Security & Privacy Disclosure, Final Report

Owlet Dream for Android (com.owletcare.sleep)

An infant pulse oximetry app with a careful consent design, a Data Safety card without health data, and no reply to the notice.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026.

Target	Owlet Baby Care, Inc., Lehi, Utah, USA
Version Audited	3.40.0 / 64832 (2026-08-22)
EU Representative	Osano International Compliance Services Limited, Dublin
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	7: 2 High, 5 Medium, plus 1 observation
Status	No reply as of 21 November 2026, to the notice or to the follow-ups of 17 October and 15 November 2026
SHA-256 (base APK)	`37544949e42f0d54c933d373585861e3ddb17d493738067ee4dab4f03c93286b`

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 Engagement Summary 6

6 Findings 7

6.1 H1: Play Data Safety omits health data although the listing says Medical device and the app's own documents call the data special category health 7

6.2 H2: Google Ads and Privacy Sandbox attribution stack compiled into the app that carries an infant's pulse oximetry stream 8

6.3 M1: Firebase registers 14 components through a directBootAware service, no third-party consent platform, tempered by a bespoke consent screen 9

6.4 M2: Cleartext traffic permitted app-wide and no certificate pinning 10

6.5 M3: Firebase API key and project ID hardcoded for the production project, three further database projects named 11

6.6 M4: Consent named as the legal basis for processing that the operator's own text calls necessary to provide the app 12

6.7 M5: At least nine independent third-party processors compiled into the binary, none named in the privacy documents 13

6.8 O1: The app's own strings say both that Owlet products are not medical devices and quote the FDA indications for use 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Data Protection: Article by Article 16

10 Consumer Protection & Platform Disclosures 16

11 Regulatory & Legal Landscape 17

12 Indicators of Compromise & Reproducible Evidence 18

13 Disclosure Timeline & Outcome 19

14 What Owlet Got Right 19

15 Residual Risk & Recommendations 19

Executive Summary

Owlet Dream is the companion app for the Dream Sock, an FDA-cleared wearable that measures the pulse rate and blood oxygen of infants from 0 to 18 months, and for the Owlet Cam. It is published on Google Play by Owlet Baby Care, Inc. under the package com.owletcare.sleep, rated PEGI 3 and tagged Medical device. On 22 August 2026 RFI-IRFOS disclosed two High and five Medium findings from a root level code analysis of version 3.40.0 under REF OWLETDREAM-2026-R1. No Critical finding was issued.

The operator's legal work is stronger than most in this programme. It has appointed a data protection officer on the stated ground that it processes special category health data, a correctly separated EU representative in Dublin and UK representative in Belfast, a specific consent screen that names pulse rate and oxygen saturation, and a separately revocable consent for AI sleep insights. The findings sit beside that design.

The first High finding is the store label. The Data Safety card lists six categories and no health data, while the listing says Medical device and the app's own documents call the data special category health (H1). The second is an advertising identifier and Privacy Sandbox attribution stack inside the app that carries an infant's vitals (H2). The Medium findings concern initialisation order, cleartext scope, the Firebase key, the legal basis chosen for consent and unnamed processors. The people behind these findings are parents of infants who need constant reassurance from the device and rely on the labels around it.

The notice went to privacy@owletcare.com on 22 August 2026 with the Austrian DSB and the EDPS in copy. Follow-ups on 17 October 2026 and 15 November 2026 repeated the three questions. As of 21 November 2026 no reply, automatic or otherwise, has arrived. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of the Google Play release 3.40.0 (versionCode 64832): manifest, resources, the two PDFs bundled in the APK, network security configuration and the string pool of nine classes*.dex files. The Google Play listing and Data Safety page and the owletcare.com privacy policy and terms were read from the public sites on 22 August 2026. No Owlet server, device, account or database was called, no traffic was intercepted and no runtime instrumentation was used. Items the package cannot show are marked as such.

ID	Severity	Title
H1	HIGH	Play Data Safety omits health data although the listing says Medical device and the app's own documents call the data special category health
H2	HIGH	Google Ads and Privacy Sandbox attribution stack compiled into the app that carries an infant's pulse oximetry stream
M1	MEDIUM	Firebase registers 14 components through a directBootAware service, no third-party consent platform, tempered by a bespoke consent screen
M2	MEDIUM	Cleartext traffic permitted app-wide and no certificate pinning
M3	MEDIUM	Firebase API key and project ID hardcoded for the production project, three further database projects named
M4	MEDIUM	Consent named as the legal basis for processing that the operator's own text calls necessary to provide the app
M5	MEDIUM	At least nine independent third-party processors compiled into the binary, none named in the privacy documents
O1	INFO	The app's own strings say both that Owlet products are not medical devices and quote the FDA indications for use

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
H1	HIGH	HIGH	Open. No reply to the notice or the follow-ups.
H2	HIGH	HIGH	Open. No reply.
M1	MEDIUM	MEDIUM	Open. Held as a question on initialisation order.
M2	MEDIUM	MEDIUM	Open. No reply.
M3	MEDIUM	MEDIUM	Open. No reply.
M4	MEDIUM	MEDIUM	Open. No reply.
M5	MEDIUM	MEDIUM	Open. No reply.
O1	Noted	INFO	Observation, not rated.

Subject & Operator Analysis

Google Play and the bundled Consumer Privacy Notice name Owlet Baby Care, Inc., 2940 W. Maple Loop Dr., Suite 203, Lehi, Utah 84048, USA, as the operator. The privacy contact is privacy@owletcare.com, which is also the data protection officer channel with the subject DPO Inquiry. The bundled notice states that Owlet has appointed a DPO under Article 37(1)(c) of the GDPR because it processes special category health data.

The EU representative under Article 27 is Osano International Compliance Services Limited, ATTN: SPZT, 25 North Wall Quay, Dublin 1, D01 H104, Ireland. The UK representative is a separate appointment, Osano UK Compliance LTD, 42-46 Fountain Street, Belfast, Antrim BT1 5EF. Both addresses match in the live policy and in the bundled PDF.

No EU main establishment appears on the public record. An Article 27 representative does not create one, so the one-stop-shop does not generally apply and the supervisory authorities of the affected data subjects may each act. For an Austrian initiated matter the competent authority is the Österreichische Datenschutzbehörde.

The app is signed by Owlet Baby Care, Lehi, Utah with the certificate SHA-256 7c7115349682fd3b818df49ef7816d110966e0e7e9269497ff533c57a8b90bc4 and carries a Google source stamp verified with apksigner, which supports the origin of the build from Google Play.

Architecture & Data Flow

Owlet Dream is a native Kotlin and Java app with Jetpack Compose and nine dex files. The Dream Sock and base station connect through the Ayla Networks IoT SDK, which uses BLE and an MQTT backend. The Owlet Cam video path uses ThroughTek. Per the bundled notice, the app processes pulse rate and oxygen saturation as health metrics, and a second consent covers AI-based sleep insights.

Firebase provides crash reporting, remote configuration, Firestore, messaging and storage across 14 registered components, with a production project and further EU, development and staging projects (M3). Braze, Klaviyo and Split.io provide marketing and experimentation, RevenueCat handles subscriptions, Sentry provides diagnostics including a session replay module, and Zendesk provides support (M5). A Google Ads conversion attribution path reads the advertising identifier (H2).

No AdMob ad-serving classes, no Meta SDK and no Chinese or sanctioned-jurisdiction analytics or advertising SDK were found. The specific vendor of the AI sleep insights is not identified in the package.

Engagement Summary

The notice REF OWLETDREAM-2026-R1 was sent on 22 August 2026 at 12:53 UTC to privacy@owletcare.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It listed H1 and H2, summarised five Medium findings, credited the appointed DPO, the Dublin and Belfast representatives, the consent screens and the absence of PRC analytics, and asked three questions.

A follow-up with the same three questions went to privacy@owletcare.com on 17 October 2026 at 18:50 UTC, 34 days before the embargo date. A final notice followed on 15 November 2026 at 12:58 UTC from s.kepp@rfi-irfos.com, 85 days after the notice, naming 20 November 2026 as the publication date. The thread contains no reply, no automatic acknowledgement and no delivery failure notice.

Findings

H1: Play Data Safety omits health data although the listing says Medical device and the app’s own documents call the data special category health

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), open, rated HIGH by blast-radius escalation

The Google Play listing for com.owletcare.sleep, captured on 22 August 2026, carries the tags Health & Fitness and Medical device. The Data Processing Practices bundled in the APK state that the data may include health metrics such as pulse rate and oxygen saturation. The bundled Consumer Privacy Notice describes infant physiological measurements as a special category of personal data. The Data Safety card lists six collected categories (app info and performance, personal info, location, device or other IDs, photos and videos, app activity) and no health category. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data are the pulse rate and blood oxygen of infants, the operator’s own documents call them special category health data, and the Data Safety card is the disclosure parents read before installing. The score is zero because no technical vector exists.

```
Google Play listing, category tags:
Health & Fitness
Medical device

Google Play Data Safety, captured 2026-08-22:
No data shared with third parties
Data collected
App info and performance - Crash logs, Diagnostics, and Other app performance data
Personal info - Name, Email address, User IDs, and Phone number
Location - Approximate location
Device or other IDs - Device or other IDs
Photos and videos - Photos
App activity - App interactions
Data is encrypted in transit
You can request that data be deleted
```

```
To create an account and access services on the Owlet Dream App, we need to process
    your
personal data. Depending on the devices connected to the App, this data may include
    health metrics
such as pulse rate and oxygen saturation, as well as sensor-generated data from your
    device.
```

```
Some information processed through our Products may relate to health, wellness, or
    physiological
measurements of an infant or child. Where this information is considered a special
    category of personal
data under applicable law, we process it only when permitted, including where: You
    have provided
explicit consent [...]
```

Impact: A parent comparing baby monitors reads the store label first. For this product the label shows no health data, while the same app measures the pulse and blood oxygen of an infant. The parent decides on a smaller picture than the operator's own documents describe.

Fix: Add the health category to the Data Safety declaration and align it with the bundled notices and the Medical device tag.

H2: Google Ads and Privacy Sandbox attribution stack compiled into the app that carries an infant's pulse oximetry stream

---

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 (CVSS-B), open, rated HIGH by blast-radius escalation

The manifest declares AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID. The library androidx.privacysandbox.ads-adservices is compiled in, and classes5.dex and classes7.dex call AdvertisingIdClient.getAdvertisingIdInfo(). Dex strings contain the endpoints https://pagead2.googlesyndication.com and https://www.googleadservices.com. Only the com.google.android.gms.ads.identifier sub-package is present and no ad-serving classes were found, so this is conversion attribution for the operator's own campaigns and not in-app advertising. The package does not show whether the identifier is linked to a child's vitals records on the server side. The checkable fact is that both pipelines are compiled into one app, one account and one Firebase project. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same app carries the pulse rate and blood oxygen of infants and the operator's own notices classify them as special category data. The vector scores only the exposure of an advertising identifier.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>

classes5.dex: AdvertisingIdClient
classes5.dex: getAdvertisingIdInfo
classes5.dex: Lcom/google/android/gms/ads/identifier
classes7.dex: AdvertisingIdClient
classes7.dex: getAdvertisingIdInfo

https://pagead2.googlesyndication.com
https://www.googleadservices.com
```

Impact: Install attribution infrastructure sits in the same app as a baby's heart rate and oxygen readings. A parent has no way to tell from the store label or the notices that an advertising identifier is read at all, and nothing in the notices names the purpose.

Fix: State the purpose of the advertising identifier, give the legal basis and the consent step that precedes it, and allow it to be switched off independently of monitoring.

M1: Firebase registers 14 components through a directBootAware service, no third-party consent platform, tempered by a bespoke consent screen

---

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), open

ComponentDiscoveryService is directBootAware and registers 14 Firebase components, among them Crashlytics, Auth, Remote Config, Firestore, Messaging, Storage, Analytics Connector, Installations, App Check and Datatransport. A dex-wide search for OneTrust, Didomi, Usercentrics, IABTCF and consentString found nothing. This target differs from others: the app ships a specific consent screen (consent_to_personal_and_child_data_processing) that names pulse rate and oxygen saturation, and a second consent for AI-based sleep insights (llm_consent_modal strings) that can be revoked without losing the account. The package does not show whether the Firebase components stay inactive until that screen is completed. The finding is held at MEDIUM for that reason.

```
<service android:directBootAware="true" android:exported="false"
    android:name="com.google.firebase.components.ComponentDiscoveryService">
    <meta-data android:name="com.google.firebase.components:...crashlytics.
    CrashlyticsRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...auth.
    FirebaseAuthRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...remoteconfig.
    RemoteConfigRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...firestore.
    FirestoreRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...messaging.
    FirebaseMessagingRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...storage.
    StorageRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...analytics.connector.
    internal.AnalyticsConnectorRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...installations.
    FirebaseInstallationsRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...appcheck.
    FirebaseAppCheckRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...abt.component.
    AbtRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:...datatransport.
    TransportRegistrar" .../>
    <!-- plus 3 Ktx registrar variants -->
</service>
```

Consent string, verbatim: I consent to the processing of my personal data, and my child's personal data (if applicable), as described in the Data Processing Practices. Revocation text for AI sleep insights, verbatim: Disabling this feature stops future AI processing but will not affect your ability to use the core Owlet app.

Impact: Most of the weight sits on a question the operator can answer in one sentence: do the Firebase components wait for the consent screen. The consent design itself is careful.

Fix: State whether Firebase and the other SDK components initialise before the consent screen is completed, and gate them if they do.

M2: Cleartext traffic permitted app-wide and no certificate pinning

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), open

The manifest sets usesCleartextTraffic to true. The network security configuration has no base-config and no pin-set. Its only domain-config re-permits cleartext for 192.168.0.1, a private address consistent with local setup of the base station, and does not restrict any other host. The manifest attribute therefore governs all other traffic. The configuration permits cleartext. The package does not show that vitals data travel over it, and no traffic was captured.

```
<!-- AndroidManifest.xml -->
<application android:usesCleartextTraffic="true" android:networkSecurityConfig="@xml/
    network_security_config" ...>

<!-- res/xml/network_security_config.xml, complete file -->
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <debug-overrides>
        <trust-anchors>
            <certificates src="system" />
            <certificates src="user" />
        </trust-anchors>
    </debug-overrides>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">192.168.0.1</domain>
    </domain-config>
</network-security-config>
```

Impact: The configuration is wider than the one local address that needs it. The app carries alarm data about a baby's pulse and oxygen level, so narrowing the cleartext scope is cheap and useful.

Fix: Remove usesCleartextTraffic or set a base-config that denies cleartext, keep the 192.168.0.1 exception, and plan pinning for operator-controlled hosts.

M3: Firebase API key and project ID hardcoded for the production project, three further database projects named

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), open

res/values/strings.xml of version 3.40.0 carries the production Firebase values in plain text. A dex string search found three more Realtime Database projects: owletcare-prod-eu, owletcare-dev and owletcare-staging. A Firebase key is not a secret by Google design, so the demonstrated exposure is availability through quota exhaustion. Whether the Security Rules are correct is not shown by the package, and no call was made against any project. Which project an EU install uses is not shown either.

```
<string name="firebase_database_url">https://owletcare-prod.firebaseio.com</string>
<string name="gcm_defaultSenderId">561089101102</string>
<string name="google_api_key">AIzaSyDlfp3urNTbyhCtHOCxZBOjHQf4WuN_Aws</string>
<string name="google_app_id">1:561089101102:android:7703b1c03673b7a486cebf</string>
<string name="google_crash_reporting_api_key">AIzaSyDlfp3urNTbyhCtHOCxZBOjHQf4WuN_Aws
    </string>
<string name="project_id">owletcare-prod</string>

owletcare-prod-eu.firebaseio.com
owletcare-dev.firebaseio.com
owletcare-staging.firebaseio.com
```

Impact: If the project were rate-limited, the service that carries the alarms of a baby monitor would be affected. The key stays in every installed copy until an app update replaces it.

Fix: Restrict the key by package name, signing certificate and API scope, enforce App Check, and confirm deny-by-default Security Rules for every named project.

M4: Consent named as the legal basis for processing that the operator's own text calls necessary to provide the app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), open

The bundled Data Processing Practices state that Owlet relies on consent where required by law, and in the same short document that the processing is necessary to provide the app, so that withdrawing consent ends the ability to use the app and may require deleting the account. The text is open about the consequence, which is better than hiding it. Consent that cannot be withdrawn without losing the whole service sits in tension with the freely given requirement, and contractual necessity under Article 6(1)(b) is the more coherent basis for processing that is truly necessary. This is a question of legal basis selection and not a claim that the processing is unlawful. It is a legal finding with no technical vector.

```
Where required by applicable law, we rely on your consent to process this information.
     [...]

You may withdraw your consent at any time through the Owlet Dream App settings or by
    contacting
privacy@owletcare.com. Withdrawal of your consent will not affect the lawfulness of
    any processing
conducted prior to withdrawal. However, because the processing described above is
    necessary to
provide the Owlet Dream App, withdrawing consent will end your ability to use the App,
     and you
may be required to delete your account.
```

Impact: A parent is told that consent is the basis and that refusing it means no app. The parent should know which of the two is true.

Fix: State the legal basis per processing purpose, using Article 6(1)(b) for what is necessary for the service and consent for what is optional.

M5: At least nine independent third-party processors compiled into the binary, none named in the privacy documents

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), open

Manifest components, compiled kotlin_module files and endpoint strings show the processors below. None of Braze, Klaviyo, Split.io, Sentry, Ayla Networks, RevenueCat, Zendesk or ThroughTek appears by name in the live owletcare.com privacy policy or in the bundled consumer_privacy_notice_en_us.pdf, which was checked by a case-insensitive string search of both. Both documents describe recipients as service providers, distributors and retail partners, trusted advertising or marketing partners and trusted research partners. Ayla Networks includes endpoint strings for several regions including .ayla.com.cn, mqtt-cndev and mqtt-cnfield. That is typical of a multi-region SDK and the package does not show which region a production install uses. No China transfer is asserted. This is a transparency finding with no technical vector.

Vendor	Function	Evidence
Google Firebase	Analytics, crash, backend	ComponentDiscoveryService, owletcare-prod.firebaseio.com
Braze	Push, in-app messaging, marketing automation	com.braze.ui.*, BrazePushReceiver, sdk.iad-01.braze.com, sondheim.braze.com
Klaviyo	Email and SMS marketing	a.klaviyo.com, static.klaviyo.com
RevenueCat	Subscriptions and in-app purchases	PaywallActivity, CustomerCenterActivity, api.revenuecat.com, api-paywalls.revenuecat.com
Split.io	Feature flags and experiments	io.split.android.client. UserConsentManager, sdk.split.io, streaming.split.io, events.split.io
Sentry	Crash and session diagnostics, Session Replay module	sentry-android-replay, io.sentry. ndk.SentryNdkPreloadProvider
Ayla Networks	IoT device cloud for the sock and base station	com.aylanetworks.aylasdk.*, mqtt-usfield.aylanetworks.com and more than 60 endpoints
Google Ads, Privacy Sandbox	Conversion attribution	see H2
Zendesk	Customer support	owletsupport.zendesk.com
ThroughTek (TUTK)	Peer to peer video path of the Owlet Cam	tutk.kotlin_module in META-INF

Impact: A parent reading the notices cannot learn that marketing, email and experimentation platforms sit inside an app that carries the vitals of their baby.

Fix: Publish a named list of processors, with their roles and locations, and mark the ones that are not needed for monitoring.

O1: The app's own strings say both that Owlet products are not medical devices and quote the FDA indications for use

---

INFO, no CVSS v4.0 score assigned, observation from the notice of 22 August 2026, not rated

res/values/strings.xml carries a graph tooltip disclaimer that Owlet products are not medical devices and are not intended to diagnose, cure, treat, mitigate, alleviate or prevent any disease or health condition. A separate string quotes the Indications for Use of the Dream Sock, which is FDA-cleared for pulse rate and oxygen saturation in healthy infants. The Play listing carries the Medical device tag. Both strings ship in the same APK. The report records the contradiction and does not rate it, and it does not assess the regulatory status of the product in any jurisdiction.

```
Owlet products are not medical devices ... They do not and are not intended to
    diagnose, cure, treat,
mitigate, alleviate or prevent any disease or health condition.

Dream Sock is indicated for use in healthy infants/children ages 0 to 18 months and
    weighing between
2.5-13.6kg ... not indicated for use with infants previously diagnosed with chronic
    cardiovascular
and/or respiratory conditions.
```

Impact: A parent who opens the graph tooltip reads that the product is not a medical device, while the product page and the indications text describe a cleared device. The reader needs one consistent account of what the numbers are for.

Fix: Align the in-app wording with the regulatory status of the product in each market.

Impact Analysis

The people affected are parents who use a wearable and an app to watch their infant's pulse and blood oxygen, and the infants who cannot consent. The product is paid hardware, so the argument that data funds a free service does not apply. The app has no ad display and the attribution stack serves the operator's own marketing measurement.

H1 affects every parent who relies on the store label. H2 and M5 concern the platforms that sit inside an app with special category data and are not named in the notices. M1, M2 and M3 concern initialisation order, the scope of cleartext traffic and the availability of the Firebase project. M4 concerns the legal basis that a parent is told applies.

The demonstrated harm is a harm of transparency and default configuration. No access to vitals, accounts or databases was shown, and none was tried.

The Complete Chain

Step 1, store: a parent compares monitors. The listing says Medical device and the Data Safety card lists six categories without health data (H1).

Step 2, install and first launch: Firebase registers through a directBootAware service and the app declares the advertising permissions (M1, H2). The package does not show whether these wait for the consent screen.

Step 3, consent: the app asks for a specific consent that names pulse rate and oxygen saturation, with a separate consent for AI sleep insights. The notice says that withdrawing consent ends the use of the app (M4).

Step 4, operation: the sock and base station report through Ayla Networks, push, email and experimentation run through Braze, Klaviyo and Split.io, and diagnostics through Sentry. Cleartext is permitted app-wide (M2, M5).

Step 5, the parent tries to learn who receives the data: the notices describe recipients as service providers and marketing partners without names (M5). The app strings describe the product both as not a medical device and as a cleared device (O1).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1, M4 and M5.

Article 5(1)(b) and (c), purpose limitation and minimisation: engaged by H2 and M5.

Article 5(2), accountability: engaged by M1.

Article 6(1), lawful basis: engaged by H2 and M4. Article 6(1)(a) against Article 6(1)(b) is the question in M4.

Article 7(1) and Article 7(4), conditions for consent: engaged by M1 and M4.

Article 9, special categories: engaged by H2 as a question of purpose separation next to the vitals stream. The operator names Article 9 data in its own notice and relies on explicit consent.

Article 13(1)(c) and (e), Article 14(1)(e): engaged by H1 and M5.

Article 25: engaged by M3.

Article 27: met. The Dublin representative is correctly appointed and is credited below.

Article 28: engaged by M5. The processors are not named in the notices.

Article 32(1)(a) and (b): engaged by M2 and M3.

Article 37(1)(c): met. The notice states the DPO appointment on that ground.

ePrivacy Directive Art. 5(3): engaged by H2 and M1, because reading the advertising identifier and starting SDK components on terminal equipment needs consent unless strictly necessary.

Consumer Protection & Platform Disclosures

The Google Play listing rates the app PEGI 3 and carries the tags Health & Fitness and Medical device. The Data Safety card on 22 August 2026 listed six collected categories, stated that no data is shared with third parties, that data is encrypted in transit and that deletion can be requested. It omitted health data (H1). The same card states that data is encrypted in transit while the manifest permits cleartext traffic app-wide (M2), and states that no data is shared with third parties while processors such as Braze, Klaviyo and Sentry are compiled in (M5). Whether those SDKs transmit data to their vendors is not shown by the package, so the contradiction is recorded as a question. The current label was not re-read for this report.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 27 for a controller outside the Union, together with Article 5(3) of the ePrivacy Directive. The operator is established in the United States and offers its products to EU households, which brings Article 3(2) GDPR into play.

The Dream Sock is described as FDA-cleared. This report does not assess the regulatory status of the products as medical devices in the EU or any other market. No obligation under NIS2 or the AI Act is asserted for this operator, because its sector and size classification has not been established.

The competent authority for an Austrian initiated matter is the Österreichische Datenschutzbehörde (dsb@dsb.gv.at). The European Data Protection Supervisor (edps@edps.europa.eu) is in copy of the notice. The disclosure follows ISO/IEC 29147 and Art. 17 StGG.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.owletcare.sleep
Version            3.40.0 (versionCode 64832), analysed 2026-08-22
base.apk SHA-256   37544949e42f0d54c933d373585861e3ddb17d493738067ee4dab4f03c93286b
XAPK SHA-256       be56139af32299525c2c2882911abc4106d7f68f033d058b43de696e48719031
Signing cert SHA-256 7c7115349682fd3b818df49ef7816d110966e0e7e9269497ff533c57a8b90bc4
Signing cert SHA-1   2a3bc26db0b8b0792dbe28e6ffdc2598f9b12b74
Signer DN          CN=Dallas Haueter, OU=Android Mobile Development, O=Owlet Baby Care
    , L=Provo, ST=Utah, C=US
Signature scheme   v3 only, Google source stamp verified

Firebase project   owletcare-prod
google_api_key     AIzaSyDlfp3urNTbyhCtHOCxZBOjHQf4WuN_Aws
google_app_id      1:561089101102:android:7703b1c03673b7a486cebf
gcm_defaultSenderId 561089101102
Database URL       https://owletcare-prod.firebaseio.com
Other projects     owletcare-prod-eu.firebaseio.com, owletcare-dev.firebaseio.com,
    owletcare-staging.firebaseio.com
Ad endpoints       https://pagead2.googlesyndication.com, https://www.googleadservices
    .com
```

```
H1  Google Play listing and Data Safety page (22 August 2026), assets/
    data_processing_terms_en_us.pdf, assets/consumer_privacy_notice_en_us.pdf
H2  AndroidManifest.xml permissions, classes5.dex and classes7.dex (
    AdvertisingIdClient), endpoint strings
M1  AndroidManifest.xml ComponentDiscoveryService, res/values/strings.xml (consent
    strings)
M2  AndroidManifest.xml usesCleartextTraffic, res/xml/network_security_config.xml
M3  res/values/strings.xml, dex strings for the three further projects
M4  assets/data_processing_terms_en_us.pdf
M5  META-INF/*.kotlin_module, AndroidManifest.xml, endpoint strings, owletcare.com
    privacy policy
O1  res/values/strings.xml (tooltip disclaimer and Indications for Use strings)
```

Reproduction: obtain com.owletcare.sleep 3.40.0 from Google Play, check the SHA-256 above, decode the manifest and resources with apktool, extract the two PDFs from the assets folder and read the named files. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 Notice REF OWLETDREAM-2026-R1 to privacy@owletcare.com, CC DSB and EDPS. Findings H1 and H2 in the text, five Medium findings summarised, three questions asked, reply requested within 30 days.

2026-10-17 Follow-up from security@rfi-irfos.com to privacy@owletcare.com, 34 days before the embargo date, with the open findings and the same three questions.

2026-11-15 Final notice from s.kepp@rfi-irfos.com to privacy@owletcare.com, 85 days after the notice, naming 20 November 2026 as the publication date. No reply followed.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026. As of 21 November 2026 no message from Owlet is on record.

What Owlet Got Right

Owlet appointed a data protection officer and states the reason, the processing of special category health data under Article 37(1)(c). It keeps a correctly separated EU representative in Dublin and UK representative in Belfast. The bundled documents name the GDPR, cite Article 46(2)(c) for transfer safeguards and state the right to lodge a complaint. The consent screen names pulse rate and oxygen saturation, and a second consent for AI sleep insights can be revoked without losing the account. Research use of vitals data is scoped to de-identified data unless the user gives explicit consent. Alarm threshold settings carry a disclaimer that limits should only be set as prescribed by a qualified healthcare professional. The indications for use match the clearance scope of 0 to 18 months and 2.5 to 13.6 kg. No Chinese or sanctioned-jurisdiction SDK, no AdMob and no Meta SDK is in the binary. fullBackupContent is false, a distinct owletcare-prod-eu project exists, targetSdkVersion is 35 and minSdkVersion is 32.

Residual Risk & Recommendations

Open at the date of publication: all items, with no written position from the operator. Only the operator can close the Data Safety category in H1, the purpose and consent path of the advertising identifier in H2, the initialisation order in M1, the Security Rules and key restrictions in M3, the legal basis in M4 and the named processor list in M5.

Recommendations: add the health category to the Data Safety declaration, state the purpose and consent path of the advertising identifier and allow it to be switched off, confirm that SDK components wait for the consent screen, narrow cleartext to the local address that needs it, restrict the Firebase key and enforce App Check, state the legal basis per purpose, publish a named processor list, and align the in-app wording on medical device status.

This report is published after the embargo date. Statements are limited to the package and to the public documents named above.

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 public documents read from the public sites. No Owlet servers, devices or accounts were

probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF OWLETDREAM-2026-R1.