Security & Privacy Disclosure, Final Report

Sleep Cycle for Android (com.northcube.sleepcycle)

A voice-identity model for the person next to you in bed, and a consent text that still cites the Privacy Shield.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. ONLY AUTOMATED ACKNOWLEDGEMENTS AND A TEMPLATE REPLY, NO TECHNICAL REPLY.

Target	Sleep Cycle AB, Reg. No. 556614-7368, Drakegatan 10, 412 50 Gothenburg, Sweden
Versions Audited	4.26.25-production / versionCode 9787 (analysed 2026-08-23). Google Play showed a later update on 2026-08-14.
Supervisory Authority	IMY, Sweden (country of main establishment)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	8: 2 High, 4 Medium, 2 Low (seven from the first notice, re-assessed, and one added)
Status	NO TECHNICAL REPLY AS OF 21 NOVEMBER 2026. Automated ticket acknowledgements and one template reply (16 November 2026) only.
SHA-256 (base APK)	`b0e512fcdf0ce63ec2593849a2b3578b4ce1939ee5111512582075668a7e44da`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Findings 6

5.1 C1: "Who's Snoring": a voice-identity model that tells a bed partner's snoring apart from the account holder's . . . 6

5.2 C2: "Teratron" whole-night raw-audio upload to US-hosted Google infrastructure, with a consent document that cites the invalidated EU-U.S. Privacy Shield 8

5.3 C3: Firebase initializes at process start through a directBootAware ContentProvider, for free users and paying subscribers alike . . . 10

5.4 H1: Three SDK client keys hardcoded in the distributed binary: Firebase, Amplitude, Braze . . . 11

5.5 H2: SleepAnalysisService is exported with foregroundServiceType location|microphone and no permission guard . . . 12

5.6 H3: Firebase, Adjust and Braze are compiled in and not named in the privacy policy . . . 13

5.7 H4: Date-of-birth field and PEGI 3 rating with no age gate located, on an app that records bedroom audio . . . 13

5.8 M1: Privacy Sandbox and AD_ID permissions on a sleep and health-adjacent app, with Adjust attribution . . . 14

6 Impact Analysis 14

7 The Complete Chain 15

8 Health Data, Biometrics & Bystanders 15

9 Data Protection: Article by Article 16

10 Regulatory & Legal Landscape 17

11 Indicators of Compromise & Reproducible Evidence 17

12 Disclosure Timeline & Outcome 18

13 What Sleep Cycle Got Right 19

14 Residual Risk & Recommendations 19

Executive Summary

Sleep Cycle is a sleep tracker published on Google Play by Sleep Cycle AB of Gothenburg, Sweden, with more than 10 million installs. Its core function is to listen to a sleeping person through the phone microphone. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF SLEEPCYCLE-2026-R1 after a root level code analysis of version 4.26.25. It described three Critical and four High findings and asked three written questions.

Two findings carry the case. The first is a feature called Who's Snoring. The app ships a voice-identity model and a classifier whose stated purpose is to tell the account holder's snoring apart from that of someone who sleeps nearby, and the person identified is typically a partner who never installed the app. The second is an audio diagnostics programme, Teratron, that uploads whole nights of raw sound to Google infrastructure in the United States. The operator's own consent document for the programme, live in 2026, tells participants that the transfer rests on the EU-U.S. Privacy Shield Framework, which the Court of Justice invalidated in July 2020.

The other findings are ordinary but real: Firebase starts before any consent screen, three SDK client keys are readable in the package, an exported service guards the microphone-based analysis without a permission, three processors are missing from the privacy policy, and a date of birth is collected without an age gate.

This report is stricter than the first notice. The seven findings of the notice are all reassessed. The three Critical labels are reduced to High, High and Medium because the evidence shows on-device processing for Who's Snoring, an opt-in programme for Teratron and only a manifest fact for Firebase. The four High labels are reduced to Medium, Medium, Medium and Low, for the reasons given in each finding. One further finding from the same analysis, the advertising permissions in M1, was not itemised in the notice and is added here at Low.

Sleep Cycle's support desk acknowledged the notice by automated ticket 267166 on the day it was sent. A notice of 15 November 2026 listing C1 to C3, H1 to H4 and M1 received automated ticket 270173. On 16 November 2026 an agent named Alice wrote "Thank you for contacting us. What can we help you with?" and on 19 November 2026 the desk sent a satisfaction survey for ticket 270173. No technical reply, no answer to the three questions and no statement on the findings has arrived. The report is published on 21 November 2026, 90 days after delivery, whether or not the operator answers.

Scope: Root level code analysis of Sleep Cycle 4.26.25-production (versionCode 9787), a 4-dex package of about 37.6 MB with an 86.29 MB bundle: AndroidManifest.xml, decoded resources, bundled model assets and the dex string pool. Public web pages read by plain HTTP GET on 23 August 2026: the Google Play listing, sleepcycle.com/privacy-policy and sleepcycle.com/sleep-cycle-privacy-information-sound. No account was created, no Sleep Cycle server was called, no key was tested and no runtime instrumentation was used. The audited build is the newest release available from a public mirror at the time. Google Play showed an update on 14 August 2026, so the build on Google Play at the date of the notice may differ from the audited build. CVSS v4.0 measures exploitability. Most findings here are data-governance findings with no attacker, so the printed scores are low and two findings carry an explicit blast-radius escalation.

ID	Severity	Title
C1	HIGH	”Who’s Snoring”: a voice-identity model that tells a bed partner’s snoring apart from the account holder’s
C2	HIGH	”Teratron” whole-night raw-audio upload to US-hosted Google infrastructure, with a consent document that cites the invalidated EU-U.S. Privacy Shield
C3	MEDIUM	Firebase initializes at process start through a directBootAware ContentProvider, for free users and paying subscribers alike
H1	MEDIUM	Three SDK client keys hardcoded in the distributed binary: Firebase, Amplitude, Braze
H2	MEDIUM	SleepAnalysisService is exported with foregroundServiceType location|microphone and no permission guard
H3	MEDIUM	Firebase, Adjust and Braze are compiled in and not named in the privacy policy
H4	LOW	Date-of-birth field and PEGI 3 rating with no age gate located, on an app that records bedroom audio
M1	LOW	Privacy Sandbox and AD_ID permissions on a sleep and health-adjacent app, with Adjust attribution

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	No answer to the legal-basis and retention question. Reassessed.
C2	CRITICAL	HIGH	No answer to the transfer-mechanism question. Reassessed.
C3	CRITICAL	MEDIUM	No answer to the pre-consent question. Reassessed.
H1	HIGH	MEDIUM	No reply. Client keys. Reassessed.
H2	HIGH	MEDIUM	No reply. Reassessed.
H3	HIGH	MEDIUM	No reply. Reassessed.
H4	HIGH	LOW	No reply. Reassessed.
M1	Not itemised	LOW	Added in this report. Advertising permissions.

Subject & Operator Analysis

The operator is Sleep Cycle AB, Swedish registration number 556614-7368, Drakegatan 10, 412 50 Gothenburg. The company is established in the Union, so no Art. 27 representative is needed. Its privacy contact is privacy@sleepcycle.com and its support contact is support@sleepcycle.com. The developer name on Google Play, Sleep Cycle AB, matches the name on the mirror download.

Because the country of main establishment is Sweden, the lead supervisory authority under Art. 56 GDPR is IMY (Integritetsskyddsmyndigheten). The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the first notice for transparency. The operator's own consent document still names the predecessor authority Datainspektionen.

A look-alike app named Sleep Cycle from a different developer (package com.lambent_labs.sleep_cycle_tracker_smart_alarm_sleep_recorder) exists on a download mirror. It is not the subject of this report and was not downloaded. The subject package is com.northcube.sleepcycle.

Architecture & Data Flow

- Audio capture: RECORD_AUDIO is the product. The app records the bedroom to detect movement, breathing and snoring and to stage sleep.
- On-device models: eleven bundled models for mel spectrograms, FFT, breathing rate, sleep staging, a general sound-event model, a triplet-loss snore embedding and a GCC-PHAT direction model, shipped in assets/ (C1).
- Who's Snoring: KNN classifier over per-person embeddings, calibration with Me Samples and Not Me Samples, stored clips presented to the user for labelling (C1).
- Audio diagnostics programme: Teratron uploader and dumper to Cloud Run in us-central1 and to App Engine projects, behind an activation dialog and an opt-in consent page (C2).
- Start-up: FirebaseInitProvider with initOrder 100 and directBootAware (C3).
- SDKs: Firebase (ten subsystems), Adjust, Braze, Amplitude (H1, H3, M1).
- Exported component: SleepAnalysisService with foregroundServiceType location|microphone (H2).
- Network configuration: network_security_config.xml has no custom trust anchors, no cleartext override and no user-CA trust.

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: ”Who’s Snoring”: a voice-identity model that tells a bed partner’s snoring apart from the account holder’s

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 ships a triplet-loss embedding model, a k-nearest-neighbour classifier over per-person embeddings, a calibration flow with Me Samples and Not Me Samples, a GCC-PHAT time-difference-of-arrival model and a repository that serves stored clips back to the user for labelling. The operator’s own copy states the purpose: ”Differentiate your snoring from others’, even if they sleep near you. We show some clips, you tell us who is snoring.”

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to HIGH because CVSS gives on-device processing with no demonstrated exposure 0.0. The finding is rated HIGH because the people affected are bystanders, partners and possibly children sharing a bedroom, who cannot see, consent to or object to the processing, because the purpose is a voice-identity classification, and because the app has more than 10 million installs on Google Play. CRITICAL, as disclosed on 23 August 2026, is withdrawn because transmission of clips to the operator outside the opt-in programme was not demonstrated.

```
assets/audio_to_mel_spectrogram.ort.enc     280.5K   mel spectrogram feature
    extraction
assets/auroracle.ort.enc / auroracle_0.4.0.tflite   6.9M   general sound-event model
assets/breathing_rate.ort.enc / breathing_rate_android.tflite   breathing-rate
    detection
assets/gcc_phat_fft.ort.enc                  75.0K   Generalized Cross-Correlation
    Phase Transform, time difference of arrival
assets/realtime_sleep_staging.ort.enc        3.8M
assets/snoracle-tripletloss-epoch=285-val_loss=0.07.tflite   3.3M   triplet-loss
    embedding model
assets/snore_signature.ort.enc               3.3M   "snore signature" model
```

```
Lcom/northcube/sleepcycle/soundanalysis/ml/SnoracleTripletlossEpoch285ValLoss007;
Lcom/northcube/sleepcycle/soundanalysis/SnoraclePcaProcessor;
Lcom/northcube/sleepcycle/soundanalysis/SnoraclePrediction;
Lcom/northcube/sleepcycle/model/whoissnoring/Snorer;
n(Lcom/northcube/sleepcycle/model/whoissnoring/Snorer;)Lcom/northcube/sleepcycle/
    soundanalysis/SnoreKnn$Snorer;
Lcom/northcube/sleepcycle/whoissnoring/AnnotatedSnoreRepository;
Lcom/northcube/sleepcycle/whoissnoring/
    AnnotatedSnoreRepository$updateAudioFileAnnotationsSdk$1;
Lcom/northcube/sleepcycle/model/whoissnoring/SnoreEventDao;
SNORACLE_EMBEDDING_SIZE
SNORACLE_ME_SAMPLES / SETTINGS_SNORACLE_ME_SAMPLES        "Snoracle - Me Samples"
SNORACLE_NOT_ME_SAMPLES / SETTINGS_SNORACLE_NOT_ME_SAMPLES  "Snoracle - Not Me Samples
    "
GCCPhatResult(tdoa=
com.sleepcycle.sdk.SleepCycleSdk$computeSnoreSignatures$2
```

```
<!-- res/values/strings.xml line 871 -->
<string name="about_who_is_snoring">Differentiate your snoring from ’others, even if
    they sleep near you. We show some clips, you tell us who is snoring. We give you
    the answers. The more you use it, the better we become at automatically
    recognizing snoring. Beyond being able to say ‘it ’wasnt ’me, you get a clear
    picture of how much you and the one you share a bed with snore.</string>
<!-- line 1643-1644 -->
<string name="pw_feature_who_is_snoring">- Settle debate and find out whos really
    snoring.</string>
<string name="pw_feature_who_is_snoring_heading">"Who's snoring"</string>
<!-- line 57 -->
<string name="About_snore_detection_forever">Audio recordings will never be discarded.
     If ’youre a snorer, this might add up to quite a lot of data, so keep an eye on
    the memory used.</string>
```

Triplet loss is the standard training objective for identity embeddings. The privacy policy describes one multi-person mechanism, the mutual and deactivatable partner link, which requires both people to be registered Sleep Cycle users on the same WiFi. ”Who’s Snoring” has no such requirement in the shipped copy and no matching disclosure in the roughly 22,000 character policy.

Reading of the retention string: it says audio recordings will never be discarded and adds ”keep an eye on the memory used”. That remark points to storage on the phone, so the string supports storage without an automatic limit and does not by itself show that Sleep Cycle AB holds these recordings. Whether clips or embeddings reach the operator outside the opt-in programme described in C2 is UNVERIFIED. For that reason this report rates C1 HIGH, reassessed from the CRITICAL label of the first notice.

GDPR: Art. 9(1), Art. 6(1), Art. 5(1)(e), Art. 14, Art. 13(1)(e), Art. 35

Impact: A person who shares a bed with a Sleep Cycle user can have their snoring recorded and classified against a voice-identity model, and clips of it are replayed to the account holder for a verdict. That person saw no notice and has no way to object.

Fix: Describe the feature and the bystander in the policy, state the Art. 6 and Art. 9(2) basis or confirm on-device processing, and publish a retention limit with automatic deletion for clips and embeddings.

C2: ”Teratron” whole-night raw-audio upload to US-hosted Google infrastructure, with a consent document that cites the invalidated EU-U.S. Privacy Shield

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 binary contains an upload pipeline named Teratron with an uploader, a dumper, sensor, snore-alert, snore-event and annotation data objects, an activation dialog and a setting called Dump whole night. Its endpoints are a Google Cloud Run service in us-central1 and Google App Engine projects. The operator’s separate consent document for this audio development programme, live on 23 August 2026 with the footer Copyright 2026 Sleep Cycle AB, states that sound recordings are listened to and annotated, may be linked to age, gender, BMI and nationality, and are transferred to the USA to recipients ”certified under the EU-U.S. Privacy Shield Framework”.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the recordings are whole nights of sleep sound, human personnel listen to them, and the safeguard that participants are told about is a framework invalidated more than five years before the document’s own copyright year. CRITICAL, as disclosed on 23 August 2026, is withdrawn because the programme is opt-in and an unlawful transfer was not demonstrated.

```
https://teratron-52ktn6hzxa-uc.a.run.app/                          Google Cloud Run,
    us-central1
https://mdlabs-sleepcycle.appspot.com                               Google App Engine
https://mdlabs-sleepcycle.appspot.com/api/v2/fileupload/init        raw file upload
    endpoint
https://mdlabs-sleepcycle-test2.appspot.com                         staging
    counterpart
api/v1/teratron/{appId}/{deviceId}/{clientSessionId}
api/v1/teratron/{appId}/{deviceId}/{clientSessionId}/{fileName}
api/v1/teratron/fileupload/init
```

```
Lcom/northcube/sleepcycle/service/teratron/TeratronApi;
Lcom/northcube/sleepcycle/logic/teratron/TeratronUploader;
Lcom/northcube/sleepcycle/logic/teratron/TeratronDumper;
Lcom/northcube/sleepcycle/service/teratron/dto/TeratronSensorData;
Lcom/northcube/sleepcycle/service/teratron/dto/TeratronSnoreAlert;
Lcom/northcube/sleepcycle/service/teratron/dto/TeratronSnoreEvent;
Lcom/northcube/sleepcycle/service/teratron/dto/TeratronAnnotation;
Lcom/northcube/sleepcycle/service/teratron/AccessTokenInterceptor;
Lcom/northcube/sleepcycle/ui/TeratronActivationDialogActivity;
PREFS_TERATRON_ENABLED / PREFS_SHOW_TERATRON_SETTINGS_ENABLED
```

```
<string name="Enable_teratron_info">Enable audio diagnostics.</string>
<string name="Enable_teratron_user_prompt">"You are logged in as %1$s, make sure it's
    your intended user id!"</string>
<string name="Teratron_settings_title">Audio diagnostics</string>
<string name="Teratron_dump_whole_night">Dump whole night</string>
```

Consent document, https://sleepcycle.com/sleep-cycle-privacy-information-sound, read on 23 August 2026, verbatim: ”The personal data that we will process about you based on this consent is a recording of the sounds you make during your sleep. We may also process personal data available through your profile such as age, gender, BMI (Body Mass Index) and nationality and connect this to the sound recording.” Further: ”We will listen to the sound recordings and annotate certain events during the night such as snoring, breathing, movements and other sounds.” Further: ”Your personal data will, as a main rule, be disclosed to and processed by entities only within the EU and EEA. Your personal data will however be transferred to and stored by entities in the USA. The recipients of personal data in the USA are certified under the EU-U.S. Privacy Shield Framework.” The complaint authority is named as ”Datainspektionen, Box 8114, 104 20 Stockholm”, the name used before the authority became IMY in 2021.

Observed fact: a currently published document dated 2026 names the EU-U.S. Privacy Shield Framework as the safeguard for a transfer to the USA. The Court of Justice invalidated that framework on 16 July 2020 (Case C-311/18, Schrems II). Its successor, the EU-US Data Privacy Framework, was adopted in July 2023 and is a different instrument. Not shown: which mechanism the transfer relies on today, whether the programme reaches ordinary users or only enrolled participants, and whether the activation setting is visible to them. The activation prompt asks the person to confirm ”your intended user id”, which reads like an enrolment step, and the programme has its own opt-in consent page. These points are UNVERIFIED. This report rates C2 HIGH, reassessed from the CRITICAL label of the first notice, because what is demonstrated is a defective safeguard citation in the consent text of an opt-in programme and not an unlawful transfer.

GDPR: Art. 44, Art. 46, Art. 13(1)(f), Art. 5(1)(a), Art. 12(1), Art. 7(2), Art. 9(2)(a)

Impact: Sleep Cycle users who join the audio programme are asked to consent on the basis of a transfer safeguard that has not existed since 2020, for recordings of themselves asleep that staff listen to. Informed consent depends on being told the real safeguard. The same document names a complaint authority that no longer exists under that name.

Fix: Replace the Privacy Shield text with the mechanism actually used (adequacy decision, certification or standard contractual clauses), name IMY as the authority, and re-collect consent from participants on the corrected text.

C3: Firebase initializes at process start through a directBootAware ContentProvider, 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. A ContentProvider of this kind runs when Android binds the process, before any activity can show a consent screen and before the device is unlocked. The behaviour does not depend on the subscription state, and the manifest declares com.android.vending.BILLING and com.android.vending.CHECK_LICENSE.

```
<provider android:authorities="com.northcube.sleepcycle.firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
```

Ten Firebase subsystems are compiled in: analytics, auth, crashlytics, remoteconfig, messaging, sessions, appcheck, installations, iid and heartbeatinfo. Whether Firebase Analytics collects data before the user answers a consent dialog is a call-order question that the string-pool analysis cannot decide and is UNVERIFIED. That is why this report rates C3 MEDIUM, reassessed from the CRITICAL label of the first notice. The same manifest pattern is a standard Firebase default, so the rating follows the demonstrated fact.

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

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

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

H1: Three SDK client keys hardcoded in the distributed binary: Firebase, Amplitude, Braze

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), reassessed from HIGH in the first notice

res/values/strings.xml contains a Google API key (also used as crash-reporting key), an Amplitude API key and a Braze API key, together with the Firebase project identifiers. All three are extractable with apktool from any Play Store download.

```
<string name="google_api_key">AIzaSyBoG7lz9oByfd2lFK20XhQ5HIyXz_34Lmw</string>
<string name="google_crash_reporting_api_key">AIzaSyBoG7lz9oByfd2lFK20XhQ5HIyXz_34Lmw
    </string>
<string name="amplitude_api_key">d086ccbe66bc91014cb07347dde9a000</string>
<string name="com_braze_api_key">fbbfe7ca-d4ba-4e29-b74b-e18415bb6d39</string>
<string name="firebase_database_url">https://sleep-cycle-android.firebaseio.com</
    string>
<string name="project_id">sleep-cycle-android</string>
<string name="google_app_id">1:750103287646:android:e31e327a15fb09b0</string>
```

These are client keys. Google, Amplitude and Braze do not treat them as 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 burden of showing that backend rules and key restrictions are in place lies with the operator under Art. 5(2). The first notice rated this HIGH. This report rates it MEDIUM, in line with the treatment of Firebase client keys elsewhere in the programme.

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 and messaging 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, review Braze and Amplitude settings for write access from client keys, and rotate any key that is not a client identifier by design.

H2: SleepAnalysisService is exported with foregroundServiceType location|microphone and no permission guard

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

The service that owns the microphone-based sleep and snore analysis is declared exported with intent filters for alarm actions and has no android:permission attribute. Another app on the same device that knows the action strings can send them to the service, including stop, snooze and reschedule for a wake alarm.

```
<service android:exported="true" android:foregroundServiceType="location|microphone"
    android:name="com.northcube.sleepcycle.sleepanalysis.SleepAnalysisService">
    <property android:name="android.app.PROPERTY_SPECIAL_USE_SLEEP_ANALYSIS" android:
    value="Sleep Cycle base sleep analysis"/>
    <intent-filter>
        <action android:name="com.northcube.sleepcycle.ACTIVATE_ALARM"/>
        <action android:name="com.northcube.sleepcycle.SNOOZE_ALARM"/>
        <action android:name="com.northcube.sleepcycle.RESCHEDULE_ALARM"/>
        <action android:name="com.northcube.sleepcycle.STOP_ALARM"/>
        <action android:name="com.northcube.sleepcycle.STOP_ALARM_SOUND_ONLY"/>
        <category android:name="com.northcube.sleepcycle.SLEEP_ANALYSIS_SERVICE"/>
    </intent-filter>
</service>
```

The action namespace is narrow and app-specific, and no generic control surface is exposed. Whether the service accepts and honours these actions from a foreign caller at runtime was not tested. The first notice rated this HIGH. This report rates it MEDIUM because the demonstrated impact is manipulation of an alarm by a co-resident app.

GDPR: Art. 32(1)

Impact: A malicious app on the same phone could silence or move a wake alarm. The microphone itself is not shown to be reachable by a third party.

Fix: Set exported to false where the intent filter is not needed from outside, or protect the service with a signature-level permission, and verify the caller in onStartCommand.

H3: Firebase, Adjust and Braze are compiled in and not named in the privacy policy

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 binary contains ten Firebase subsystems, the Adjust attribution SDK (309 class-string hits) and Braze marketing and push automation (1,278 class-string hits, the largest non-Google SDK footprint). A full-text search of the live privacy policy (about 22,000 characters, read on 23 August 2026) for firebase, adjust, braze, google analytics and analytics returned no matches. The policy names Amplitude with a good disclosure: pseudonymised hashed ID, named sub-processor Amplitude Inc. and Amazon Web Services, retention of three years or until consent is withdrawn.

Art. 13(1)(e) requires recipients or categories of recipients. Naming each vendor is not mandatory, so the demonstrated gap is that neither the vendors nor a matching category (analytics provider, attribution provider, messaging provider) appear in the policy text that was searched. The first notice rated this HIGH. This report rates it MEDIUM on that reading.

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

Impact: A reader of the policy learns about one analytics vendor and cannot learn that attribution and messaging vendors are also in the app.

Fix: List the recipients or categories of recipients for Firebase, Adjust and Braze with purpose and legal basis, in the style already used for Amplitude.

H4: Date-of-birth field and PEGI 3 rating with no age gate located, on an app that records bedroom audio

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), reassessed from HIGH in the first notice

The profile collects a Birthday field. No minimum-age string, parental-consent flow or age-enforcement string was found in the resource dump. The Google Play rating is PEGI 3. PEGI rates content and not data processing.

The practical exposure is a bystander minor in the room (C1) and a minor account holder. Art. 8 is not engaged for an adult account holder. The first notice rated this HIGH. This report rates it LOW because the app is not directed at children, no age claim by the operator is contradicted, and the absence of a gate is a statement about what was not found.

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: Use the date of birth for an age-appropriate consent path or drop it, and address the minor-bystander case in the DPIA for C1.

M1: Privacy Sandbox and AD_ID permissions on a sleep and health-adjacent app, with Adjust attribution

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

The manifest declares ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and com.google.android.gms.permission.AD_ID and configures android.adservices.AD_SERVICES_CONFIG. Together with the Adjust SDK (H3) this indicates advertising attribution infrastructure. The privacy policy has no matching advertising-data section, and its cookie mention is the only related hit.

```
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<property android:name="android.adservices.AD_SERVICES_CONFIG" android:resource="@xml/
    ga_ad_services_config"/>
```

A declared permission shows capability and not use. This report rates it LOW and treats the disclosure gap together with H3.

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

Impact: An advertising identifier is available to attribution code in an app whose users record their sleep.

Fix: Say in the policy whether the advertising identifier is used and for what purpose, or remove the permissions.

Impact Analysis

- Bed partners and household members. They are recorded, classified against a voice-identity model and shown to the account holder as clips, without a notice or a way to object (C1). Children who share a room are included by the physical setting.
- Participants in the audio programme. They consent to whole nights of sleep sound being listened to by staff and transferred to the USA on a safeguard that was invalidated in 2020 (C2).
- All users. The Firebase start-up runs before they can choose (C3), client keys are public (H1), an alarm service can be commanded by another app (H2), three processors are not in the policy (H3, M1) and a date of birth is collected without an age gate (H4).

The Complete Chain

- 1. A person installs Sleep Cycle and places the phone by the bed. At process start Firebase initializes before any consent screen (C3).
- 2. The app records the night. On the device, models extract breathing, movement and snoring and stage the sleep.
- 3. If the user enables Who's Snoring, a classifier compares each snore against stored embeddings and presents clips so the user can say who is snoring. A partner who sleeps nearby is part of the data without being a user (C1).
- 4. If the user joins the audio programme, whole nights of raw sound go to Cloud Run and App Engine in the United States, are listened to and annotated, and may be linked to age, gender, BMI and nationality. The consent text cites the Privacy Shield (C2).
- 5. The policy names Amplitude and omits Firebase, Adjust and Braze (H3), while advertising identifier permissions are declared (M1).
- 6. The user asks who is responsible and on what basis. The operator's answer so far is an automated ticket number.

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 processed with a partner as an unnamed participant and with a transfer basis that does not exist.

Health Data, Biometrics & Bystanders

Art. 9(1) GDPR covers data concerning health and biometric data used to identify a natural person. Sleep staging, breathing rate and snoring are health-related. A triplet-loss snore signature used to tell two people apart is a biometric-style identity embedding. Whether it meets the legal definition of biometric data for the purpose of uniquely identifying a person is a question the operator has to answer in its Data Protection Impact Assessment, and Art. 35(3)(b) points to such an assessment where special-category data is processed on a large scale.

The bystander is the unusual element. 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 the feature. 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. 5(1)(a)	Transparency. Three processors absent from the policy (H3), a stale safeguard in the consent text (C2), a bystander feature without disclosure (C1).
Art. 5(1)(e)	Storage limitation. The retention string says recordings are never discarded (C1).
Art. 6(1)	Legal basis for bystander data (C1) and for pre-consent start-up (C3).
Art. 7	Consent must be informed. The programme consent cites a defunct framework (C2). Firebase starts before any choice (C3).
Art. 8	Child's consent. Relevant to a minor account holder and to a minor bystander (H4, C1).
Art. 9(1), 9(2)	Sleep and breathing data, snore identity embedding, raw sleep audio (C1, C2).
Art. 12(1), 13(1)(e), 13(1)(f), 13(2)(a)	Recipients and safeguards must be stated accurately (H3, M1, 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. Exported service, client keys (H2, H1).
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.
Art. 35	DPIA for the combination of C1 and C2.
Art. 44, 46	Transfer to the USA. The stated safeguard is invalid (C2).
ePrivacy Directive Art. 5(3)	Access to information on the terminal device (C3).

Regulatory & Legal Landscape

IMY is the lead authority for a Swedish controller. 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 Amplitude disclosure in the policy is a good model of what the missing vendors should receive. The partner link is a consensual household feature with a second account, an opt-in and a deactivation switch. Who's Snoring lacks all three properties.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The package was obtained from APKMirror because no device was available on the analysis day. The developer name was confirmed as Sleep Cycle AB against the Google Play listing.

```
Package       com.northcube.sleepcycle
Version       4.26.25-production / versionCode 9787 (build date 2026-06-23)
Bundle        90,480,425 bytes (base.apk + arm64-v8a, xxhdpi, xxxhdpi splits)
base.apk      SHA-256 b0e512fcdf0ce63ec2593849a2b3578b4ce1939ee5111512582075668a7e44da
Firebase      project sleep-cycle-android, app 1:750103287646:android:e31e327a15fb09b0
              google_api_key AIzaSyBoG7lz9oByfd2lFK20XhQ5HIyXz_34Lmw
Amplitude     d086ccbe66bc91014cb07347dde9a000
Braze         fbbfe7ca-d4ba-4e29-b74b-e18415bb6d39
```

```
https://teratron-52ktn6hzxa-uc.a.run.app/
https://mdlabs-sleepcycle.appspot.com
https://mdlabs-sleepcycle-test2.appspot.com
https://sleep-cycle-android.firebaseio.com
https://sleepcycle.com/privacy-policy
https://sleepcycle.com/sleep-cycle-privacy-information-sound
```

```
Operator contacts  privacy@sleepcycle.com, support@sleepcycle.com
Support ticket     267166 (automated acknowledgment, 2026-08-23)
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 4.26.25. Notice REF SLEEPCYCLE-2026-R1 sent to privacy@sleepcycle.com and support@sleepcycle.com, copied to the Datenschutzbehörde and the EDPS. Three written questions. Same day: automated acknowledgment, ticket 267166.
2026-09-12	Follow-up on the same thread. Asked whether the notice had been forwarded to a data protection or engineering contact, whether a fix had shipped, and which channel to use. Answer requested by 19 September 2026.
2026-10-17	Reminder, 35 days before publication. Three questions unchanged.
2026-11-15	Notice from the security team six days before publication, itemising C1 to C3, H1 to H4 and M1. Automated acknowledgement, ticket 270173, one minute later.
2026-11-16	Reply from an agent named Alice at Sleep Cycle AB: ”Thank you for contacting us. What can we help you with?” It addresses no finding and no question.
2026-11-19	Automated satisfaction survey for ticket 270173. Whether the ticket was closed is not verified.
2026-11-21	No technical reply and no answer to any question received. No bounce received for any message. Publication, 90 days after delivery of the notice, as announced in every message.

The operator received the same embargo date in every message. No request to extend it was made and none was granted.

What Sleep Cycle Got Right

- The network security configuration is empty and inherits Android's secure default: no cleartext, system CAs only.
- The Amplitude disclosure is a good model: named sub-processor, hashed identifier, a stated retention period and deletion on withdrawal.
- Partner link is a properly designed consensual household feature: second registered account, opt-in, disclosed, deactivatable.
- A data protection contact with a working address exists, and the programme consent includes a clear withdrawal route.
- The audio programme has its own opt-in consent page and is not bundled into the base policy.

Residual Risk & Recommendations

All eight findings are open. No technical answer has been given. Versions after 4.26.25 are not covered by this report.

- State the legal basis, retention limit and storage location for Who's Snoring clips and embeddings, and describe the bystander in the policy.
- Correct the transfer text in the audio programme consent, name the real mechanism and IMY, and re-collect consent.
- Start Firebase after the consent state is known.
- Restrict client keys and enforce App Check.
- Protect SleepAnalysisService with a signature permission or make it non-exported.
- List Firebase, Adjust and Braze in the policy by recipient or category.
- Use or drop the date of birth, and cover minor bystanders in the DPIA.
- 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 consent pages. No Sleep Cycle 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 SLEEPCYCLE-2026-R1.