartext setting.
M3	Not itemised	LOW	Added in this report. Remote config.

Subject & Operator Analysis

The operator is Reviva Softworks Ltd, 10c Printing House Yard, Hackney Road, London E2 7PR, United Kingdom. The developer name on Google Play, Reviva Softworks Ltd, matches the name on the mirror download. The notice went to support@snorelab.com and android@snorelab.com, the Android support address named in Play Store developer replies. The Play developer contact address is team@reviva.works. No dedicated press or privacy-officer address was found.

The operator is not established in the Union and discloses no EU main establishment, so no lead supervisory authority exists under Art. 56 GDPR. The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the first notice for transparency. The UK Information Commissioner's Office is the operator's domestic regulator.

SnoreLab is a freemium app. The free version shows ads and a Premium subscription adds Cloud Backup and BreathFlow trend history. The Google Play listing shows PEGI 3, more than 5 million installs, a rating of 4.3 from 52.4 thousand reviews, the Health and Fitness category and the labels Contains ads and In-app purchases.

Architecture & Data Flow

- Audio capture: RECORD_AUDIO and two microphone foreground services, SnoreDetectionService and SnoreDetectionServiceV2 (C1).
- On-device models: desaturation, hypopnea and snore-end models plus a MobileNet file, with BreathFlow and apnea epoch classes in the dex pool (C1).
- Local storage: WavFile and AudioSession, with playback activities for recordings and a deletion activity.
- Cloud Backup: Premium feature, per-user encrypted audio stored on the operator's server according to the privacy policy (C1).
- Start-up: FirebaseInitProvider with initOrder 100 and directBootAware, Facebook SDK with automatic initialization and advertising ID collection (C3).
- SDKs: Firebase, Segment, Google Mobile Ads, Facebook, AppsFlyer, Customer.io and a legacy Fabric key (C2, H2, H3).
- Pharmaceutical touchpoint: EliLillyAnalytics and an Eli Lilly campaign card on the apnea-risk result flow (H1).
- Remote Config: DSPRuntimeRemoteConfig flags for the audio runtime (M3).
- Exported component: SnoreLabContentProvider (M1). Network configuration permits cleartext (M2).

What this report does not show is any payload that leaves the phone. Where a statement depends on it, the finding says UNVERIFIED.

Findings

C1: Whole-room, all-night microphone capture with no isolation of the account holder from a bed partner, feeding on-device apnea-risk models

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from CRITICAL in the first notice, rated HIGH by blast-radius escalation

The app runs two microphone foreground services and the operator's own copy says its results "may be affected by ambient noise and bed partners". The audio is written to a local WAV file and processed by bundled desaturation and hypopnea models. For Premium subscribers with Cloud Backup, recordings can be transferred to the operator's server, encrypted with a per-user key according to the privacy policy. The policy speaks only to the account holder and has no provision for a second person in the recording.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to HIGH because CVSS gives local processing with no demonstrated exposure 0.0. The finding is rated HIGH because the people affected are partners and household members, possibly children, who cannot see, consent to or object to the capture, because the audio is health-related, and because the app has more than 5 million installs on Google Play. CRITICAL, as disclosed on 23 August 2026, is withdrawn because upload is limited to opted-in Premium subscribers with per-user encryption stated by the operator, and because no per-person identification feature exists in the package.

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE_MICROPHONE"/>
<service android:exported="false" android:foregroundServiceType="microphone"
    android:name="com.snorelab.app.audio.SnoreDetectionService"/>
<service android:exported="false" android:foregroundServiceType="microphone"
    android:name="com.snorelab.app.service.tracking.SnoreDetectionServiceV2"/>
```

```
<string name="BREATHING_METRICS_CAVEAT">SnoreLab metrics are based on acoustic
    patterns and may be affected by ambient noise and bed partners.</string>
<string name="DISTURBANCES_FOOTNOTE">"Scores are based on acoustic patterns and may be
     affected by ambient noise and bed partners. SnoreLab statistics should not be
    viewed as medical advice. "</string>
```

```
assets/retrained_ends_model.tflite                                21.5K
assets/..._events_desat_model.tflite                            21.8K
assets/..._two_stage_hypopnea_desats_model.tflite               21.8K
Lcom/snorelab/app/audio/storage/WavFile;
Lcom/snorelab/app/model/BreathFlowDataType;
ApneaEpochHasEndProbabilityExtreme / ApneaEpochHasEndProbabilityNormal
apnea_risk_test_result_button_tapped / apnea_risk_test_completed
```

Privacy policy, read live on 23 August 2026: "Audio recordings of your snoring... Stored on your device. Only collected by us if you have subscribed to Cloud Backup or opted in to

research. Recordings in Cloud Backup are encrypted." and "Audio recordings are encrypted using a unique key for each user before being transferred and stored on our server". Cloud Backup is a Premium feature (PREMIUM_CLOUD_BACKUP_TITLE: "Premium feature: Cloud Backup").

Observed fact: continuous whole-room capture with no per-person isolation, by the operator's own written admission, local processing by health-adjacent models, optional upload for subscribers. Legal inference: a co-sleeper has acoustic data, and through the model pipeline derived breathing data, captured and in the Premium case stored, without a notice, an account or a route to object. The policy's rights and retention sections address only "you". This app has no per-person identification feature. The sibling sleep tracker in this wave ships a voice-identity classifier, and SnoreLab does not. Attribution of model outputs and operator access to uploads were not tested.

GDPR: Art. 9(1), Art. 9(2), Art. 6(1), Art. 5(1)(e), Art. 14, Art. 13(1)(e), Art. 13(2)

Impact: A spouse or partner who shares a bed with a SnoreLab user has their own breathing and snoring recorded every night, run through the same apnea-risk models as the account holder and, if the account holder pays for Cloud Backup, stored on a UK company's server. The account holder can replay the recording at will. The partner is not told and cannot object.

Fix: State in the policy that other people in the room are recorded, give the Art. 6 and Art. 9(2) basis, offer an Art. 14 route for non-users and set a retention limit for uploaded recordings.

C2: Google Play Data Safety says "No data shared with third parties" while the operator's own policy names six recipient platforms and the package contains advertising SDKs

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), reassessed from CRITICAL in the first notice, rated HIGH by blast-radius escalation

The live Data Safety page for com.snorelab.app states "No data shared with third parties". The privacy policy, section 4, names Firebase, BigQuery, Customer.io, Google Forms, AppsFlyer and AWS as recipients and describes AppsFlyer as enabling third parties to track activity across apps and websites. The package also contains a Google Mobile Ads SDK and a Meta SDK that collects the advertising identifier.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the label is the first and often the only disclosure a user reads, the app processes breathing and sleep data of more than 5 million installs, and the operator's own policy describes cross-app tracking. CRITICAL, as disclosed on 23 August 2026, is withdrawn because several of the named recipients are plausibly processors and the form classification of each flow was not established.

Play Store Data Safety page, fetched 2026-08-23, verbatim: "No data shared with third parties. The developer says that this app doesn't share user data with other companies or organisations." Data collected per the same page: app interactions, device or other IDs, crash logs, diagnostics, other app performance data and email address. Security practices: data is encrypted in transit, and data deletion can be requested.

```
Firebase (Google)      email, UUID, device data, country, permissions, demographic
    data
BigQuery (Google Cloud) UUID
Customer.io            email, UUID, device data, country, permissions, demographic
    data
Google Forms           name, email, testimonial content
AppsFlyer              AppsFlyerID, UUID, advertising data, purchase data, device data
    ,
                       permission data, country, demographic data, install, session
    and app-open data
                       (policy wording: enables "third parties to track your activity
    across apps and websites")
AWS                    UUID, demographic data, device data, Apple Health data
```

```
https://googleads.g.doubleclick.net/mads/gma
https://pagead2.googlesyndication.com/pagead/gen_204
https://admob-gmats.uc.r.appspot.com/
com.google.android.libraries.ads.mobile.sdk.common.AdActivity
```

Observed fact: two public statements by the same operator about the same app disagree. Not every recipient in the policy table is a third party in the Play sense. Firebase, BigQuery, AWS and similar processors acting on the operator's behalf are commonly treated as service providers. AppsFlyer, the advertising SDK and the Meta advertising identifier are harder to place under that reading, and the policy's own AppsFlyer wording describes cross-app tracking. Which flows Google's form classifies as sharing depends on contract and purpose

details that are not visible in the package. That is why this report rates the finding HIGH and not CRITICAL.

GDPR: Art. 5(1)(a), Art. 13(1)(e), Art. 12(1)

Impact: A person choosing a sleep app that records their bedroom reads the Data Safety label first. The label tells them nothing is shared, while the operator's own policy describes tracking across apps. The label is the disclosure that most users see, and for a health-related app it sets the expectation about who else receives their data.

Fix: Correct the Data Safety declaration so that it matches the policy and the package, name the advertising and attribution recipients in both documents, and state which recipients are processors and which are independent controllers.

C3: Firebase and the Facebook SDK initialize at process start, before any consent screen, for free users and paying subscribers alike

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), reassessed from CRITICAL in the first notice

FirebaseInitProvider is declared with initOrder 100 and directBootAware true, and the Facebook SDK is configured with AutoInitEnabled, AutoLogAppEventsEnabled and AdvertiserIDCollectionEnabled all set to true. A ContentProvider runs when Android binds the process, before any activity can show a consent screen. The behaviour does not depend on the subscription state, and the manifest declares com.android.vending.BILLING.

```
<provider android:authorities="com.snorelab.app.firebaseinitprovider" android:
    directBootAware="true"
    android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<meta-data android:name="com.facebook.sdk.ApplicationId" android:value="@string/
    facebook_app_id"/>
<meta-data android:name="com.facebook.sdk.AutoInitEnabled" android:value="true"/>
<meta-data android:name="com.facebook.sdk.AutoLogAppEventsEnabled" android:value="true
    "/>
<meta-data android:name="com.facebook.sdk.AdvertiserIDCollectionEnabled" android:value
    ="true"/>
```

The app does show an onboarding tickbox (PRIVACY_TICKBOX_TERMS_PRIVACY: "I have read and agree to the Terms of Use and Privacy Notice"). That screen is an Activity, and Activities start after ContentProviders and application-level SDK initialization. The Facebook flags are an advertising SDK with automatic event logging, which is a heavier case than analytics alone. Whether the app overrides these flags in code before the first network call is a call-order question that the string pool cannot decide and is UNVERIFIED. The first notice rated this CRITICAL. This report rates it MEDIUM because the evidence is a manifest fact and no transmitted payload was observed.

GDPR: Art. 7(1), Art. 5(1)(a), Art. 5(2), Art. 6(1), ePrivacy Directive Art. 5(3)

Impact: A subscriber who pays to use the app gets the same start-up behaviour as a free user, with an advertising SDK among the components that start before any choice is possible. What that start-up transmits was not measured.

Fix: Disable automatic initialization for Firebase and the Facebook SDK in the manifest, start both after the consent state is known, and state in the policy what Premium changes for analytics and advertising.

H1: A class named EliLillyAnalytics tracks a pharmaceutical sleep-apnea marketing card that sits on the result screen of the in-app apnea-risk questionnaire

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), reassessed from HIGH in the first notice

The dex pool contains a dedicated analytics class for an Eli Lilly obstructive-sleep-apnea awareness card, with events for card visibility, first tap and tap. The card links to a UTM-tagged Eli Lilly campaign page, and a button string attached to the apnea-risk test result reads ”Talk to a Doctor About Obstructive Sleep Apnea”. Neither Eli Lilly nor a pharmaceutical marketing relationship appears in the privacy policy.

```
Lcom/snorelab/app/analytics/EliLillyAnalytics;
Lcom/snorelab/app/analytics/EliLillyAnalytics$Origin;
eliLillyCardVisible
eliLillyQuestionnaireButtonVisible
eliLillyTouchpointFirstTapped
eli_lilly_touchpoint_first_tapped
eli_lilly_touchpoint_tapped
showCardEliLilly
showEliLillyQuestionnaireButton
talk_to_a_doctor_eli_lilly
https://dontsleeponosa.lilly.com?utm_source=snorelab&utm_medium=referral&utm_campaign=
    cy25_dse-osa_awareness_p4&utm_content=pp-zp-us-1490
https://go.lilly.com/sleep-apnea-2
```

```
<string name="APNEA_RISK_TEST_RESULT_BUTTON_LILLY">Talk to a Doctor About Obstructive
    Sleep Apnea</string>
<string name="CARD_ELI_LILLY_TITLE">"Don't Sleep On OSA"</string>
<string name="CARD_ELI_LILLY_DETAIL">Learn how to recognize and manage moderate-to-
    severe obstructive sleep apnea symptoms. </string>
```

Observed fact: a branded pharmaceutical campaign link, a card and first-party engagement events for it exist in the package, and the button string belongs to the apnea-risk result flow. Not shown: whether the card is displayed only to users whose questionnaire result indicates risk, since the string pool shows names and not control flow. Not shown: whether the engagement events reach Eli Lilly or stay in SnoreLab’s own analytics (Firebase, Segment, Customer.io). Both points are UNVERIFIED. The first notice rated this HIGH. This report rates it MEDIUM because those two points decide the weight of the finding and neither is established.

GDPR: Art. 13(1)(c), Art. 13(1)(e), Art. 9(1), Art. 9(2), Art. 5(1)(a)

Impact: A person who completes the apnea-risk questionnaire and is worried about a health condition is shown a named pharmaceutical company’s awareness campaign in the same flow, and the app counts whether they looked at it and tapped it. The policy does not say that a pharmaceutical partner is involved.

Fix: Name the pharmaceutical relationship and the purpose in the privacy policy, state whether any data reaches Eli Lilly, state whether display of the card depends on the questionnaire result, and obtain explicit consent before a health-risk result triggers any promotional content.

H2: The Segment analytics pipeline and the Google Mobile Ads SDK are compiled in and not named in the privacy policy's platform table

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), reassessed from HIGH in the first notice

The dex pool contains the Segment analytics-kotlin SDK (com/segment/analytics/kotlin/core) and the Google Mobile Ads footprint listed in C2. The privacy policy section 4 names Firebase, BigQuery, Customer.io, Google Forms, AppsFlyer and AWS only. Even reading the policy against the package without the Play label, two SDK integrations are missing from the recipient table.

Segment is a customer-data pipeline that can forward events to many downstream destinations, so its presence says little about the end recipient and a lot about the need to name them. The Play listing carries the label Contains ads, so the advertising SDK is not a surprise to the user. The gap is that the policy does not name the recipient. The first notice rated this HIGH. This report rates it MEDIUM because it is a disclosure gap with no demonstrated payload and the ad label is public.

GDPR: Art. 13(1)(e), Art. 5(1)(a)

Impact: Users cannot find out from the policy which companies receive their event data. For an app that records sleep, the recipient list is the information a person needs before deciding whether to use the free version with ads.

Fix: Add Segment, the Google advertising SDK and every downstream Segment destination to the recipient table with purposes and legal basis.

H3: Firebase, legacy Fabric and Facebook client keys are hardcoded in the distributed package

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), added in this report, not itemised in the first notice

res/values/strings.xml holds the Firebase project identifiers and a Google API key, the manifest holds a legacy Fabric ApiKey, and the Facebook app id is in the resources. All are extractable with apktool from any Play Store download.

```
<string name="firebase_database_url">https://snorelab-app.firebaseio.com</string>
<string name="gcm_defaultSenderId">1080675189825</string>
<string name="google_api_key">AIzaSyDX_9MKTxzS91sXOf5oMb8iyYYob4w0yqU</string>
<string name="google_app_id">1:1080675189825:android:d3e5d025d894ef25</string>
<string name="project_id">snorelab-app</string>
<string name="facebook_app_id">148684738637073</string>
```

```
<meta-data android:name="io.fabric.ApiKey" android:value="317
    c36cf1de901704f126d4549ec013f35141fc3"/>
```

These are client identifiers. Google, Fabric and Facebook do not treat them as confidentiality secrets, and the reportable risk is availability and integrity of the event streams (quota exhaustion, spoofed events), not confidentiality. No key was tested against any server. The Fabric key is notable because Fabric and Crashlytics were folded into Firebase years ago, and its presence points to a legacy integration that may no longer be monitored. The burden of showing that key restrictions and backend rules are in place lies with the operator under Art. 5(2). This report rates it MEDIUM because no server-side weakness was shown.

GDPR: Art. 32(1)(b), Art. 5(2)

Impact: Anyone can read the keys from the public app. The effect on users is indirect: analytics streams that feed profile and engagement data could be polluted, and project quotas could be consumed.

Fix: Restrict each key by package name and signing certificate where the vendor allows it, enforce App Check for Firebase, remove the legacy Fabric key if the integration is dead, and review the Firebase database rules for the project snorelab-app.

H4: PEGI 3 rating and a demographic profile with age on an app that records bedroom audio, with no age gate located

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), added in this report, not itemised in the first notice

The Play Store rating is PEGI 3. The privacy policy lists demographic data (sex, age, weight, height) collected at onboarding and profile setup. No minimum-age string, parental-consent flow or age-enforcement string was found in the resource dump.

PEGI rates content and not data processing, so the rating is not a defect by itself. The practical exposure is a minor who shares a room with an adult user (C1) and a minor account holder. Art. 8 is not engaged for an adult account holder. This report rates it LOW because the absence of a gate is a statement about what was not found in a string dump, the app is not directed at children, and no age claim by the operator is contradicted.

GDPR: Art. 8, Art. 25, Art. 5(1)(c)

Impact: A young person could create an account without any age-appropriate handling, and a child asleep in the room can be recorded without anyone having considered that case.

Fix: Add an age-appropriate consent path or state the minimum age, and address the minor-bystander case in the DPIA for C1.

H5: UK-established controller, special-category health data of EU users at scale, and no Art. 27 EU representative disclosed

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from HIGH in the first notice, rated MEDIUM by blast-radius escalation

Reviva Softworks Ltd is registered at 10c Printing House Yard, Hackney Road, London E2 7PR. The UK is a third country for GDPR purposes. The privacy policy describes automatic collection of respiratory rate, breathing disturbances, sleep stages and motion activity, optional BMI which the policy itself labels health data, and optional audio recordings, for an app with more than 5 million installs. A full-text search of the policy for "representative", "Article 27" and "EU representative" returned no matches, and no representative is listed on the Play developer page.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because CVSS has no metric for a missing legal representative and gives 0.0. The finding is rated MEDIUM because the operator processes special-category health data of EU users at a scale of more than 5 million installs and the representative is the route through which rights are exercised. HIGH, as disclosed on 23 August 2026, is withdrawn because a designation may exist outside the documents that were searched.

Art. 3(2) brings a controller outside the Union within scope when it offers services to people in the Union. Art. 27(1) then requires a written designation of a representative in the Union. The Art. 27(2)(a) exemption covers processing that is occasional, does not involve special categories on a large scale and is unlikely to result in a risk. Automatic nightly collection of health data at this scale does not read as occasional. The EU adequacy arrangement for the UK concerns transfers to the UK and does not change Art. 3(2) or Art. 27.

Observed fact: no representative is named in the two places searched. Not shown: whether one has been designated and simply not published. If one exists, Art. 13(1)(a) still requires the controller's information to name the representative and give contact details. The first notice rated this HIGH. This report rates it MEDIUM because it is a governance gap whose existence outside the published documents is UNVERIFIED.

GDPR: Art. 27(1), Art. 3(2), Art. 13(1)(a)

Impact: A person in the Union who wants to exercise a right against a company in London has no local contact to write to, and a supervisory authority has no local address to serve.

Fix: Designate an EU representative in writing, name and address them in the privacy policy and in the Play developer information, and document why the Art. 27(2)(a) exemption does not apply.

M1: SnoreLabContentProvider is exported with no permission guard

---

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), added in this report, not itemised in the first notice

A custom ContentProvider is declared exported with no readPermission, writePermission or path-permission. Any other app on the same device can address content://com.snorelab.app.contentprovider without holding a SnoreLab permission. This is separate from the FileProvider used for share intents.

```
<provider android:authorities="com.snorelab.app.contentprovider" android:exported="
    true"
    android:name="com.snorelab.app.contentprovider.SnoreLabContentProvider"/>
```

This is the manifest-level gap. What the provider returns to a caller cannot be read from a resources decompile, and its query and insert bodies were not disassembled. The data exposure is UNVERIFIED. This report rates it LOW because the demonstrated impact is a declaration and not a data leak.

GDPR: Art. 32(1)

Impact: If the provider returns session data, another app on the phone could read sleep and snoring records without the user's knowledge. Whether it does so is not established.

Fix: Set exported to false unless an external caller needs the provider, or protect it with a signature-level permission, and check the caller in query and insert.

M2: network_security_config.xml permits cleartext traffic globally and sets no certificate pinning

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), added in this report, not itemised in the first notice

base-config sets cleartextTrafficPermitted to true, which applies to every domain without a specific override, and no pinning is configured. No traffic was captured, so no cleartext transmission is shown.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors><certificates src="system" /></trust-anchors>
    </base-config>
    <debug-overrides>
        <trust-anchors><certificates src="user" /></trust-anchors>
    </debug-overrides>
</network-security-config>
```

This is a configuration finding and not a demonstrated interception. The missing pinning is a hardening gap and not a vulnerability by itself. This report rates it LOW because an attacker would need a position on the local network and a cleartext request, and none was observed.

GDPR: Art. 32(1)

Impact: On an untrusted network, any request the app or an embedded SDK sends over plain HTTP could be read or altered by someone nearby. Which requests do so is not established.

Fix: Set cleartextTrafficPermitted to false in base-config and list the few domains that need an exception, and consider pinning for the operator’s own backend.

M3: Firebase Remote Config is wired into the on-device audio DSP runtime

LOW, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), added in this report, not itemised in the first notice

A class DSPRuntimeRemoteConfig with a Flags subclass exists next to the generic remote-config repository and fetch use case. The naming indicates a remote-config surface scoped to the audio processing runtime. This is a capability finding. It shows that the operator's backend can change parameters of the audio pipeline without an app update. It does not show that any flag changes recording behaviour.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS has no metric for a capability that the operator holds over its own pipeline and gives 0.0. The finding is rated LOW because the surface touches the microphone pipeline and users are not told about it. A higher rating is not supported because only a class name is evidenced.

```
Lcom/snorelab/app/remoteconfig/DSPRuntimeRemoteConfig;
Lcom/snorelab/app/remoteconfig/DSPRuntimeRemoteConfig$Flags;
Lcom/snorelab/app/remoteconfig/FirebaseRemoteConfig;
com.snorelab.app.usecase.FetchRemoteConfigUseCase
com.snorelab.app.remoteconfig.RemoteConfigRepository
```

Remote Config for detection thresholds is a normal engineering practice. The flags and their effect are UNVERIFIED without a bytecode pass or runtime instrumentation. This report rates it LOW because the evidence is a class name.

GDPR: Art. 5(1)(a), Art. 13

Impact: The behaviour of a microphone pipeline that runs in the bedroom can be changed from the operator's side. Users are not told which parameters are controlled remotely.

Fix: State in the policy that audio-processing parameters can be changed remotely, document which flags exist, and confirm that no flag can extend what is recorded or uploaded.

Impact Analysis

- Bed partners and household members. They are recorded every night, run through the same apnea-risk models as the account holder, and for Premium accounts may be stored on the operator's server, without a notice or a way to object (C1). Children who share a room are included by the physical setting.
- Users who read the Data Safety label. They are told nothing is shared while the operator's own policy describes tracking across apps (C2).
- Users who complete the apnea-risk questionnaire. A pharmaceutical campaign is placed in that flow and engagement with it is counted (H1).
- All users. Firebase and the Facebook SDK start before they can choose (C3), advertising and analytics recipients are missing from the policy (H2), client keys are public (H3), and no EU contact exists for the operator (H5).

The Complete Chain

- 1. A person installs SnoreLab and places the phone by the bed. At process start Firebase and the Facebook SDK initialize before any consent screen (C3).
- 2. The app records the night. On the device, models extract breathing and apnea-related events from audio that the app's own copy says may include a bed partner.
- 3. If the user subscribes to Cloud Backup, recordings are encrypted with a per-user key and stored on the operator's server (C1).
- 4. After the apnea-risk questionnaire the user sees a pharmaceutical campaign card, and the app counts the view and the tap (H1).
- 5. The policy names six recipients and omits Segment and the advertising SDK, while the Data Safety label says nothing is shared (C2, H2).
- 6. The user, or the partner, asks who is responsible and where to send a request. No EU representative is named (H5), and the operator's answer to the notice so far is silence.

Each later section of this report refers to one of these six links. The harm is that the most private setting a person has, sleep, is recorded with a partner as an unnamed participant and described to the public in two documents that disagree.

Health Data & Bystanders

Art. 9(1) GDPR covers data concerning health. Breathing rate, breathing disturbances, sleep stages and an apnea-risk result are health-related, and the operator's own policy treats BMI as health data. The account holder is covered by a legal-basis table that assigns performance of contract, legitimate interest or consent to each purpose. That table is a real strength. It does not mention the second person in the room.

Art. 14 requires information for data not obtained from the data subject, and the bystander has no account through which a notice could reach them. Whether the household exemption of Art. 2(2)(c) covers the account holder does not decide the operator's own position, because the operator designed and sells the whole-night recording product and stores the audio for subscribers. This app has no voice-identity feature, so the bystander is present as sound in the room and not as a labelled person. The operator was asked on what basis it processes a person who never saw a consent screen. The question is open.

Data Protection: Article by Article

Article	How it is engaged
Art. 3(2), 27	UK controller, no EU representative disclosed (H5).
Art. 5(1)(a)	Transparency. Data Safety label contradicts the policy (C2), recipients missing (H2), pharmaceutical touchpoint unnamed (H1).
Art. 5(1)(e)	Storage limitation. No retention period for a bystander in a stored recording (C1).
Art. 6(1)	Legal basis for bystander audio (C1) and for pre-consent start-up (C3).
Art. 7	Consent must come first. Firebase and the Facebook SDK start before the tickbox screen (C3).
Art. 8	Child's consent. Relevant to a minor account holder and a minor bystander (H4, C1).
Art. 9(1), 9(2)	Breathing and apnea-risk data, bystander audio, risk-triggered pharmaceutical content (C1, H1).
Art. 12(1), 13(1)(a), 13(1)(c), 13(1)(e), 13(2)	Representative, purposes and recipients must be stated accurately (H5, H1, H2, C2).
Art. 14	Information for data not obtained from the data subject. No route to the bystander (C1).
Art. 25	Data protection by design. Bystander and minor cases (C1, H4).
Art. 32(1)	Security of processing. Client keys, exported provider, cleartext setting (H3, M1, M2).
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.

Article	How it is engaged
Art. 35	DPIA for large-scale health data and the bystander case.
ePrivacy Directive Art. 5(3)	Access to information on the terminal device (C3).

Regulatory & Legal Landscape

The operator has no EU main establishment, so the one-stop-shop does not apply and any EU authority may act on a complaint. The Datenschutzbehörde and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: the privacy policy is better structured than most in this wave, with a legal basis for each data type, a rolling 12-month anonymization rule for inactive non-subscribers and a CSV export for portability. The weakness is not structure. It is that the structure addresses one person per recording.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The bundle was obtained from APKPure as a split-APK file and base.apk was extracted and hashed. Google Play search confirmed that the package hinted in an earlier working note, com.snorelab.app.snoring, does not exist, and that the subject package is com.snorelab.app.

```
Package       com.snorelab.app
Version       2.32.1.7317 / versionCode 73170
base.apk      76.18 MB (79,878,879 bytes)
base.apk      SHA-256 f81694bc3560adc33993636f5abb938186b3ff35401e3fb9d21b4be8e3e563c7
XAPK bundle   95,812,828 bytes
XAPK bundle   SHA-256 555367d9a52f330f57aa5ac8c971f15442c976707eb267839cc44893309c2ce1
Firebase      project snorelab-app, sender 1080675189825
              app 1:1080675189825:android:d3e5d025d894ef25
              google_api_key AIzaSyDX_9MKTxzS91sXOf5oMb8iyYYob4w0yqU
Fabric        io.fabric.ApiKey 317c36cf1de901704f126d4549ec013f35141fc3
Facebook      app id 148684738637073
```

```
https://snorelab-app.firebaseio.com
https://googleads.g.doubleclick.net/mads/gma
https://pagead2.googlesyndication.com/pagead/gen_204
https://admob-gmats.uc.r.appspot.com/
https://dontsleeponosa.lilly.com?utm_source=snorelab&utm_medium=referral&utm_campaign=
    cy25_dse-osa_awareness_p4&utm_content=pp-zp-us-1490
https://go.lilly.com/sleep-apnea-2
https://play.google.com/store/apps/datasafety?id=com.snorelab.app
```

```
Operator contacts  support@snorelab.com, android@snorelab.com, team@reviva.works
Postal address     10c Printing House Yard, Hackney Road, London E2 7PR, United
    Kingdom
```

Operator Response of 20 November 2026

On 20 November 2026 at 17:06 UTC the SnoreLab Team (support@snorelab.com) replied to the reminder of 17 October 2026, 89 days after the original notice. The reply opens with the request "We ask that you correct your report before publishing anything" and answers seven points. Every statement below is stated by the operator, not verified by RFI-IRFOS.

- 1. EliLillyAnalytics (H1): the operator states that Eli Lilly is a US affiliate partner, that it does not share user data with Eli Lilly, that the class records events "in our own analytics only", that a user who follows the link sees a card labelled "Independent Affiliate Link", and that it provides Lilly with an aggregate report each month under an affiliate arrangement.
- 2. Segment (H2): the operator states that the code identified is the Customer.io SDK, which is built on an open-source library, and that the privacy notice lists Customer.io as a processor. The report identified the package path com/segment/analytics/kotlin/core. The operator says it only collects emails and sends email marketing through Customer.io to users who opt in.
- 3. Facebook (C3): the operator states the report is "incorrect for the iOS app, which contains no Facebook SDK" and that the references found are "leftover configuration, which we are removing". The report analysed the Android build 2.32.1.7317, so the statement about the iOS app does not describe the audited build. The announced removal is not confirmed by any build.
- 4. Advertising (C2, H2): the operator states that users of the ad-supported version see ads through Google AdMob and that it does not send personalised or targeted ads.
- 5. Audio and other people in the room (C1): the operator states that the privacy notice says recordings may capture others in the room and requires users who opt in to Audio Research or Cloud Backup to inform third parties and obtain their consent, that Cloud Backup is solely for storage and recovery, and that "The Audio Research is to train our audio models". The reply names no legal basis for the bed partner.
- 6. Google Play Data Safety listing (C2): the operator states that the listing has been updated and is consistent with the privacy notice. RFI-IRFOS has not re-checked the live listing for this report, which describes the declaration as audited.
- 7. EU representative (H5): the operator states that it is established in the UK with no EU establishment and is reviewing whether the exemption under Art. 27(2) EU GDPR continues to apply. If it does not, it will appoint a representative under Art. 27(1) and update the privacy notice.

RFI-IRFOS records the request to correct the report. The operator did not ask for a later publication date, and the embargo date of 21 November 2026 was given in each notice. The report is therefore published on 21 November 2026 as it stands, with the operator's statements recorded in this section. The findings, severities and technical evidence are unchanged, because the reply names no build or observation that contradicts them.

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 2.32.1.7317. Notice REF SNORELAB-2026-R1 sent to support@snorelab.com and android@snorelab.com, copied to the Datenschutzbehörde and the EDPS. Three written questions.
2026-09-12	Follow-up on the same thread. Six findings restated. Answer to the three questions requested by 19 September 2026.
2026-10-17	Reminder, 35 days before publication. Three questions unchanged.
2026-11-15	Notice, 6 days before publication, from RFI-IRFOS with the reassessed grades for H2 to H5 and M1 to M3. No acknowledgment, ticket number or reply had been received on any earlier message. No bounce was received for any message.
2026-11-20	Reply from the SnoreLab Team (support@snorelab.com). Requests that the report be corrected before publication and answers seven points. The statements are stated by the operator, not verified by RFI-IRFOS. No extension of the publication date was requested.
2026-11-21	Publication, 90 days after delivery of the notice, on the embargo date given in every notice.

The operator received the same embargo date in every message. No request to extend it was made and none was granted. The first reply from the operator arrived on 20 November 2026, one day before publication.

What SnoreLab Got Right

- Cloud Backup audio is described as encrypted with a unique key for each user before transfer, and the operator states that it cannot listen to recordings unless a user sends them. This is a concrete commitment that can be checked.
- A granular in-app deletion function exists (SettingsDeleteAudioActivity and the storage-limit activities), so users can remove recordings without deleting the account.
- The privacy policy has a legal basis for each data type, a 12-month rolling anonymization rule for inactive non-subscribers, and CSV export for portability.
- Users who installed before 1 July 2025 and never subscribed to Cloud Backup are limited to UUID, country, app metrics, technical data and usage data until they opt in.
- RECORD_AUDIO is a runtime permission, so the account holder must grant microphone access through the Android dialog before any recording starts.

Residual Risk & Recommendations

All eleven findings are rated as audited. The operator replied on 20 November 2026 and disputes parts of C1, C2, C3, H1 and H2 in the statements recorded in the section Operator Response, and announced a review of the Art. 27 position. RFI-IRFOS has not verified these statements. Versions after 2.32.1.7317 are not covered by this report.

- State in the policy that other people in the room are recorded, give the legal basis, and open an Art. 14 route for non-users.
- Correct the Data Safety declaration and name every recipient, including Segment and the advertising SDK.
- Start Firebase and the Facebook SDK after the consent state is known.
- Name the pharmaceutical relationship, say whether data reaches Eli Lilly, and obtain explicit consent before a health-risk result triggers promotional content.
- Restrict the client keys, enforce App Check and retire the Fabric key.
- Designate and publish an EU representative.
- Protect or remove the exported ContentProvider and disable cleartext traffic.
- Answer the three written questions.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published application plus the operator’s public policy and Google Play pages. No SnoreLab servers or accounts were probed and no key was tested. Severity per CVSS v4.0 (CVSS-B) with explicit blast-radius escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF SNORELAB-2026-R1.