Security & Privacy Disclosure, Final Report

Perifit Care for Android (starshipproduct.perifitmainapp)

A pelvic floor trainer whose store label says name and email only, while the package requests menstruation and heart rate history and starts advertising signals at launch.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	X6 Innovations SAS, Paris, France (operator named in the privacy policy)
Versions Audited	4.161.0 / 10001915 (2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	8: 4 High, 3 Medium, 1 Low
Status	Only automated replies from an AI agent, no human reply as of 14 November 2026.
SHA-256 (base APK)	`f06739f8ac601fcde32542587ab0b4d67857970d1747f129729ae23bad9e744f`

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 5

6 Findings 6

6.1 C1: The Google Play Data Safety label says name and email only and no sharing, while the package and the operator's own privacy policy show health permissions and at least ten recipients . . . 6

6.2 C2: Twelve Health Connect read permissions are declared, including menstruation, heart rate, sleep and the full data history, and neither the privacy policy nor the store label names them . . . 7

6.3 C3: Firebase, Meta and advertising signals start with the process and the manifest sets every Consent Mode default to granted, in a paid medical device app 8

6.4 H1: The JavaScript bundle holds a function and a field for a clinical urge incontinence score . . . 9

6.5 H2: A full Meta SDK bridge and the Sentry Session Replay module ship in the package, and neither appears as a recipient in the operator's policy . . . 10

6.6 H3: Firebase API key and Realtime Database URL of project perifit-63b7d are stored in plain text . . . 11

6.7 M1: No network security configuration and no certificate pinning for an app that sends health data . . . 11

6.8 M2: The store rating is PEGI 3 while the operator's policy excludes users under 16, and the package shows no age gate . . . 12

7 Impact Analysis 12

8 The Complete Chain 13

9 Data Protection: Article by Article 13

10 Consumer Protection & Platform Disclosures 14

11 Regulatory & Legal Landscape 14

12 Indicators of Compromise & Reproducible Evidence 15

13 Disclosure Timeline & Outcome 16

14 What Perifit Got Right 16

15 Residual Risk & Recommendations 17

Executive Summary

Perifit Care is the companion app for the Perifit connected pelvic floor trainer. X6 Innovations SAS of Paris operates it. Google Play lists it as a medical device with more than 500,000 installs and a PEGI 3 rating. On 22 August 2026 RFI-IRFOS disclosed eight findings from a root level code analysis of version 4.161.0 under REF PERIFITCARE-2026-R1.

The design has points in its favour. Cleartext traffic is denied, backup is off, Crashlytics collection is off by default, the microphone permission traces to the support chat only, and the privacy policy names a working deletion path and EU hosting for AWS and Bugfender. The findings sit beside that design.

Three findings carry the weight. The store label says name and email only and no sharing, while the package and the operator's own policy show more (C1). The package declares twelve Health Connect read permissions including menstruation, heart rate, sleep and the full history, and neither the policy nor the label names them (C2). Every Consent Mode default is set to granted and Firebase and the Meta SDK start with the process, in a product that users pay for (C3). The people behind the findings are users of a medical device who share intimate data with an app that tells them less than the package shows.

The notice of 22 August 2026 went to support@perifit.co with the Austrian DSB and the EDPS in copy. Two automated replies from an AI agent called Peribot arrived, the first within two minutes, and gave general statements. Follow-ups of 3 September and 17 October 2026 asked for a named person and for answers. No human reply is on record. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of release 4.161.0 (versionCode 10001915), arm64-v8a: manifest, resources, the dex string pool and the string table of the Hermes JavaScript bundle. The APK came from APKPure because the audit device was not connected, and the signer value below is taken from that mirror and was not re-derived. The live Google Play listing, the Data Safety section and the operator privacy policy were read on 2026-08-22. No Perifit server or database was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. The 965 MB install time asset pack was not analysed. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	HIGH	The Google Play Data Safety label says name and email only and no sharing, while the package and the operator’s own privacy policy show health permissions and at least ten recipients
C2	HIGH	Twelve Health Connect read permissions are declared, including menstruation, heart rate, sleep and the full data history, and neither the privacy policy nor the store label names them
C3	HIGH	Firebase, Meta and advertising signals start with the process and the manifest sets every Consent Mode default to granted, in a paid medical device app
H1	MEDIUM	The JavaScript bundle holds a function and a field for a clinical urge incontinence score
H2	HIGH	A full Meta SDK bridge and the Sentry Session Replay module ship in the package, and neither appears as a recipient in the operator’s policy
H3	MEDIUM	Firebase API key and Realtime Database URL of project perifit-63b7d are stored in plain text
M1	MEDIUM	No network security configuration and no certificate pinning for an app that sends health data
M2	LOW	The store rating is PEGI 3 while the operator’s policy excludes users under 16, and the package shows no age gate

Finding Status at a Glance

ID	Disclosed	This report	Status on 14 November 2026
C1	CRITICAL	HIGH	Open. Automated reply only.
C2	CRITICAL	HIGH	Open. Automated reply gives a general statement.
C3	CRITICAL	HIGH	Open. Automated reply only.
H1	HIGH	MEDIUM	Open. Not answered.
H2	HIGH	HIGH	Open. Not answered.
H3	HIGH	MEDIUM	Open. Not answered.
M1	MEDIUM	MEDIUM	Open. Not answered.
M2	MEDIUM	LOW	Open. Not answered.

Subject & Operator Analysis

The privacy policy at eu.perifit.co names X6 Innovations SAS, 128 rue La Boétie, 75008 Paris, France, as controller. The company has a main establishment in the Union, so the one-stop-shop mechanism applies and the Commission Nationale de l'Informatique et des Libertés is the lead authority under Article 56. No Article 27 representative is needed for the controller. Chapter V questions remain for processors in the USA that the policy itself names.

The contact for privacy rights and support is support@perifit.co. The address product@perifit.co was found by public web search only and is UNVERIFIED. No data protection officer is named in the package or in the public policy, which is UNVERIFIED. The base APK signer SHA-1 is 8fc5dab03b5e53d9cf08c3efb5a48e264a2c7e71 per APKPure and was not re-derived.

Architecture & Data Flow

The app is a React Native application. The logic sits in a 14 MB Hermes bytecode bundle, and four dex files of about 29 MB hold the native layer. The package bundles Firebase with the React Native Firebase wrapper, a Health Connect wrapper from dev.matinzd, the Meta SDK bridge, Mixpanel, Segment, Sentry, Intercom, Bugfender, Ably, RevenueCat and Stripe web billing. A dedicated DFU service updates the firmware of the connected device.

Firebase, the advertising signals and the Meta SDK start from content providers and manifest flags before the JavaScript bundle loads (C3). Health Connect permissions are requested in the app (C2). The Realtime Database of project perifit-63b7d backs the app (H3). Where the clinical score is stored is not shown (H1).

Engagement Summary

The notice REF PERIFITCARE-2026-R1 was sent on 22 August 2026 at 22:41 UTC to support@perifit.co, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated C1, C2 and C3 as critical, H1, H2 and H3 as high and M1 and M2 as medium. At 22:43 UTC an AI agent named Peribot answered that Health Connect is read only with user authorization, that menstrual or cycle data is not synced from Health Connect, that training and usage data is anonymised or encrypted on the device and on EU hosted AWS, that sharing with third parties happens with consent or for lawful reasons, and that the matters require a detailed internal review.

RFI-IRFOS asked for a named responsible person at 23:54 UTC. A second Peribot reply at 23:55 UTC offered that a human agent could assist. A follow-up of 3 September 2026 gave a chronology, three questions and a deadline of 5 September 2026. A further follow-up of 17 October 2026 repeated the open points, 34 days before the embargo date. No human reply is on record.

Findings

C1: The Google Play Data Safety label says name and email only and no sharing, while the package and the operator's own privacy policy show health permissions and at least ten recipients

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), disclosed as CRITICAL on 22 August 2026, rated HIGH in this report, rated HIGH by blast-radius escalation

The Data Safety section of the app, read live on 2026-08-22, lists Personal info, Name and Email address as the only collected data and states: No data shared with third parties. The package declares twelve Health Connect read permissions (C2) and holds SDK classes and endpoints for Firebase Analytics, Crashlytics, Cloud Messaging and Remote Config, Meta, Mixpanel, Segment, Sentry with Session Replay, Intercom, Bugfender, Ably and RevenueCat with an embedded Stripe web billing flow. That is at least ten independent recipients. The operator's own privacy policy, read live on the same day, names recipients and collects gender, country, name, age, height, weight and data concerning health such as menopausal status. Google defines sharing for the Data Safety section so that transfers to service providers acting for the developer are not counted, which may cover part of the list. The Meta SDK and the advertising signals in C3 do not fit that exception. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the app is rated as a medical device with more than 500,000 installs, handles intimate health data, and the label contradicts the operator's own policy. The CVSS vector scores zero because this is a transparency finding with no technical attack path.

```
The live Data Safety section (fetched 2026-08-22):
  No data shared with third parties
  The developer says this app doesn't share user data with other companies or
    organizations.
  Data collected: Personal info - Name and Email address


Privacy policy (https://eu.perifit.co/pages/app-privacy-policy, fetched 2026-08-22):
  gender, country, name; age, height and weight, and data pertaining to Your health
    such as your menopausal status.
```

```
com.facebook.reactnative.androidsdk.*   api.segment.io   io/sentry/sentry-android-
    replay
api.revenuecat.com   api-paywalls.revenuecat.com   (also Firebase, Mixpanel, Intercom,
     Bugfender, Ably)
```

Impact: A person who buys a pelvic floor trainer reads on the store page that only name and email are collected and that nothing is shared. The package and the operator's own policy say otherwise. The person decided on the first statement.

Fix: Correct the Data Safety section so that it lists the health and device data and every recipient, or publish in writing which recipients are service providers and why.

C2: Twelve Health Connect read permissions are declared, including menstruation, heart rate, sleep and the full data history, and neither the privacy policy nor the store label names them

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), disclosed as CRITICAL on 22 August 2026, rated HIGH in this report, rated HIGH by blast-radius escalation

The merged manifest declares twelve android.permission.health.READ permissions. The package ships matching React Native bridge classes, including menstruation flow and period, sleep session and heart rate. READ_HEALTH_DATA_HISTORY reaches beyond the default 30 day window of Health Connect. READ_OVULATION_TEST exists only as library surface and is not declared. The privacy policy names only menopausal status as health data, and the store label names none. Rating basis: a Health Connect read needs the user's grant at runtime, and the package does not show what happens to the values after reading. The automated reply of the operator states that menstrual or cycle data is not synced from Health Connect, which the package neither confirms nor contradicts. Declaring the permissions and shipping the bridge for menstruation records is the evidence. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data types are special category data, READ_HEALTH_DATA_HISTORY requests the full history, and nothing public names them. The CVSS vector scores zero because the package shows a permission request and no transfer.

```
<uses-permission android:name="android.permission.health.READ_MENSTRUATION"/>
<uses-permission android:name="android.permission.health.READ_HEART_RATE"/>
<uses-permission android:name="android.permission.health.READ_RESTING_HEART_RATE"/>
<uses-permission android:name="android.permission.health.READ_SLEEP"/>
<uses-permission android:name="android.permission.health.READ_STEPS"/>
<uses-permission android:name="android.permission.health.READ_DISTANCE"/>
<uses-permission android:name="android.permission.health.READ_EXERCISE"/>
<uses-permission android:name="android.permission.health.READ_HYDRATION"/>
<uses-permission android:name="android.permission.health.READ_NUTRITION"/>
<uses-permission android:name="android.permission.health.READ_WEIGHT"/>
<uses-permission android:name="android.permission.health.READ_HEIGHT"/>
<uses-permission android:name="android.permission.health.READ_HEALTH_DATA_HISTORY"/>
```

```
Ldev/matinzd/healthconnect/records/ReactMenstruationFlowRecord;
Ldev/matinzd/healthconnect/records/ReactMenstruationPeriodRecord;
Ldev/matinzd/healthconnect/records/ReactSleepSessionRecord;
Ldev/matinzd/healthconnect/records/ReactHeartRateRecord;
Ldev/matinzd/healthconnect/records/ReactRestingHeartRateRecord;
Ldev/matinzd/healthconnect/records/ReactWeightRecord; (also Height, Hydration,
    Nutrition, Steps, Distance, ExerciseSession)
```

Impact: Menstrual cycle, heart rate and sleep history can show pregnancy, fertility and health conditions. A person who connects Health Connect to a pelvic floor trainer is not told in the policy or on the store page that this data is requested.

Fix: Name every Health Connect data type in the policy and the label, request only the types needed, and complete an impact assessment.

C3: Firebase, Meta and advertising signals start with the process and the manifest sets every Consent Mode default to granted, in a paid medical device app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 22 August 2026, rated HIGH in this report, rated HIGH by blast-radius escalation

The manifest sets firebase_analytics_collection_enabled, the advertising ID flag, the SSAID flag and all four Consent Mode defaults (analytics storage, ad storage, ad user data, ad personalization signals) to true, together with app_data_collection_default_enabled. The ad services configuration opens attribution, custom audiences and topics to every bundled SDK. FirebaseInitProvider at initOrder 100, two React Native Firebase providers and the Facebook init provider run at process start, before the JavaScript bundle that would hold any consent screen has loaded. The package also holds Play Billing, RevenueCat and a Stripe web checkout, so this is a paid product. Whether the SDKs transmit before consent was not measured, no traffic was captured. The declared defaults say that the operator has already granted every signal. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app is rated as a medical device, the user pays for it, the data is intimate, and the defaults are explicit grants and not a missing control. The CVSS vector scores the technical exposure of low sensitivity telemetry and no traffic was captured.

```
<meta-data android:name="firebase_analytics_collection_enabled" android:value="true"/>
<meta-data android:name="google_analytics_adid_collection_enabled" android:value="true
    "/>
<meta-data android:name="google_analytics_ssaid_collection_enabled" android:value="
    true"/>
<meta-data android:name="google_analytics_default_allow_analytics_storage" android:
    value="true"/>
<meta-data android:name="google_analytics_default_allow_ad_storage" android:value="
    true"/>
<meta-data android:name="google_analytics_default_allow_ad_user_data" android:value="
    true"/>
<meta-data android:name="google_analytics_default_allow_ad_personalization_signals"
    android:value="true"/>
<meta-data android:name="app_data_collection_default_enabled" android:value="true"/>
<property android:name="android.adservices.AD_SERVICES_CONFIG" android:resource="@xml/
    ad_services_config"/>

<provider android:name="com.google.firebase.provider.FirebaseInitProvider" android:
    directBootAware="true" android:initOrder="100"/>
<provider android:name="io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider"
    android:initOrder="99"/>
<provider android:name="io.invertase.firebase.crashlytics.
    ReactNativeFirebaseCrashlyticsInitProvider" android:initOrder="98"/>
<provider android:name="com.facebook.internal.FacebookInitProvider"/>
```

```
<!-- res/xml/ad_services_config.xml -->
<ad-services-config>
    <attribution allowAllToAccess="true" />
    <custom-audiences allowAllToAccess="true" />
    <topics allowAllToAccess="true" />
</ad-services-config>
```

Impact: A person who pays for a medical device and its app is, from the first launch, also measured by advertising and analytics SDKs, before any consent screen can appear.

Fix: Set the Consent Mode defaults to denied, start Firebase and the Meta SDK only after a recorded consent, and close the Privacy Sandbox configuration to a named list.

H1: The JavaScript bundle holds a function and a field for a clinical urge incontinence score

---

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), disclosed as HIGH on 22 August 2026, rated MEDIUM in this report, rated MEDIUM by blast-radius escalation

The Hermes string table of assets/index.android.bundle contains the function name computeMedicalUrgeScore and the field name medical_life_score_urge_incontinence. Urge incontinence is a named medical category. The names show that the app derives a score locally, and a derived health score is itself special category data. Neither the privacy policy nor the store label mentions a computed score. Whether the score leaves the device, is stored in the Firebase Realtime Database or changes recommendations is UNVERIFIED, since only the string table was read and no code path was traced. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the field name denotes a medical condition and the score is a derived health value. The CVSS vector scores zero because only the existence of the names is shown.

```
computeMedicalUrgeScore
medical_life_score_urge_incontinence
```

Impact: If the score is stored or transmitted, the operator holds an assessment of a medical condition that the user may not know exists.

Fix: State in the privacy policy whether the score is computed, where it is stored and what it is used for.

H2: A full Meta SDK bridge and the Sentry Session Replay module ship in the package, and neither appears as a recipient in the operator's policy

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), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The package holds React Native bridges for Facebook App Events, Graph Request, Login Manager, Profile, Share Dialog and Game Request Dialog, a FacebookInitProvider and the fbconnect scheme. App Events is advertising attribution analytics and not only a login button. The package also holds the verification file of the Sentry Session Replay sub SDK, which records screens and is distinct from crash reporting. The privacy policy names Mixpanel, AWS, Typeform, Intercom, Tribe, Bugfender, Sentry, Jira, Segment and Zapier. Meta is not among them, and Session Replay is not separated from crash reporting. Whether Session Replay is enabled at runtime was not tested and is UNVERIFIED. The Meta SDK starts with the process (C3). RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the recipient is an advertising company, the app is a medical device and the SDK starts before consent. The CVSS vector scores only the technical exposure of low sensitivity telemetry.

```
Lcom/facebook/reactnative/androidsdk/FBAppEventsLoggerModule;
Lcom/facebook/reactnative/androidsdk/FBGraphRequestModule;
Lcom/facebook/reactnative/androidsdk/FBLoginManagerModule;
Lcom/facebook/reactnative/androidsdk/FBProfileModule;
Lcom/facebook/reactnative/androidsdk/FBShareDialogModule;
Lcom/facebook/reactnative/androidsdk/FBGameRequestDialogModule;

<provider android:name="com.facebook.internal.FacebookInitProvider" android:exported="
    false"/>
<activity ... android:host="cct.starshipproduct.perifitmainapp" android:scheme="
    fbconnect"/>

META-INF/io/sentry/sentry-android-replay/verification.properties
```

Impact: A person who enters weight, birth year and menopausal status, or views contraction results, may have those screens recorded or measured by companies the policy does not name.

Fix: List Meta and the Session Replay function as recipients, confirm the processor contracts, and mask every screen that shows health input if Session Replay is enabled.

H3: Firebase API key and Realtime Database URL of project perifit-63b7d are stored in plain text

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 22 August 2026, rated MEDIUM in this report

The Firebase values sit in res/values/strings.xml. The project uses the Realtime Database product, so a queryable database exists behind the project id. A Firebase key is not secret by Google design, so this is an availability and resilience finding and not a confidentiality finding. The key and the project id allow quota probing, and they make the security rules of the Realtime Database and of the storage bucket the line that protects the health related data. No call was made and the rules were not tested.

```
<string name="google_api_key">AIzaSyDOvXlBghXCi14XrwsZz4YAdQRaEjGGJHg</string>
<string name="google_app_id">1:35754232379:android:2e7d5d96f4e497db</string>
<string name="firebase_database_url">https://perifit-63b7d.firebaseio.com</string>
<string name="google_storage_bucket">perifit-63b7d.appspot.com</string>
<string name="project_id">perifit-63b7d</string>
<string name="gcm_defaultSenderId">35754232379</string>
<string name="default_web_client_id">35754232379-le2qdrvi3aa5n97gm6klieqfqo2aei35.apps
    .googleusercontent.com</string>
```

Impact: The key gives nobody access to user data by itself. The protection of the health related records rests on the database and storage rules, which only the operator can show.

Fix: Confirm that the Realtime Database and storage rules deny unauthenticated access, and restrict the key by package and certificate.

M1: No network security configuration and no certificate pinning for an app that sends health data

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

The application element sets usesCleartextTraffic to false and declares no networkSecurityConfig. The resource tree has no network_security_config.xml. Cleartext traffic is denied, which is a point in the app's favour. No certificate pinning exists for api.perifit.co, app.perifit.co, auth.perifit.co or the SDK endpoints. An attacker who can install a trusted CA on the device could read the channel.

```
<application android:usesCleartextTraffic="false" ... />   (no android:
    networkSecurityConfig)

res/xml/ contains no network_security_config.xml
```

Impact: On a managed device or a hostile network with an installed CA, the health data in transit could be read.

Fix: Add a network security configuration with pinning for the operator's own API hosts.

M2: The store rating is PEGI 3 while the operator’s policy excludes users under 16, and the package shows no age gate

LOW, 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), disclosed as MEDIUM on 22 August 2026, rated LOW in this report

The Play listing shows PEGI 3. The operator’s privacy policy states in section 6 that the product is not marketed to and should not be used by anybody under the age of 16. The Hermes bundle holds date of birth fields (given_birthdate, year_of_birthdate, account_info_year_of_birthdate), so a birth year is collected. No COPPA string, no eligibility block and no age gate logic was found in the dex or JavaScript string tables. This shows that the rating and the policy disagree, and that the package contains no mechanism that resolves the disagreement. It does not show that a minor used the app.

```
PEGI 3 (Google Play listing, 2026-08-22)
Privacy policy section 6: "The Product is not marketed to, and should not be used by,
    anybody under the age of 16."

assets/index.android.bundle: given_birthdate, year_of_birthdate,
    account_info_year_of_birthdate
Search for COPPA and for an age block string: no hits
```

Impact: The finding concerns a mismatch between two statements of the operator. It does not describe a harm that was shown.

Fix: Align the rating with the policy and enforce the stated minimum age at registration.

Impact Analysis

The people affected are users of a connected pelvic floor trainer with more than 500,000 installs. The data includes training sessions, body measurements, menopausal status, and where the user grants Health Connect access, menstrual cycle, heart rate and sleep. A derived incontinence score may exist.

C1 affects every user who read the Data Safety section. C2 affects users who connect Health Connect. C3 and H2 affect every launch. H1 concerns a derived medical value. H3 and M1 concern the technical protection of the data. M2 concerns the position of minors.

The demonstrated harm is a harm of transparency and design. No access to user data was shown and none was attempted.

The Complete Chain

Step 1, store: the label says name and email only and no sharing (C1).

Step 2, install and first launch: Firebase, Meta and the advertising signals start with the process, with every default set to granted (C3, H2).

Step 3, onboarding: birth year, gender, weight and menopausal status are collected. No age gate is visible (M2).

Step 4, use: sessions feed a locally computed urge incontinence score (H1). Where the user grants Health Connect, menstruation, heart rate, sleep and history are readable (C2).

Step 5, transport and storage: no pinning protects the channel (M1), and the Realtime Database rules protect the stored data (H3).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2, C3 and M2.

Article 5(1)(c), data minimisation: engaged by H1 and H2.

Article 5(2), accountability: engaged by C3.

Article 6(1) and Article 7(1), lawful basis and conditions for consent: engaged by C3.

Article 8, child's consent: engaged by M2.

Article 9(1) and 9(2), special categories: engaged by C2 and H1.

Article 12, Article 13 and Article 14, information to the data subject: engaged by C1, C2, H1 and H2.

Article 13(1)(e) and Article 14(1)(e), recipients: engaged by H2.

Article 25, data protection by design and by default: engaged by C1, H2, H3 and M1.

Article 28, processors: engaged by H2.

Article 32(1)(a) and (b), security of processing: engaged by H3 and M1.

Article 35(3)(b), impact assessment for large scale processing of special categories: engaged by C2.

Article 5(3) of the ePrivacy Directive, storage of and access to information on the terminal: engaged by C3.

Consumer Protection & Platform Disclosures

The Google Play Data Safety section, read on 2026-08-22, lists Name and Email address as collected data, states that no data is shared with third parties, that data is encrypted in transit and that deletion can be requested. The listing shows the category Medical device, a rating of 4.9 from about 6,150 reviews, more than 500,000 installs and PEGI 3. The sharing statement and the collected data types are the statements that C1 sets against the package.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 9 for data concerning health and Article 5(3) of the ePrivacy Directive for terminal access. The operator is established in France, so the Commission Nationale de l’Informatique et des Libertés is the lead authority under Article 56. The Österreichische Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) are in copy of the notice under the standing practice of the programme. 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 from the published package. All values are given in full.

```
Package            starshipproduct.perifitmainapp
Version            4.161.0 (versionCode 10001915), analysed 2026-08-22
base.apk SHA-256   f06739f8ac601fcde32542587ab0b4d67857970d1747f129729ae23bad9e744f
Signer SHA-1       8fc5dab03b5e53d9cf08c3efb5a48e264a2c7e71 (per APKPure, not re-
    derived)
minSdk / targetSdk 26 / 36

Firebase project   perifit-63b7d
google_api_key     AIzaSyDOvXlBghXCi14XrwsZz4YAdQRaEjGGJHg
google_app_id      1:35754232379:android:2e7d5d96f4e497db
Database URL       https://perifit-63b7d.firebaseio.com
Storage bucket     perifit-63b7d.appspot.com
sender id          35754232379
web client id      35754232379-le2qdrvi3aa5n97gm6klieqfqo2aei35.apps.googleusercontent
    .com
```

```
C1  Play Data Safety section, eu.perifit.co privacy policy, classes*.dex, index.
    android.bundle
C2  AndroidManifest.xml (health permissions), classes2.dex (dev/matinzd/healthconnect/
    records)
C3  AndroidManifest.xml (meta-data, providers), res/xml/ad_services_config.xml
H1  assets/index.android.bundle (computeMedicalUrgeScore,
    medical_life_score_urge_incontinence)
H2  classes2.dex (com/facebook/reactnative/androidsdk), META-INF/io/sentry/sentry-
    android-replay
H3  res/values/strings.xml
M1  AndroidManifest.xml, res/xml (no network_security_config.xml)
M2  Play listing, privacy policy section 6, assets/index.android.bundle
```

Reproduction: obtain starshipproduct.perifitmainapp 4.161.0 from Google Play or APKPure, check the SHA-256, decode the manifest and resources with apktool, extract the dex strings and the Hermes string table and read the named entries. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 22:41 UTC Notice REF PERIFITCARE-2026-R1 to support@perifit.co, CC DSB and EDPS. Findings C1, C2, C3, H1, H2, H3, M1, M2. The time equals 00:41 on 23 August in Austria, and all correspondence states the notice date as 22 August 2026.

2026-08-22 22:43 UTC First reply from Peribot, the AI agent of Perifit, with general statements.

2026-08-22 23:54 UTC Follow-up from RFI-IRFOS asking for a named responsible person.

2026-08-22 23:55 UTC Second Peribot reply stating that a human agent from the team can assist.

2026-09-03 15:37 UTC Follow-up with chronology, three questions and a deadline of 2026-09-05.

2026-10-17 19:34 UTC Follow-up from security@rfi-irfos.com, 34 days before the embargo date.

No human reply has been received.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026.

What Perifit Got Right

Cleartext traffic is denied by usesCleartextTraffic false, and the platform default for target SDK 36 supports it. allowBackup is false. Crashlytics collection is explicitly off by default, one of few signals that are not on. The RECORD_AUDIO permission traces only to the voice message feature of the Intercom support chat, and the microphone hardware is declared as not required. READ_OVULATION_TEST is library surface and is not requested. The privacy policy documents a deletion and rights path through support@perifit.co with a two year inactivity retention. AWS and Bugfender store data in the Union according to the policy. Firmware updates run in a dedicated DFU service typed as a connected device service. The operator answered within two minutes, although by an automated agent.

Residual Risk & Recommendations

Open at the date of publication: all eight items, with no written position from a person at the operator. Items that only the operator can close are the Data Safety correction in C1, the Health Connect purpose and legal basis in C2, the consent defaults in C3, the use of the urge score in H1, the Session Replay and Meta status in H2, the rules of the Realtime Database in H3 and the age handling in M2.

Recommendations: align the store label and the policy with the package, name every Health Connect data type and request only what is needed, set the Consent Mode defaults to denied and start the SDKs after consent, publish what the urge score is used for, list Meta and Session Replay as recipients and mask health screens, confirm the database and storage rules, add pinning and enforce the stated minimum age.

This report is published after the embargo date. Statements are limited to the package and to the public documents named above, and every item the package cannot show is marked UNVERIFIED.

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 Perifit servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF PERIFITCARE-2026-R1.