Security & Privacy Disclosure, Final Report

Hume Health (com.elink.fittrackhealth.pro)

A body composition app whose operator appears under four names, with analytics that start before consent.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 19 NOVEMBER 2026. ONLY AUTOMATED MESSAGES AND A SHORT ESCALATION NOTICE, NO SUBSTANTIVE REPLY.

Target	Hume Health (Hume Health LLC, Hume Health Corp, FitTrack Inc)
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	9.24.0 / 6023 (analysed 2026-08-21)
Findings	8: 3 High, 4 Medium, 1 Low (C1 reassessed from Critical, H3 from High)
Status	AUTOMATED MESSAGES AND A SHORT ESCALATION NOTICE (15 NOVEMBER 2026) ONLY, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`36ccd4821abe0fd8eca8f732a66b9d92b0837760eec8d9a2409cb4e77e13ea00`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Findings 6

5.1 C1: Operator identity splits across four names, Apple lists a dead privacy policy link, and no EU representative is named . . . 6

5.2 H1: Firebase and Sentry providers initialise before any consent screen, and the app code contains no consent management . . . 8

5.3 H2: Klaviyo marketing SDK is wired into the analytics layer and the policy's recipient categories are not mapped to named processors . . . 9

5.4 H3: The body composition data path runs through a Bluetooth SDK under the namespace aicare.net.cn that the policy does not name . . . 10

5.5 M1: Location is described as coarse on Apple, as precise GPS in the policy, and requested as fine in the manifest, with three location SDKs bundled . . . 11

5.6 M2: One Google API key serves maps and crash reporting, with no evidence of restriction . . . 12

5.7 M3: A notification listener service gives unscoped access to the content of every notification once the user grants it . . . 13

5.8 L1: A Facebook App ID is hardcoded but no Facebook SDK is compiled into the app . . . 14

6 Impact Analysis 14

7 The Complete Chain 15

8 Data Protection: Article by Article 15

9 Consumer Protection & Platform Disclosures 16

10 Regulatory & Legal Landscape 16

11 What Hume Got Right 17

12 Indicators of Compromise & Reproducible Evidence 17

13 Disclosure Timeline & Outcome 18

14 Residual Risk & Recommendations 19

Executive Summary

Hume Health is the Android companion app for the Hume Body Pod scale and the Hume Band wearable. It records body composition from bioelectrical impedance readings, weight, heart rate and sleep, and it syncs with Android Health Connect. The package is com.elink.fittrackhealth.pro, version 9.24.0.

On 21 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF HUMEHEALTH-2026-R1 to support@myhumehealth.com, copying devsupport@myhumehealth.com, the Austrian Datenschutzbehörde and the European Data Protection Supervisor. It reported eight findings from a root level code analysis and asked three written questions. A follow-up on 12 September 2026, a reminder on 17 October 2026 and a further follow-up on 15 November 2026, four days before the publication date, restated them. The answers on record are three automated helpdesk messages, on 21 August, 12 September and 18 October 2026, and one short message of 15 November 2026 at 12:38 UTC from the support address. The 18 October message is a queue notice about support delays that mentions refunds and returns. The 15 November message reads ”I’m escalating your message to the appropriate team and someone will follow up with you directly.” None addresses a finding or a question, and no follow-up has arrived as of 21 November 2026.

The governing thesis of this report is that a data subject cannot tell who is responsible. The signing certificate, the Java namespace, the Firebase project and the deep link scheme say FitTrack. Google Play says Hume Health Corp. The privacy policy says Hume Health LLC. The Apple App Store says FitTrack Inc, and the privacy policy link on that listing returned HTTP 404 (C1). No EU representative is named. On top of that identity gap sit the consequences: analytics and crash tooling start before consent (H1), a marketing platform receives profile data (H2), and the vendor library at the start of the body composition path is not named (H3).

The report is specific about limits. No network traffic was captured, so the report shows what the code is built to do and not what a given user sends. The Android network security configuration forbids cleartext traffic without exception, background location is not requested and the body composition arithmetic runs on the phone. The Facebook angle that the audit set out to test was not supported by the binary and is recorded as such (L1).

Scope: Root level code analysis of the Google Play release 9.24.0 (versionCode 6023): manifest, resources, eight dex files, the Flutter and Dart AOT snapshot libapp.so (30.9 MB) and the arm64-v8a native libraries. Public web pages read by plain HTTP GET on 21 August 2026: the Play Store and App Store listings and the privacy policy pages. No backend was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. Report prepared for the publication date. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89.

ID	Severity	Title
C1	HIGH	Operator identity splits across four names, Apple lists a dead privacy policy link, and no EU representative is named
H1	HIGH	Firebase and Sentry providers initialise before any consent screen, and the app code contains no consent management
H2	HIGH	Klaviyo marketing SDK is wired into the analytics layer and the policy's recipient categories are not mapped to named processors
H3	MEDIUM	The body composition data path runs through a Bluetooth SDK under the namespace aicare.net.cn that the policy does not name
M1	MEDIUM	Location is described as coarse on Apple, as precise GPS in the policy, and requested as fine in the manifest, with three location SDKs bundled
M2	MEDIUM	One Google API key serves maps and crash reporting, with no evidence of restriction
M3	MEDIUM	A notification listener service gives unscoped access to the content of every notification once the user grants it
L1	LOW	A Facebook App ID is hardcoded but no Facebook SDK is compiled into the app

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	No substantive reply. Reassessed: transparency and accountability defect with no exploit path.
H1	HIGH	HIGH	No substantive reply.
H2	HIGH	HIGH	No substantive reply.
H3	HIGH	MEDIUM	No substantive reply. Reassessed: transfer to the vendor is not demonstrated.
M1	MEDIUM	MEDIUM	No substantive reply.
M2	MEDIUM	MEDIUM	No substantive reply.
M3	MEDIUM	MEDIUM	No substantive reply.
L1	LOW	LOW	No substantive reply. Records that the Facebook line of inquiry was not supported.

Subject & Operator Analysis

Four names appear across the product surfaces. The signing certificate carries fittrackhealth in every field. The code carries FitTrack and myhealth in its namespace, Firebase project, deep link scheme and a legacy customer domain. Google Play shows the developer as Hume Health Corp. The privacy policy at humehealth.com names Hume Health LLC (doing business as Hume) as controller with an address in Dover, Delaware, which matches the pattern of a registered agent address and was not verified against a company register. The Apple App Store shows FitTrack Inc. The privacy policy URL that the app actually reaches, myhumehealth.com/pages/privacy-policy, redirects with HTTP 301 to humehealth.com/pages/privacy-policy.

The policy names a Data Protection Officer without a direct contact address. It also lists two working support addresses, support@myhumehealth.com and devsupport@myhumehealth.com. The policy cites Standard Contractual Clauses for transfers of EEA and UK data, which implies that EEA users are expected.

Whether Hume Health LLC, Hume Health Corp and FitTrack Inc are related entities is not established by the material. That is the first question put to the operator.

Architecture & Data Flow

The app is a hybrid. A Java and Kotlin platform layer in eight dex files (about 44 MB) wraps a Dart application core compiled into libapp.so (30.9 MB) in the package fittrack_health_flutter. The package name is com.elink.fittrackhealth.pro and the Application class is com.example.watch_flutter_plugin.FlutterApp, a template name that shipped to production.

Data flow as the client shows it: the Hume Pod and Band connect by Bluetooth. Body composition is computed on the phone by six libbh*BodyComposition libraries, one per supported scale generation, behind a Bluetooth service namespaced aicare.net.cn. The analytics layer dispatches events through two strategies, Firebase and Klaviyo, with separate Crashlytics and Sentry services. Location comes from three plugins. Health Connect permissions are granular (steps, weight, heart rate, sleep, body fat). A notification listener mirrors phone notifications to the band.

What the client does not show: the content of Klaviyo and Firebase payloads, what the backend stores, and whether the Bluetooth SDK transmits anything. These are outside the analysis and no claim is made about them.

Findings

C1: Operator identity splits across four names, Apple lists a dead privacy policy link, and no EU representative is named

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 21 August 2026, reassessed in this report

The signing certificate reads CN=fittrackhealth, OU=fittrackhealth, O=fittrackhealth. The launchable activity is com.fittrack.myhealth.MainActivity, the Firebase project is myhealth-production, the Dart application package is fittrack_health_flutter, the deep link scheme is fittrack://app, and the legacy endpoint myhealth.fittrack.com/customer/account/indext is still hardcoded. Google Play lists the developer as Hume Health Corp. The privacy policy at humehealth.com names Hume Health LLC (doing business as Hume) as controller, with an address in Dover, Delaware. The Apple App Store lists FitTrack Inc, and the privacy policy link on that listing, getfittrack.com/pages/privacy-policy, returned HTTP 404 when fetched on 21 August 2026. The privacy policy cites Standard Contractual Clauses for EEA and UK transfers and names no Art. 27 representative. Whether these names are related legal entities (parent, subsidiary, trading name) was not verified against a company register. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the app processes biometric and health-related measurements (body composition, weight, heart rate, sleep) under Standard Contractual Clauses for EEA users, and across the Play Store, the App Store, the privacy policy and the code no single document tells a data subject which entity is the controller. The absence of any EU representative removes the one contact an EU resident could use to enforce rights.

```
Signer #1 certificate DN: CN=fittrackhealth, OU=fittrackhealth, O=fittrackhealth,
                          L=fittrackhealth, ST=fittrackhealth, C=fittrackhealth
```

```
package="com.elink.fittrackhealth.pro"
<application android:label="Hume" android:name="com.example.watch_flutter_plugin.
    FlutterApp" ...>
<activity android:name="com.fittrack.myhealth.MainActivity" ...>
<data android:host="app" android:scheme="fittrack"/>
<string name="project_id">myhealth-production</string>
package:fittrack_health_flutter/main.dart
https://myhealth.fittrack.com/customer/account/indext
```

Surface	Name given	Read on
Signing certificate, Java namespace, Firebase project, Dart package	fittrackhealth, FitTrack, myhealth	Binary
Google Play developer	Hume Health Corp	2026-08-21

Surface	Name given	Read on
Privacy policy, data controller	Hume Health LLC (d/b/a Hume), Dover, DE	2026-08-21
Apple App Store developer	FitTrack Inc, listed policy link returns HTTP 404	2026-08-21

Disclosed as CRITICAL on 21 August 2026. This is an accountability and transparency defect with no exploit path, so the CVSS vector expresses the data exposure it enables and the published severity rests on the escalation reason above.

Impact: A person in Austria who buys the scale or band and wants to ask what is held about their weight, body fat, heart rate and sleep has four possible counterparties, a dead link on one storefront and no representative in the EU.

Fix: Publish one controller identity across all stores and the policy, fix the Apple privacy policy link, name an Art. 27 representative with an EU address, and give the named Data Protection Officer a direct contact address.

H1: Firebase and Sentry providers initialise before any consent screen, and the app code contains no consent management

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)

SentryNdkPreloadProvider (initOrder 2000000000), SentryPerformanceProvider (200), FirebaseInitProvider (100, directBootAware true) and FlutterFirebaseMessagingInitProvider (99) are declared in the manifest. Android instantiates ContentProviders in decreasing initOrder before any Activity, so no consent dialog can run first. A string search of the app's own fittrack_health_flutter Dart package for consent, gdpr, privacy_dialog, cmp_ and tcf returned zero hits, and a search of libapp.so for OneTrust, Didomi, Usercentrics, ConsentManager and ConsentForm also returned zero. The only consent strings in the binary are the IABTCF key names and dma_consent_state machinery that ship dormant inside the Google Analytics for Firebase SDK. No manifest meta-data sets a default consent state. Whether data is transmitted before a choice is the direct consequence of the initialisation order combined with the missing consent gate, and was not observed on the network. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because four SDK providers start at process start on a product that handles body composition, heart rate and sleep data, and the absence of any consent code in the app's own source shows this is the design and not an oversight in one screen.

```
<provider android:authorities="com.elink.fittrackhealth.pro.SentryNdkPreloadProvider"
    android:exported="false" android:initOrder="2000000000"
    android:name="io.sentry.ndk.SentryNdkPreloadProvider"/>
<provider android:authorities="com.elink.fittrackhealth.pro.SentryPerformanceProvider"
    android:exported="false" android:initOrder="200"
    android:name="io.sentry.android.core.SentryPerformanceProvider"/>
<provider android:authorities="com.elink.fittrackhealth.pro.firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.elink.fittrackhealth.pro.
    flutterfirebasemessaginginitprovider"
    android:exported="false" android:initOrder="99"
    android:name="io.flutter.plugins.firebase.messaging.
    FlutterFirebaseMessagingInitProvider"/>
```

Impact: Anyone who installs the app has crash, performance and analytics tooling running from the first launch, before they can accept or refuse anything, on an app built to track their body.

Fix: Disable automatic initialisation in the manifest, start Firebase and Sentry from application code after a recorded consent, and set Consent Mode defaults to denied.

H2: Klaviyo marketing SDK is wired into the analytics layer and the policy's recipient categories are not mapped to named processors

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)

The app's analytics layer (src/data/analytics/core/) implements exactly two strategies, firebase_analytics_strategy.dart and klaviyo_analytics_strategy.dart, next to separate crashlytics and sentry services. A KlaviyoProfile class and the klaviyo_flutter package are present. The privacy policy names ad networks and retargeting platforms, sales and marketing tools, affiliate marketing programs, joint marketing partners, public databases and data providers, data analytics services and performance monitoring tools. From the binary RFI-IRFOS can name Klaviyo (sales and marketing tools) and Firebase and Sentry (analytics and performance monitoring). No AppsFlyer, Adjust, Branch, AppLovin, AdMob display plumbing, ironSource, InMobi, Moloco, Mixpanel, Amplitude or Segment class exists in the eight dex files or the Dart string table. A false positive for the word amplitude in classes6.dex resolved to signal amplitude functions. Which fields reach Klaviyo (body fat, weigh-in frequency, streaks) was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because a marketing and CRM platform receives user profile data as a normal operation of an app that records body composition and heart rate, and the policy lists five recipient categories that the binary substantiates only partly, which leaves a user unable to know who the recipients are.

```
package:fittrack_health_flutter/src/data/analytics/core/klaviyo/
    klaviyo_analytics_strategy.dart
package:klaviyo_flutter/klaviyo_flutter.dart
package:klaviyo_flutter/src/klaviyo_profile.dart
KlaviyoAnalyticsStrategy
KlaviyoProfile(
Klaviyo Public Api Key
```

Impact: A user who weighs in on the scale has a marketing platform receiving profile data about them as routine, and the policy gives them a list of possible recipients that is longer than what the code shows and names none of them.

Fix: Name each recipient and its role in the policy, remove recipient categories that do not apply, and document which fields reach Klaviyo and on what basis.

H3: The body composition data path runs through a Bluetooth SDK under the namespace aicare.net.cn that the policy does not name

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 21 August 2026, reassessed in this report

The manifest declares the service aicare.net.cn.iweightlibrary.wby.WBYService verbatim. The class name reads as a weight and body composition Bluetooth interface library and the package namespace reads as the domain aicare.net.cn. In the arm64 native library split six libraries named libbhBodyComposition.so and libbh1 to libbh5BodyComposition.so perform the on-device conversion from impedance readings to body metrics, next to libRtkAesJni.so (Realtek BLE AES) and libjl_ota_auth.so (BLE OTA authentication). The privacy policy names only generic categories such as data analytics services and cloud computing services. Whether this SDK vendor receives raw bytes off the device, and under which jurisdiction the vendor operates, is UNVERIFIED because no network traffic was captured. The presence of local calculation libraries suggests that at least part of the computation happens on the device.

```
<service android:name="aicare.net.cn.iweightlibrary.wby.WBYService"/>
libbhBodyComposition.so  libbh1BodyComposition.so  ...  libbh5BodyComposition.so
libRtkAesJni.so  libjl_ota_auth.so
```

Disclosed as HIGH on 21 August 2026. This report rates the finding Medium. The demonstrated fact is that a third-party SDK sits in the path of the most sensitive data and is not named. A High rating would need evidence that data leaves the device to that vendor, which the analysis does not contain. The vector uses AT:P for that reason.

Impact: The measurements people take on the Hume scale pass through a vendor library that the privacy policy does not name, so a user cannot find out who handles the first step of their body data.

Fix: Name the SDK vendor and its role in the policy, state whether raw sensor data leaves the device, and document the Art. 28 and Art. 44 position if it does.

M1: Location is described as coarse on Apple, as precise GPS in the policy, and requested as fine in the manifest, with three location SDKs bundled

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)

The Apple App Store privacy label states coarse location only. The privacy policy states "GPS and precise location tracking via mobile device". The Android manifest requests ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION. Three overlapping location plugins are present: com.transistorsoft.locationmanager (a commercial background geolocation library), com.baseflow.geolocator and com.lyokone.location. ACCESS_BACKGROUND_LOCATION is not requested, which limits continuous tracking to foreground and foreground-service scope.

```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE_LOCATION"/>
<service android:foregroundServiceType="location" android:name="com.transistorsoft.
    locationmanager.service.TrackingService"/>
<service android:foregroundServiceType="location" android:name="com.transistorsoft.
    locationmanager.service.LocationRequestService"/>
<service android:foregroundServiceType="location" android:name="com.baseflow.
    geolocator.GeolocatorLocationService"/>
<service android:foregroundServiceType="location" android:name="com.lyokone.location.
    FlutterLocationService"/>
```

The manifest also carries a license key for the transistorsoft library. The value is not reproduced here.

Impact: The same controller tells iPhone users location is coarse, tells everyone in its policy that it is precise GPS, and ships Android users three overlapping location libraries.

Fix: Align the store labels, the policy and the manifest on one description of location use, request only the precision the features need, and remove redundant location libraries.

M2: One Google API key serves maps and crash reporting, with no evidence of restriction

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)

The same Google API key is declared as com.google.android.geo.API_KEY in the manifest and as google_api_key and google_crash_reporting_api_key in res/values/strings.xml. No test against the key was made, so whether it carries application or API restrictions is not known. The vector reflects quota exhaustion as the most plausible effect, which would degrade map display or crash telemetry and not a safety function. The value is abbreviated here and is available in the public APK.

```
<meta-data android:name="com.google.android.geo.API_KEY" android:value="AIzaSyBY90TgKZ
    -UTlrpGJLxkyFl_4K1VvH1ZRQ"/>
<string name="google_api_key">AIzaSyBY90TgKZ-UTlrpGJLxkyFl_4K1VvH1ZRQ</string>
<string name="google_crash_reporting_api_key">AIzaSyBY90TgKZ-UTlrpGJLxkyFl_4K1VvH1ZRQ
    </string>
```

The vector uses AT:P because the effect depends on the key lacking restrictions, which was not tested.

Impact: If the key is unrestricted, someone can use up the quota the app relies on for maps and crash reports, which would degrade those functions for users.

Fix: Restrict the key by application signature and API in the Google Cloud console and use separate keys per service.

M3: A notification listener service gives unscoped access to the content of every notification once the user grants it

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.6 (CVSS-B)

The manifest declares com.example.watch_flutter_plugin.notifications.AndroidNotificationListenerService, exported, bound by android.permission.BIND_NOTIFICATION_LISTENER_SERVICE. It serves a legitimate feature, mirroring phone notifications to the Hume Band. The operating system grant behind it is all or nothing: once a user enables Notification Access, the app can read the content of every notification from every app, including one-time passcodes, message previews and email subjects. The manifest gives no technical scoping of what the service reads.

```
<service android:exported="true"
    android:name="com.example.watch_flutter_plugin.notifications.
    AndroidNotificationListenerService"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action android:name="android.service.notification.NotificationListenerService
    "/>
    </intent-filter>
</service>
```

The vector uses UI:A and AT:P because the user must switch on Notification Access in system settings, which is the platform mechanism for this feature.

Impact: A person who turns on notification mirroring for the band gives the app the ability to read banking codes and private messages on the same phone, for a feature that needs only the notifications they want on their wrist.

Fix: Filter notifications to the apps the user selects, document the data handled by the listener and assess it in a data protection impact assessment.

L1: A Facebook App ID is hardcoded but no Facebook SDK is compiled into the app

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B)

res/values/strings.xml contains facebook_app_id and fb_login_protocol_scheme and the manifest sets com.facebook.sdk.ApplicationId. A search for the com/facebook/ class prefix across all eight dex files returned zero hits. The only Facebook strings are share target package names (com.facebook.katana, com.facebook.orca) and the generic FacebookAuthProvider classes bundled with Firebase Authentication. The notice used this strand to rule Facebook out as a marketing data recipient. Klaviyo (H2) is the conduit the binary supports, Facebook is not.

```
<string name="facebook_app_id">822308861912068</string>
<string name="fb_login_protocol_scheme">fb822308861912068</string>
```

Impact: A leftover third-party identifier ships in every copy of the app without a function, which is an accountability and minimisation gap and carries no demonstrated data flow.

Fix: Remove unused third-party identifiers from the production resources.

Impact Analysis

People affected: owners of the Hume Body Pod and Hume Band, who record body composition, weight, heart rate and sleep over long periods. Biometric and health-related measurements of this kind are the data the GDPR treats with the most care.

- No clear counterparty (C1). A person wanting access or erasure faces four names, a dead policy link on one storefront and no EU representative.
- Tooling that runs before consent (H1). Crash, performance and analytics components start from the first launch.
- A marketing platform as a routine recipient (H2). Profile data goes to a CRM tool, and the policy's recipient list cannot be mapped to the code.
- An unnamed vendor library on the first step of the body data path (H3).
- Conflicting statements on location (M1), a reusable API key (M2) and a notification listener that reads every notification once granted (M3).

The ratings stay conservative. Nothing in the analysis shows what the Klaviyo or Firebase payloads contain, and the code keeps some strong protections, listed below.

The Complete Chain

Step 1, purchase and install: a household buys a Hume scale or band and installs the app. Google Play shows Hume Health Corp, the App Store shows FitTrack Inc, and the signing certificate says fittrackhealth (C1).

Step 2, first launch: Sentry, Firebase and Firebase Messaging providers start at process start, before any consent screen, and no consent code exists in the app's own source (H1).

Step 3, account and profile: the app collects date of birth with no age gate found, and syncs with Health Connect permissions for weight, heart rate, sleep and body fat.

Step 4, weighing in: the scale connects over Bluetooth, the vendor library in the aicare.net.cn namespace sits in the path, and the six native libraries compute body metrics on the phone (H3).

Step 5, analytics: events and profile data go to Firebase and to Klaviyo, a marketing platform (H2). Location libraries and the notification listener add further reach when the user grants those permissions (M1, M3).

Step 6, the person tries to act: the policy names Hume Health LLC and a DPO without a direct address, the Apple listing links a dead policy, and no EU representative is named (C1).

Data Protection: Article by Article

Article	Engaged by	Finding
Art. 4(7)	Four names, one controller to be identified	C1
Art. 5(1)(a)	Disclosures that differ by surface and recipients not mapped	C1, H1, H2, M1
Art. 5(1)(c)	Three location SDKs, unscoped notification access, unused identifier	M1, M3, L1
Art. 5(2)	Controller must be able to demonstrate compliance	C1, H1, L1
Art. 7(1)	Providers initialise before any consent mechanism	H1
Art. 9(1)(2)	Biometric and health measurements, vendor in the path	H3, Impact
Art. 12(1)	Dead policy link on the Apple listing	C1, M1
Art. 13(1)(a)(b)	Controller identity and EU contact	C1
Art. 13(1)(c)	Location purpose and precision	M1
Art. 13(1)(e)	Recipients not named	H2, H3
Art. 27	No EU representative	C1
Art. 28	Processors not identified	H2, H3
Art. 32(1)(b)	Key reuse without evidence of restriction	M2

Article	Engaged by	Finding
Art. 35	Notification access in a DPIA	M3
Art. 44	Transfer question for the vendor SDK, open	H3

Minors and age: the app collects date of birth (dateOfBirth, birthdateMillis) with a bounded date picker. No age gate, minimum age string or parental consent flow was found in the libapp.so string table. The policy says the controller does not knowingly collect data from or market to children under 18. Google Play rates the app Everyone and the App Store lists age 9+. Whether the under-18 exclusion is enforced technically is not established. This is an observation with no standalone severity.

Consumer Protection & Platform Disclosures

Store labels are summaries that users read before the policy. Here the Apple label says coarse location and the policy says precise GPS (M1), and the Apple listing links a policy URL that returned HTTP 404 (C1). RFI-IRFOS makes no determination about either platform's own developer rules and records the conflict between the controller's documents.

Regulatory & Legal Landscape

Competent authority: no EU main establishment is identified, so the one-stop-shop mechanism does not apply and each concerned authority is competent. For a matter initiated from Austria the Österreichische Datenschutzbehörde is the authority, with the European Data Protection Supervisor copied on the notice.

Pre-consent initialisation also engages Art. 5(3) of Directive 2002/58/EC as implemented in Austria by § 165(3) TKG 2021, which requires prior consent for storing or accessing information on terminal equipment unless strictly necessary for a service the user requested.

Comparison within the programme: pre-consent initialisation of Firebase and crash tooling is a recurring pattern. This case differs in the identity gap. The binary and the storefronts carry different operator names, which is rare in the apps reviewed.

What Hume Got Right

- The network security configuration sets cleartextTrafficPermitted to false at base-config level with no domain overrides, stronger than several peer apps in the programme.
- ACCESS_BACKGROUND_LOCATION is not requested anywhere, so continuous tracking is capped to foreground and foreground-service scope.
- Body composition is computed on the phone by six native libraries and not sent off the device as raw readings for basic computation.
- Health Connect permissions are granular and purpose-specific, not a single broad grant.
- BLUETOOTH_SCAN, BLUETOOTH_CONNECT and BLUETOOTH_ADVERTISE carry the neverForLocation flag.
- Two working support addresses exist, and the policy names a Data Protection Officer.

Indicators of Compromise & Reproducible Evidence

Every point below is reproducible by another researcher from the public Google Play release and the public web pages named.

```
Package        com.elink.fittrackhealth.pro
Version        9.24.0 (versionCode 6023)
Size           62.6 MB base.apk, 119.9 MB full split bundle
Stack          8 dex files, Flutter and Dart AOT libapp.so (30.9 MB)

base.apk SHA-256
36ccd4821abe0fd8eca8f732a66b9d92b0837760eec8d9a2409cb4e77e13ea00

libapp.so (arm64-v8a) SHA-256
6ebb7b05b3d58a3939c7a21cc22bccc00d39629e22446cbe976d85095242e6c6
```

```
Signer DN      CN=fittrackhealth, OU=fittrackhealth, O=fittrackhealth
Activity       com.fittrack.myhealth.MainActivity
Firebase       project_id myhealth-production
Dart package   fittrack_health_flutter
Deep link      fittrack://app
Legacy host    myhealth.fittrack.com/customer/account/indext
BLE service    aicare.net.cn.iweightlibrary.wby.WBYService
Facebook ID    822308861912068 (no Facebook SDK classes)
```

```
humehealth.com/pages/privacy-policy         controller Hume Health LLC
myhumehealth.com/pages/privacy-policy        301 to humehealth.com
getfittrack.com/pages/privacy-policy         HTTP 404 (App Store listing link)
Google Play developer                        Hume Health Corp
Apple App Store developer                    FitTrack Inc
```

Chain of custody: the package was not installed on an RFI-IRFOS test device. The APK and the split bundle were obtained from the APKPure CDN. The signer certificate was verified with apksigner on the base APK and on the arm64 split and was identical, a self-signed developer key and not a mirror key, which is consistent with an unmodified copy. No backend was contacted.

Disclosure Timeline & Outcome

2026-08-21 First notice (REF HUMEHEALTH-2026-R1) to support@myhumehealth.com, CC devsupport@myhumehealth.com, the Austrian Datenschutzbehörde and the European Data Protection Supervisor. Findings C1, H1, H2, H3 stated in full, four further findings summarised, three questions asked, reply requested within 14 days.

2026-08-21 Automated helpdesk acknowledgement from support@myhumehealth.com promising a human reply within 24 hours.

2026-09-12 Follow-up to the same addresses restating the findings and three questions with a deadline of 19 September 2026. A second automated acknowledgement of identical wording arrived the same day.

2026-10-17 Reminder from security@rfi-irfos.com, 33 days before publication.

2026-10-18 Third automated message from support, signed by a customer support agent, saying the request is in a queue and that response times are longer than usual, with generic text on order cancellations, returns and warranty. It addresses none of the findings or questions.

2026-11-15 Follow-up from s.kepp@rfi-irfos.com at 12:27 UTC, four days before publication, 86 days after delivery of the first notice.

2026-11-15 Short message from Hume Health Support at 12:38 UTC: the message is being escalated to the appropriate team and someone will follow up directly. It addresses no finding and no question. Whether a person or an automated process wrote it is not verified.

2026-11-21 No substantive reply, no follow-up to the escalation and no delivery failure notice on record.

2026-11-19 Publication date, unchanged since 21 August 2026 and independent of any reply. This report appears on 21 November 2026.

Residual Risk & Recommendations

Open on the evidence of this report: all eight findings. No answer to any question is on record at 21 November 2026. The findings describe version 9.24.0 as analysed on 21 August 2026. The state of later builds is not part of this report.

For the operator, in order of effect: state one controller identity across Google Play, the App Store, the policy and the code, and name an Art. 27 representative with an EU address (C1), move Firebase and Sentry behind a recorded consent (H1), name each recipient including Klaviyo and the Bluetooth vendor and document which fields they receive (H2, H3), align the location description across stores and policy and remove redundant libraries (M1), restrict the Google API key (M2), scope the notification listener (M3), remove the unused Facebook identifier (L1).

For users: review which permissions you granted, in particular Notification Access, and contact the operator in writing with an access request if you want to know which entity holds your data.

Questions that remain open and are not answered by the client: whether the Bluetooth SDK vendor receives data off the device, what the Klaviyo payload contains, and how the four named entities relate.

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 All findings derive from root level code analysis of the published application using publicly available tooling, plus public web pages read by plain HTTP GET. No servers, accounts or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF HUMEHEALTH-2026-R1.