Security & Privacy Disclosure, Final Report

Pump with Elvie for Android (com.chiaro.elviepump)

A breast pump app that starts analytics before any consent screen can exist, and shares its login infrastructure with a pelvic floor trainer.

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

Target	Willow Blossom Holdco Limited, London, trading as Elvie (controller named in the privacy policy)
Versions Audited	1.37.11 / 2136 (2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged); final report published 2026-11-21
Findings	7: 1 High, 5 Medium, 1 Low
Status	NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026. Three messages sent (22 August, 17 October and 15 November 2026), no automatic acknowledgement received.
SHA-256 (base APK)	`a6ece41d4d424d555796a8aaf3a398a3eed67769df7c2cf7de649d35979be38f`

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: Firebase Analytics and the advertising ID pipeline start with the process, no consent management platform exists in the package, and the store label says no data is shared with third parties . . . 6

6.2 H1: The Firebase API key, the project configuration, a legacy Realtime Database URL and the storage bucket of project elvie-pump are stored in plain text . . . 7

6.3 H2: The FullStory session replay SDK is instrumented into the Compose interface and no in-app consent screen exists . . . 8

6.4 H3: Elvie Pump and Elvie Trainer share one signing certificate and one OAuth endpoint, which points to one identity plane over lactation and pelvic floor data 9

6.5 M1: No network security configuration and no certificate pinning for the endpoints that carry OAuth tokens and pumping session data . . . 10

6.6 M2: Five activities are exported on the custom elvieapp scheme and the package does not show whether they validate the caller . . . 11

6.7 M3: The privacy policy offers an Article 27 representative and the linked contact document returns HTTP 404 . . . 12

7 Impact Analysis 13

8 The Complete Chain 13

9 Data Protection: Article by Article 14

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 Elvie Got Right 16

15 Residual Risk & Recommendations 17

Executive Summary

Pump with Elvie is the companion app for the Elvie Pump and Elvie Stride wearable breast pumps. It processes lactation sessions with milk volume, timing and frequency, which works as a feeding schedule signal for the pumping parent. The privacy policy names Willow Blossom Holdco Limited, trading as Elvie, as controller. On 22 August 2026 RFI-IRFOS disclosed seven findings from a root level code analysis of version 1.37.11 under REF ELVIEPUMP-2026-R1.

The permission footprint is small and well scoped. No microphone, camera, contacts or biometric permission is requested, location permissions are capped to Android 11 and below, BLUETOOTH_SCAN carries neverForLocation, and no advertising or attribution SDK and no PRC SDK was found. The app has no billing SDK, allowBackup is false and the target SDK is 35. The policy names an Article 27 representative mechanism, which many peers lack.

One finding carries the weight. Firebase Analytics and the advertising ID pipeline start from a content provider with the highest initialisation priority, before any consent screen can exist, and no consent management platform exists in the package (C1). The other findings concern the Firebase configuration and legacy database URL (H1), FullStory session replay with no consent screen (H2), a shared signing certificate and OAuth endpoint with Elvie Trainer (H3), missing pinning (M1), five exported entry points (M2) and a dead link to the Article 27 representative (M3). The people behind the findings are parents who pump milk and train their pelvic floor with devices from one company.

The notice of 22 August 2026 went to privacy@elvie.com, questions@elvie.com and appdev@onewillow.com with the Austrian DSB and the EDPS in copy. The address questions@elvie.com rejected the message at once, so the notice reached two of the three addresses. A follow-up of 17 October 2026 went to the same three addresses and described all three as reached, which the bounce does not support. A third message of 15 November 2026 went to the two working addresses, corrected that statement, removed questions@elvie.com from the correspondence and repeated the three questions. No reply of any kind is on record as of 21 November 2026, including no automatic acknowledgement. The embargo date of 20 November 2026, named in both follow-ups, has passed, and this final report is published on 21 November 2026.

Scope: Root level code analysis of release 1.37.11 (versionCode 2136), a Kotlin and Jetpack Compose application: manifest, resources and the string pool of the five dex files, plus the signing certificate. No smali disassembly was done, so control flow questions are marked UNVERIFIED. The APK came from APKPure, and APKCombo agrees on the version code. The live Google Play listing, the Data Safety section and the operator privacy policy were read on 2026-08-22. Elvie Trainer was compared only for the signing certificate and endpoint strings. No Elvie server or database was called, no account was created, no traffic was intercepted and no runtime instrumentation was used.

ID	Severity	Title
C1	HIGH	Firebase Analytics and the advertising ID pipeline start with the process, no consent management platform exists in the package, and the store label says no data is shared with third parties
H1	MEDIUM	The Firebase API key, the project configuration, a legacy Realtime Database URL and the storage bucket of project elvie-pump are stored in plain text
H2	MEDIUM	The FullStory session replay SDK is instrumented into the Compose interface and no in-app consent screen exists
H3	MEDIUM	Elvie Pump and Elvie Trainer share one signing certificate and one OAuth endpoint, which points to one identity plane over lactation and pelvic floor data
M1	MEDIUM	No network security configuration and no certificate pinning for the endpoints that carry OAuth tokens and pumping session data
M2	LOW	Five activities are exported on the custom elvieapp scheme and the package does not show whether they validate the caller
M3	MEDIUM	The privacy policy offers an Article 27 representative and the linked contact document returns HTTP 404

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Open. No reply of any kind.
H1	HIGH	MEDIUM	Open. No reply of any kind.
H2	HIGH	MEDIUM	Open. No reply of any kind.
H3	HIGH	MEDIUM	Open. No reply of any kind.
M1	MEDIUM	MEDIUM	Open. Summarised in the notice, no reply.
M2	MEDIUM	LOW	Open. Summarised in the notice, no reply.
M3	MEDIUM	MEDIUM	Open. Described in the notice without a label, no reply.

Subject & Operator Analysis

The operator picture has four layers. Google Play shows the publisher name Willow Innovations, Inc. and names EXPLORAMED NC7, LLC, 1975 W El Camino Real Ste 306, Mountain View, CA 94040, USA, as developer. The privacy policy names Willow Blossom Holdco Limited, trading as Elvie, UK Companies House number 16306329, registered office 9th Floor, 107 Cheapside, London EC2V 6DN, as controller. The package is still signed with the release key of Chiaro Technology Limited, London. According to public reports cited in the notice, Willow Innovations sued Chiaro Technology for patent infringement, Chiaro entered administration in the UK, and Willow took over the Elvie business and its 178 staff out of the administration on 28 March 2025. The sequence of entities explains why the Article 27 document under M3 carries a Chiaro era name.

The controller is registered in the United Kingdom, which is a third country for the Union. No Union main establishment was identified, so the Österreichische Datenschutzbehörde is the competent authority for an Austrian initiated matter. The mailbox privacy@elvie.com comes from the live privacy policy. No named data protection officer was found, and whether one exists is UNVERIFIED.

Architecture & Data Flow

The app is a Kotlin and Jetpack Compose application with five dex files. It connects to the pump over Bluetooth Low Energy, signs in against auth.chiaro.co.uk with OAuth, and talks to api.chiaro.co.uk under the path segment pump. Firebase project elvie-pump receives analytics and crash data. FullStory is instrumented into the Compose tree. There is no advertising or attribution SDK and no billing SDK.

Firebase starts from a content provider before any screen exists (C1). The identity plane at auth.chiaro.co.uk is shared with Elvie Trainer, while telemetry projects are separate (H3).

Engagement Summary

The notice REF ELVIEPUMP-2026-R1 was sent on 22 August 2026 at 12:49 UTC to privacy@elvie.com, questions@elvie.com and appdev@onewillow.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated C1 as critical, H1, H2 and H3 as high, mentioned two medium findings (M1 and M2) and described the dead representative link (M3), asked three questions and requested a written reply within 30 days. At 12:49:29 UTC the mail system returned a failure notice because questions@elvie.com does not exist (5.1.3). The notice therefore reached privacy@elvie.com and appdev@onewillow.com.

A follow-up from security@rfi-irfos.com went to the same three addresses on 17 October 2026 at 18:52 UTC, 34 days before the embargo date, with the open findings and the three questions unchanged. No bounce for that message was found. It named all three addresses as reached, which the bounce of 22 August does not support.

A third message from s.kepp@rfi-irfos.com went on 15 November 2026 at 13:00 UTC to privacy@elvie.com and appdev@onewillow.com, 5 days before the embargo date and 85 days after the notice. It corrected the earlier statement, removed questions@elvie.com from the correspondence and repeated the three questions. No bounce for the two later messages was found. No message from Elvie or Willow is on record as of 21 November 2026, 91 days after the notice, and no automatic acknowledgement arrived.

Findings

C1: Firebase Analytics and the advertising ID pipeline start with the process, no consent management platform exists in the package, and the store label says no data is shared with third parties

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

FirebaseInitProvider is declared with initOrder 100 and directBootAware true. Content providers run during Application creation, before any Activity can show a consent screen, and a direct boot aware provider may start before the device is unlocked. Through it the full Google Analytics for Firebase pipeline (receiver, service and job service) starts together with Crashlytics, Sessions and Installations. The AD_ID permission is declared. A search of all 255 resource strings and every string in the five dex files for onetrust, didomi, usercentrics, iabtcf, consentmanager, cmpsdk and tcf returned no match, and no manifest component resembles a consent screen. The Data Safety section of the app states: No data shared with third parties. Whether Google acts as a service provider or as a third party for this processing is a disputed labelling question in the industry, so this report states the tension and makes no claim that the label is false. Whether the pipeline transmits before any user action was not measured and no traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the data comes from a lactation device and works as a postpartum feeding signal, the start precedes any possible consent screen, and no consent platform exists in the package. The CVSS vector scores only the technical exposure of low sensitivity telemetry and no traffic was captured.

```
<provider android:authorities="com.chiaro.elviepump.firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<receiver android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measurement.AppMeasurementReceiver"/>
<service android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measurement.AppMeasurementService"/>
<service android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measurement.AppMeasurementJobService" .../>
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>

Consent platform strings searched in res/values/strings.xml (255 entries) and classes
    *.dex: 0 matches
```

Impact: A person who pumps milk with a health related device is measured by analytics and advertising identifiers from the first launch, before any consent screen can exist, in an app whose store label says that nothing is shared.

Fix: Disable Firebase Analytics collection in the manifest, start it only after a recorded consent, and align the Data Safety section with the Google pipeline that remains.

H1: The Firebase API key, the project configuration, a legacy Realtime Database URL and the storage bucket of project elvie-pump 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 values sit in res/values/strings.xml of every copy distributed through Google Play. Google documents that Firebase keys are not secret by design, so this is an availability and resilience finding and not a confidentiality finding. An extracted key allows quota probing against the project. The legacy firebaseio.com URL means that Firebase security rules, in addition to the rules of the storage bucket, must deny unauthenticated access. Without enforced App Check the backend cannot tell the real app from a replayed key. RFI-IRFOS did not test the endpoint, and the rules are UNVERIFIED.

```
<string name="firebase_database_url">https://elvie-pump.firebaseio.com</string>
<string name="gcm_defaultSenderId">254733974683</string>
<string name="google_api_key">AIzaSyB9G9CjeQi7NlGBpsDX6knBv7Lc0aeuUrQ</string>
<string name="google_app_id">1:254733974683:android:58ad2ea745085c1d</string>
<string name="google_crash_reporting_api_key">AIzaSyB9G9CjeQi7NlGBpsDX6knBv7Lc0aeuUrQ
    </string>
<string name="google_storage_bucket">elvie-pump.appspot.com</string>
<string name="project_id">elvie-pump</string>
<string name="default_web_client_id">254733974683-tfq5uv7202vq1n9vjungat4iv1kdifa8.
    apps.googleusercontent.com</string>
```

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

Fix: Confirm that the Realtime Database and storage rules deny by default, enforce App Check, and restrict the key by package and certificate.

H2: The FullStory session replay SDK is instrumented into the Compose interface and no in-app consent screen exists

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

The dex files hold the FullStory bootstrap and Compose specific instrumentation classes for anchors, views, canvas, click modifiers and annotated strings. The SDK observes the screen structure and interaction of this app and is not an unused dependency. It ships its own consent state plumbing, a consent_settings table and an FS.consent call. No manifest component, string resource or dex string resembles a consent screen for it. Whether FS.consent is called unconditionally at start, or after a user action, is a control flow question that this analysis of resources and strings could not answer, so the trigger is UNVERIFIED. The masking capability of the SDK is a design feature in the operator's favour. Whether it masks health related fields in this app is not shown.

```
com/fullstory/FS
com/fullstory/instrumentation/Bootstrap
com/fullstory/instrumentation/frameworks/compose/FSComposeAnchor
com/fullstory/instrumentation/frameworks/compose/FSComposeAndroidComposeView
com/fullstory/instrumentation/frameworks/compose/FSComposeCanvas
com/fullstory/instrumentation/frameworks/compose/FSComposeClickModifier
com.fullstory.LOG_PRIVACY_RULES
FS.consent(consented: %b)
"select consent_state from consent_settings where app_id=? limit 1;"
```

Impact: If session replay is active, screens that show pumping controls, milk volumes and account settings can be recorded as interaction data.

Fix: State in the privacy policy whether session replay runs, name the recipient, mask health related screens, and start the SDK only after consent.

H3: Elvie Pump and Elvie Trainer share one signing certificate and one OAuth endpoint, which points to one identity plane over lactation and pelvic floor data

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

Both apps are signed with the same certificate and both reference the same token endpoint auth.chiaro.co.uk/oauth/token and the same API host api.chiaro.co.uk, differentiated by the path segments pump and trainer. Each app uses its own Firebase project (elvie-pump and elvie-trainer, with different keys, sender ids and buckets), so telemetry is separated while the identity infrastructure is shared. The Trainer binary also references delete-my-account and reset-product-data endpoints that the Pump binary does not reference. That does not show that the Pump app has no deletion route, because only strings were read. Whether one account or one bearer token reaches both data categories was not tested and is UNVERIFIED. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because two kinds of intimate body data, lactation and pelvic floor, plausibly sit behind one authorization server. The CVSS vector scores zero because the package shows shared infrastructure and no weakness.

```
Elvie Pump    (com.chiaro.elviepump)  signer SHA-256
    db4be23befc3656ad3a55571d486c0df25411717008b425f99a8faa4ce6fad3c
Elvie Trainer (com.uk.elvie)          signer SHA-256
    db4be23befc3656ad3a55571d486c0df25411717008b425f99a8faa4ce6fad3c
    CN=Ben Levy, OU=Product, O=Chiaro, L=London, ST=London, C=GB

Pump endpoints:    https://api.chiaro.co.uk/pump/
                   https://auth.chiaro.co.uk/oauth/token
                   https://auth.chiaro.co.uk/password/email
Trainer endpoints: https://api.chiaro.co.uk/trainer/
                   https://auth.chiaro.co.uk/oauth/token
                   https://auth.chiaro.co.uk/password/email
                   https://auth.chiaro.co.uk/delete-my-account
                   https://auth.chiaro.co.uk/reset-product-data
```

```
Firebase elvie-pump:    google_api_key AIzaSyB9G9CjeQi7NlGBpsDX6knBv7Lc0aeuUrQ, sender
     254733974683
Firebase elvie-trainer: google_api_key AIzaSyCkuAhSCG9cBRnbjzz_VyUfkIq-y6P-hE0, sender
     499019774832
```

Impact: A parent who pumps and also trains the pelvic floor with the same company may have both kinds of intimate data behind one account, without being told how the two are separated.

Fix: State whether the two apps share accounts, show how tokens are scoped per app, and document the impact assessment for the combined identity.

M1: No network security configuration and no certificate pinning for the endpoints that carry OAuth tokens and pumping session 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 declares no networkSecurityConfig and the resource tree has no network_security_config.xml. Because targetSdkVersion is 35, the platform default denies cleartext traffic, which is a point in the app's favour. No pinning exists for auth.chiaro.co.uk or api.chiaro.co.uk. An attacker who can install a trusted CA on the device could read the channel.

```
<application ... />   (no android:networkSecurityConfig attribute)

res/xml/ contains no network_security_config.xml
targetSdkVersion 35
```

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

Fix: Add a network security configuration with pinning for auth.chiaro.co.uk and api.chiaro.co.uk.

M2: Five activities are exported on the custom elvieapp scheme and the package does not show whether they validate the caller

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, rated LOW in this report

Five activities for account, home, session history, insights and pump controls are exported and respond to VIEW intents on the scheme elvieapp. Custom schemes have no domain verification, so any app on the device can send a matching intent. Whether the activities validate the caller, require a permission or check the intent extras is a control flow question that this analysis could not answer. Exploitability is UNVERIFIED. This is an observation about the attack surface, and no vulnerability is claimed.

```
<activity android:exported="true" android:name="...feature.account.activity.
    AccountActivity" ...>
    <data android:host="account" android:scheme="elvieapp"/></activity>
<activity android:exported="true" android:launchMode="singleTask" android:name="...ui.
    home.HomeActivity" ...>
    <data android:host="home" android:scheme="elvieapp"/></activity>
<activity android:exported="true" android:launchMode="singleTask" android:name="...ui.
    history.SessionHistoryActivity" ...>
    <data android:host="sessions" android:scheme="elvieapp"/></activity>
<activity android:exported="true" android:name="...ui.insights.InsightsActivity" ...>
    <data android:host="insights" android:scheme="elvieapp"/></activity>
<activity android:exported="true" android:name="...feature.controls.activity.
    ControlsActivity" ...>
    <data android:host="controls" android:scheme="elvieapp"/></activity>
```

Impact: The finding concerns attack surface. It does not describe a harm that was shown.

Fix: Confirm caller validation in the five activities, or move the entry points to verified App Links.

M3: The privacy policy offers an Article 27 representative and the linked contact document returns HTTP 404

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 in the notice text without a severity label, open, rated MEDIUM by blast-radius escalation

The privacy policy at global.elvie.com/privacy-policy, read on 2026-08-22, says that residents of the EEA can find the contact details of the representative in the EEA through a link. The linked PDF has a filename from 2021 under the former operator Chiaro Technology. A header request on 2026-08-22 returned a redirect and then HTTP 404, and no alternate path was found. The policy shows that a representative mechanism exists, which many peers lack. This finding concerns the broken link. Who holds the mandate today is UNVERIFIED. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the dead link is the only route the policy offers to reach the representative, and the controller sits outside the Union. The CVSS vector scores zero because this is a legal and transparency finding with no technical attack path.

```
$ curl -sIL "https://www.elvie.com/assets/main/downloads/chia01---representative-
    contact-summary-2021.pdf"
HTTP/2 301  ->  https://elvie.com/assets/main/downloads/chia01---representative-
    contact-summary-2021.pdf
HTTP/2 404

"If you are a resident of the EEA and wish to contact our representative in the EEA,
    you can find their contact details here."
```

Impact: A person in the EEA who wants to reach the representative of the controller finds a dead link.

Fix: Publish a working document that names the current representative and its contact route, and confirm the mandate.

Impact Analysis

The people affected are users of the Elvie Pump and Elvie Stride apps. The data includes pumping sessions with volume, timing and frequency, account data and device identifiers, and where Elvie Trainer is also used, pelvic floor sensor data on the same identity infrastructure. The sessions work as a postpartum feeding schedule.

C1 affects every launch. H1 and M1 concern the technical protection of the backend and the channel. H2 concerns possible recording of the interface. H3 concerns the combination of two intimate data categories. M2 and M3 concern an attack surface observation and a dead representative link.

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

The Complete Chain

Step 1, store: the Data Safety section says that no data is shared with third parties (C1).

Step 2, first launch: FirebaseInitProvider starts Analytics, Crashlytics, Sessions and the AD_ID pipeline with the process (C1). FullStory is instrumented into the interface (H2).

Step 3, sign-in: OAuth against auth.chiaro.co.uk, the same server as Elvie Trainer (H3). No pinning protects the channel (M1).

Step 4, use: pumping sessions are recorded and shown. Five activities can be opened by other apps through the elvieapp scheme (M2).

Step 5, the user acts on a right: the link to the Article 27 representative returns HTTP 404 (M3).

Data Protection: Article by Article

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

Article 5(1)(b), purpose limitation: engaged by H3.

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

Article 5(2), accountability: engaged by C1.

Article 6(1) and Article 7(1), lawful basis and conditions for consent: engaged by C1.

Article 12(1) and Article 13(1)(a), transparent information and identity of the controller: engaged by M3.

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

Article 25, data protection by design and by default: engaged by H1, H2 and H3.

Article 27(1), representative: engaged by M3.

Article 32(1)(a) and (b), security of processing: engaged by H1, M1 and M2.

Article 35, impact assessment: engaged by H3.

Article 5(3) of the ePrivacy Directive, storage of and access to information on the terminal: engaged by C1.

Consumer Protection & Platform Disclosures

The Google Play listing, read on 2026-08-22, shows the app as Pump with Elvie with a PEGI 3 rating. The Data Safety section states that no data is shared with third parties. Publisher and developer entities differ as described under the operator analysis. The sharing statement is the one that C1 sets against the Google pipeline in the package, and the classification of Google as service provider or third party is the open point.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 27 for a controller outside the Union and Article 5(3) of the ePrivacy Directive for terminal access. The controller is registered in the United Kingdom and offers its product to users in Austria, which brings Article 3(2) GDPR into play. 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 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            com.chiaro.elviepump
Version            1.37.11 (versionCode 2136), analysed 2026-08-22
base.apk SHA-256   a6ece41d4d424d555796a8aaf3a398a3eed67769df7c2cf7de649d35979be38f
XAPK SHA-256       ede3c46e984a3cb3acadd968153507bb769c73c404323ae74673505e8473b9dd
Signer SHA-256     db4be23befc3656ad3a55571d486c0df25411717008b425f99a8faa4ce6fad3c
                   CN=Ben Levy, OU=Product, O=Chiaro, L=London, ST=London, C=GB
minSdk / targetSdk 26 / 35

Firebase project   elvie-pump
google_api_key     AIzaSyB9G9CjeQi7NlGBpsDX6knBv7Lc0aeuUrQ
google_app_id      1:254733974683:android:58ad2ea745085c1d
Database URL       https://elvie-pump.firebaseio.com
Storage bucket     elvie-pump.appspot.com
sender id          254733974683
web client id      254733974683-tfq5uv7202vq1n9vjungat4iv1kdifa8.apps.
    googleusercontent.com

Elvie Trainer      com.uk.elvie, project elvie-trainer, sender 499019774832
                   google_api_key AIzaSyCkuAhSCG9cBRnbjzz_VyUfkIq-y6P-hE0
```

```
C1  AndroidManifest.xml (FirebaseInitProvider, AppMeasurement components, AD_ID), res/
    values/strings.xml, classes*.dex
H1  res/values/strings.xml
H2  classes.dex and classes5.dex (com/fullstory)
H3  APK signing block of both apps, classes.dex and classes3.dex (endpoint strings)
M1  AndroidManifest.xml, res/xml (no network_security_config.xml)
M2  AndroidManifest.xml (five exported activities on elvieapp)
M3  global.elvie.com/privacy-policy and the linked PDF (HTTP 404)
```

Reproduction: obtain com.chiaro.elviepump 1.37.11 from Google Play or APKPure, check the SHA-256, decode the manifest and resources with apktool, search the dex strings and print the signing certificate with apksigner. For M3 request the linked PDF header. No device, account or backend access is needed.

Disclosure Timeline & Outcome

2026-08-22 12:49 UTC Notice REF ELVIEPUMP-2026-R1 to privacy@elvie.com, questions@elvie.com and appdev@onewillow.com, CC DSB and EDPS. Findings C1, H1, H2 and H3 in the text, two medium findings summarised, the dead representative link described, three questions asked, reply window 30 days.

2026-08-22 12:49 UTC Mail system failure notice for questions@elvie.com, address not found.

2026-10-17 18:52 UTC Follow-up from security@rfi-irfos.com to the same three addresses, 34 days before the embargo date.

2026-11-15 13:00 UTC Message from s.kepp@rfi-irfos.com to privacy@elvie.com and appdev@onewillow.com, 5 days before the embargo date. It corrects the earlier statement about delivery, removes questions@elvie.com and repeats the three questions.

No reply of any kind has been received as of 21 November 2026, including no automatic acknowledgement.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026. It passed without a reply.

2026-11-21 Final report published.

What Elvie Got Right

The permission footprint is minimal. No RECORD_AUDIO, CAMERA, contacts, biometric or READ_PHONE_STATE permission is requested. The Android 12 Bluetooth migration is correct. Location permissions are capped with maxSdkVersion 30, BLUETOOTH_SCAN carries neverForLocation, and a dedicated activity explains the legacy location request. No advertising or attribution SDK was found among AppLovin, AdMob, Meta Audience Network, Vungle, Unity Ads, ironSource, InMobi, Moloco, AppsFlyer, Adjust and Branch. No PRC or sanctioned jurisdiction SDK or endpoint appears among more than 15 markers. The app has no billing SDK. allowBackup is false, and target SDK 35 denies cleartext traffic by platform default. The telemetry projects of the two Elvie apps are separate. The privacy policy names an Article 27 representative mechanism, and the finding concerns only the broken link.

Residual Risk & Recommendations

Open on 21 November 2026: all seven items, with no written position from the operator. Items that only the operator can close are the consent control and Data Safety alignment in C1, the database and storage rules in H1, the replay status and masking in H2, the account and token scope across the two apps in H3, caller validation in M2 and the representative mandate in M3.

Recommendations: disable Analytics collection in the manifest and enable it after consent, align the store label, confirm deny by default rules and App Check, state and mask session replay, document the shared identity and its impact assessment, add pinning, validate callers or use App Links, and publish a working representative contact.

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 and public documents. No servers or accounts probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF ELVIEPUMP-2026-R1.