Security & Privacy Disclosure, Final Report

Withings (com.withings.wiscale2), including U-Scan

A carefully built health app with two structural gaps: third-party SDKs that start before consent and Google Cloud keys that ship in every install.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	Withings SAS, Issy-les-Moulineaux, France
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	8.10.0 / versionCode 8100001 (analysed 2026-08-21)
Findings	5: 0 Critical, 2 High, 3 Medium
Regulators in copy	Austrian DSB and EDPS (first notice)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026. ONE REDIRECT TO A BUG BOUNTY PLATFORM, ONE AUTOMATIC CLOSURE NOTICE
SHA-256 (base APK)	`12d62eda5d6804152dc0ab31a5a8a192b636b0e486177f30d43235328e9704c4`

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 4

4 Architecture & Data Flow 5

5 Engagement Summary 5

6 Findings 6
- 6.1 H1: Firebase, Google ML Kit and a Huawei advertising-ID provider start before any consent, no consent platform present . . . 6
- 6.2 H2: Two Google Cloud API keys hardcoded, Firebase project and Realtime Database URL exposed . . . 7
- 6.3 M1: No network security configuration, no certificate pinning . . . 8
- 6.4 M2: RudderStack analytics SDK not named in the privacy policy, runtime destination unverified . . . 9
- 6.5 M3: Breadth of special-category data under one account, including U-Scan urine biomarkers . . . 10

7 Impact Analysis 11

8 The Complete Chain 11

9 Child Protection & Dependent Profiles 12

10 Data Protection: Article by Article 12

11 Regulatory & Legal Landscape 13

12 Indicators of Compromise & Reproducible Evidence 14

13 Disclosure Timeline & Outcome 15

14 What Withings Got Right 15

15 Residual Risk & Recommendations 16

Executive Summary

Withings (com.withings.wiscale2) is the companion app for the Withings family of scales, blood-pressure cuffs, ECG watches and sleep trackers and, since October 2025, for the U-Scan toilet-mounted urine analysis device. The operator is Withings SAS, 2 rue Maurice Hartmann, 92130 Issy-les-Moulineaux, France. On 21 August 2026 RFI-IRFOS disclosed five findings from a root level code analysis of version 8.10.0 under REF WITHINGS-2026-R1.

This is one of the more carefully built apps in the programme, and the report says so first. A sweep for the usual advertising, attribution, session-replay and PRC-linked SDKs found none. Every hardcoded backend hostname sits under withings.com or withings.net or belongs to a processor the app names. The Health Assistant AI feature carries one of the most specific in-app disclosures the programme has read, naming Google Vertex AI, pseudonymisation, EU-only processing and a working consent withdrawal.

The two gaps that remain are structural. Firebase, Google ML Kit and a Huawei advertising-ID provider start as ContentProviders before any screen can ask for consent, with no consent platform in the build and none of the three named in the app privacy policy (H1). And two Google Cloud keys, one for the Firebase project new-healthmate and one for Maps, ship in every install next to a configured Realtime Database URL (H2). Three medium findings concern missing certificate pinning, an unnamed RudderStack analytics SDK and the breadth of special-category data under one account, including U-Scan urine biomarkers.

RFI-IRFOS sent the notice to privacy@withings.com with the Austrian DSB and the EDPS in copy. A follow-up went out on 12 September 2026. On 14 September 2026 Withings Customer Service replied and directed RFI-IRFOS to the YesWeHack public program. RFI-IRFOS answered on 15 September 2026 that a bug bounty platform does not change the addressee of a GDPR notice. A reminder on 17 October 2026 drew an automatic message on 18 October 2026 that the support request was closed. No substantive reply has arrived as of 14 November 2026. Publication stays at 19 November 2026, independent of any reply. The analysis is static, so the report states what the binary and the policy show and marks what only the operator can show.

Scope: Root level code analysis of Withings version 8.10.0 (versionCode 8100001): the base APK (72.07 MB) taken from the split bundle obtained from APKMirror (release page apk/withings/nokia-health-mate/withings-8-10-0-release), cross-checked for version number, developer name and changelog text against the live Google Play listing. The app was not installed. Manifest, resources and the four dex files were decoded and searched. The live privacy policy at withings.com/legal/privacy-policy was read by plain HTTP GET on 21 August 2026. No endpoint was called, no key was used, no account was created, no traffic was intercepted and no runtime instrumentation was used.

ID	Severity	Title
H1	HIGH	Firebase, Google ML Kit and a Huawei advertising-ID provider start before any consent, no consent platform present
H2	HIGH	Two Google Cloud API keys hardcoded, Firebase project and Realtime Database URL exposed
M1	MEDIUM	No network security configuration, no certificate pinning
M2	MEDIUM	RudderStack analytics SDK not named in the privacy policy, runtime destination unverified
M3	MEDIUM	Breadth of special-category data under one account, including U-Scan urine biomarkers

Finding Status at a Glance

ID	Severity	CVSS-B	Status on 14 November 2026
H1	HIGH	6.9	Not answered substantively. Open.
H2	HIGH	6.9	Not answered substantively. Open.
M1	MEDIUM	6.3	Not answered substantively. Open.
M2	MEDIUM	0.0	Not answered substantively. Open.
M3	MEDIUM	0.0	Not answered substantively. Open.

Subject & Operator Analysis

The operator is Withings SAS, 2 rue Maurice Hartmann, 92130 Issy-les-Moulineaux, France, as the live privacy policy states. The policy names privacy@withings.com as the data protection contact and notes the right to complain to the CNIL. Withings SAS is itself an EU legal entity, so no Art. 27 representative is needed.

Because the main establishment is in France, the CNIL is the lead supervisory authority under Art. 56. The first notice copied the Austrian Datenschutzbehörde and the European Data Protection Supervisor.

The app serves the whole Withings hardware range. Withings also uses regional processors for specific features: DPV Analytics for the Cardio Check-Up in the EU, Canada and Hong Kong, and Heartbeat Health in the United States. Google Vertex AI is named as the processing partner for the Health Assistant feature.

Architecture & Data Flow

The app is native Kotlin and Java with four dex files, 317 declared activities, 106 permission entries, 10 providers, 24 services and 19 receivers. minSdkVersion is 32 and targetSdkVersion is 36.

Across the four dex files RFI-IRFOS found 105 distinct hardcoded hostnames. Every core backend hostname sits under withings.com or withings.net, for example account.withings.com, scalews.withings.net and intelligence.withings.com. The remaining hosts belong to named processors for regulated features. No AWS, GCP or Azure non-EU region string was found. Support runs through Zendesk.

The SDK stack is lean. Firebase components, Google ML Kit, a Huawei advertising-ID provider and the RudderStack SDK are present. No ad-mediation, attribution or session-replay SDK and no PRC-linked SDK was found. A China-market code path exists with its own policy URL and its own opt-in consent strings, and it is separated from the global flow.

The app aggregates data from Withings devices and from Health Connect through 35 read and write permissions. U-Scan adds urine biomarker data through a Wpa02 class family. What the RudderStack SDK transmits at runtime and which region Google Vertex AI uses in practice are runtime questions that this review did not examine.

Engagement Summary

The first notice went out on 21 August 2026 to privacy@withings.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy and asked for answers to three questions within 14 days. The window closed on 4 September 2026. A follow-up on 12 September 2026 restated the questions.

On 14 September 2026 Withings Customer Service (request 3025447) replied and directed RFI-IRFOS to the YesWeHack public program. RFI-IRFOS replied on 15 September 2026 that a bug bounty platform does not change who answers the GDPR questions, restated the three questions and asked that the notice reach the data protection and security teams. A reminder followed on 17 October 2026. On 18 October 2026 an automatic message from privacy@withings.com said the support request was already closed and that there would be no reply. No substantive answer to any of the three questions has arrived as of 14 November 2026.

Findings

H1: Firebase, Google ML Kit and a Huawei advertising-ID provider start before any consent, no consent platform present

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)

Three ContentProviders start with the process: MlKitInitProvider (initOrder 99), FirebaseInitProvider (initOrder 100, directBootAware) and Huawei's AAID InitProvider (initOrder 500). Android runs them during Application creation, before any Activity, so before any screen that could ask for consent. The Firebase component registry carries Performance, Auth, Crashlytics, Messaging, Dynamic Links, Remote Config, A/B testing, Sessions and Installations, and FirebaseAnalytics is present as a class. The manifest requests AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID. A search of the four dex files and the resource strings for OneTrust, Didomi, Usercentrics, consentmanager, IABTCF, cmpsdk, Sourcepoint and Cookiebot returned zero matches, and no collection-default-off flag exists in the manifest or the resources. The live privacy policy handles cookies and trackers for the website and does not name Firebase, ML Kit or Huawei Mobile Services as recipients for the Android app.

```
<provider android:authorities="com.withings.wiscale2.mlkitinitprovider" android:
    exported="false"
          android:initOrder="99" android:name="com.google.mlkit.common.internal.
    MlKitInitProvider"/>
<provider android:authorities="com.withings.wiscale2.firebaseinitprovider" android:
    directBootAware="true"
          android:exported="false" android:initOrder="100" android:name="com.google.
    firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.withings.wiscale2.aaidinitprovider" android:
    exported="false"
          android:initOrder="500" android:name="com.huawei.hms.aaid.InitProvider"/>

com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
```

Limits of this finding. The analysis is static. RFI-IRFOS captured no traffic and measured no payload. The finding is the start order and the absence of any technical gate, not a measurement of what each SDK transmits. The app contains consent screens for specific features, noted under What Withings Got Right, and RFI-IRFOS did not trace whether a consent choice at first launch governs these three providers.

The finding is rated below Critical in the notice because the binary carries no ad-mediation network and the policy makes no explicit consent-gating claim that the build contradicts.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app aggregates Art. 9 data from ECG, blood pressure, sleep and urine measurements, and the build offers no technical gate before third-party SDKs start. The same missing gate applies on every launch of a mass-market consumer product.

Impact: On the first launch of an app that holds heart, blood-pressure, sleep and urine mea-

surements, Google and Huawei components are already running and nothing in the build lets a user decline them first.

Fix: Disable automatic initialisation for Firebase Analytics, Crashlytics, Performance and the Huawei provider in the manifest and start them from code only after a recorded consent choice. Name the SDKs as recipients in the app privacy policy.

H2: Two Google Cloud API keys hardcoded, Firebase project and Realtime Database URL exposed

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)

res/values/strings.xml contains a Firebase API key for project new-healthmate and a Google Maps Platform key. The same file configures a Realtime Database URL, new-healthmate.firebaseio.com, and a Storage bucket for that project. Google documents that Firebase API keys are not secrets by design. The exposure is one of availability and configuration: an extracted key can be used against project and Maps quotas, and whether the database and storage rules restrict access depends on server-side settings the binary does not show.

```
google_api_key                AIzaSyBb5H_6VVbr_DP4s2MFc2DYjc-ybZ7opcw
google_crash_reporting_api_key [same value as google_api_key]
google_app_id                 1:655894465677:android:23d5a0248490faa7e066c4
firebase_database_url         https://new-healthmate.firebaseio.com
google_storage_bucket         new-healthmate.appspot.com
gcm_defaultSenderId           655894465677
project_id                    new-healthmate
default_web_client_id         655894465677-bqkicrepbj1fs3as10cabhat5ornado7.apps.
    googleusercontent.com
maps_api_key                  AIzaSyCNTrDQOaCmax6b2N8iHGYpwROhP647N18 [referenced as
    com.google.android.geo.API_KEY]
```

What is not established. RFI-IRFOS sent no request with either key, did not test whether the Realtime Database is active and tested no security rules. No App Check client component is registered in the manifest. Whether enforcement is switched on for the project is a server-side setting. The notice described read, write and quota paths as consequences if the rules are not locked down, and asked the operator to show that they are. It did not assert that they are open.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the keys belong to the production project of an app that handles Art. 9 data and the operator, not an outside observer, holds the evidence that the restrictions and rules are correct (Art. 5(2)).

Impact: A Firebase project and a Maps Platform account that belong to a health app can be reached with keys that every installed copy carries. Beyond consuming quota, what a third party could do depends on rules and key restrictions that the operator has not shown.

Fix: Restrict both keys by application signature and API, enforce App Check, keep Realtime Database and Storage rules at deny-by-default with per-user scoping, and retire the project's database URL if it is unused.

M1: No network security configuration, no certificate pinning

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

The manifest declares no networkSecurityConfig attribute and res/xml/ holds 18 XML files, none of which is a network_security_config.xml. Because targetSdkVersion is 36, the platform default denies cleartext traffic app-wide, which works in the app's favour. Without a configuration, however, no certificate pinning exists for the API hosts that carry weight, blood-pressure, ECG, sleep and U-Scan data, such as account.withings.com, scalews.withings.net and intelligence.withings.com.

```
<application ...>  (no android:networkSecurityConfig attribute)
res/xml/: 18 files, no network_security_config.xml
targetSdkVersion 36: cleartext denied by platform default
```

Limits of this finding. RFI-IRFOS did not test TLS interception. Pinning at code level, for example inside an HTTP client, was not examined, and the finding concerns the configuration layer only.

Impact: On a managed device or hostile network where a rogue certificate authority has been installed, the TLS channel depends solely on the operating-system trust store.

Fix: Add a network security configuration that pins the operator's API domains and denies cleartext explicitly.

M2: RudderStack analytics SDK not named in the privacy policy, runtime destination unverified

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)

The dex files contain the RudderStack Android SDK with its e-commerce event taxonomy: CheckoutStartedEvent, OrderCompletedEvent, PaymentInfoEnteredEvent and CouponAppliedEvent. The SDK's configuration is fetched from a Withings-hosted URL. The same string pool contains api.rudderlabs.com and hosted.rudderlabs.com, the vendor's own US control-plane domains, which most likely are library defaults. The fetched privacy policy addresses cookies and other trackers for the website only and does not name RudderStack.

```
Lcom/rudderstack/android/sdk/core/RudderServerConfigManager
Lcom/rudderstack/android/sdk/core/EventRepository
Lcom/rudderstack/android/sdk/core/ecomm/events/CheckoutStartedEvent
Lcom/rudderstack/android/sdk/core/ecomm/events/OrderCompletedEvent
Lcom/rudderstack/android/sdk/core/ecomm/events/PaymentInfoEnteredEvent
Lcom/rudderstack/android/sdk/core/ecomm/events/CouponAppliedEvent
"https://static.withings.com/content/app/healthmate/rudderstack"
api.rudderlabs.com, hosted.rudderlabs.com (string pool)
```

UNVERIFIED. Which host receives event payloads at runtime, whether the instance is hosted by Withings itself, and whether the SDK starts before or after in-app consent were not determined. The SDK is called from code and is not a manifest ContentProvider. A Withings-hosted instance would answer the recipient question and the transfer question in one step.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the SDK tracks the paywall and purchase funnel of a health-data app and the recipient is not named. CVSS gives a disclosure gap 0.0.

Impact: Subscription and purchase behaviour of users of a health app is tracked by an SDK that the app's privacy policy does not name.

Fix: Name RudderStack or the actual recipient in the app privacy policy, state where the data plane runs and document whether the SDK waits for consent.

M3: Breadth of special-category data under one account, including U-Scan urine biomarkers

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)

The manifest declares 35 distinct Health Connect read and write permissions. They cover steps, distance, exercise and GPS routes, VO2 max, calories, heart rate and variability, blood pressure, blood glucose, oxygen saturation, respiratory rate, body temperature, weight and body composition, sleep, and menstruation, sexual activity, cervical mucus and ovulation tests. Native Withings features add ECG and AFib detection, vascular age, nerve health, stethoscope heart and lung sounds, sleep apnea and snoring detection, and the U-Scan family. A Wpa02 class family implements the U-Scan toilet puck, and the tokens ketone, urine, Nutrio, Calci and specific gravity confirm both launched cartridges are in this build.

```
android.permission.health.*  35 READ_/WRITE_ permission strings, including
    menstruation,
   sexual activity, cervical mucus, ovulation test, blood pressure, blood glucose,
    sleep
Wpa02ToiletActivity  ToiletType  Region  ArmType  Wpa02CartridgeActivationActivity
Wpa02CleansingActivity  Wpa02RinsingActivity  Wpa02HumidityNotificationSchedulerWorker
Wpa02AboutTheBiomarkersViewModel
string tokens: ketone, urine, Nutrio, Calci, specific gravity
```

This is a structural finding. No single technical flaw is reported. Each metric maps to its own scoped activity and permission pair, which is good practice. The risk is the aggregation: cardiac, metabolic, reproductive and sexual-health, sleep and location data under one profile, plus third-party sources through Health Connect. A DPIA under Art. 35 should assess the aggregate risk and not each metric alone. Whether the DPIA was updated for the U-Scan launch of October 2025 is the question the notice asked.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the combination covers reproductive, sexual-health, cardiac and urine data of a consumer population, which raises profiling risk beyond any single flaw. CVSS has no way to score aggregation.

Impact: A single account can hold a person’s heart rhythm, blood pressure, sleep, urine chemistry and menstrual and sexual-health records together, which makes the account a far richer profile than any one measurement.

Fix: Document the aggregate risk in a DPIA that covers U-Scan and the Health Connect data types, and limit cross-use between data categories.

Impact Analysis

The people affected are users of Withings devices and of the app, a consumer population that measures weight, blood pressure, heart rhythm, sleep and now urine chemistry, and that can add menstrual and sexual-health records through Health Connect. The app also supports child profiles.

What the evidence shows is narrow. Third-party SDKs start before any consent choice can be made (H1), the project keys ship in every install (H2), pinning is absent at the configuration layer (M1), one analytics SDK is not named in the policy (M2), and a single account can hold a very rich profile (M3).

The analysis found no evidence of a breach or misuse and did not examine the server side. It does not say what any SDK transmits or what the Firebase rules allow. The practices that matter most for this operator are the ones it already does well, and the report names them below.

The Complete Chain

Step 1, install and first launch: a user installs the app. MIKitInitProvider, FirebaseInitProvider and the Huawei AAID provider start before any screen (H1). The advertising permissions are present (H1).

Step 2, account and device setup: the user connects a scale, a watch or a U-Scan device. Feature-specific consents appear for the Health Assistant and the Cardio Check-Up, and the child profile has a guardian declaration. The build offers no first-launch gate for the three providers in Step 1 (H1).

Step 3, daily use: the user's measurements travel to Withings hosts that sit under withings.com and withings.net. No pinning exists at the configuration layer (M1). RudderStack records purchase-funnel events and the policy does not name it (M2).

Step 4, aggregation: the account holds cardiac, metabolic, urine, sleep and reproductive-health data together (M3).

Step 5, the project behind the app: Firebase and Maps keys ship in every install, and a Realtime Database URL is configured for the project (H2).

Step 6, the user tries to act: privacy@withings.com is a working channel and the policy names the CNIL. The questions in the notice about SDK recipients and the DPIA remain unanswered.

Child Protection & Dependent Profiles

The app lets an adult create a child profile and declares a guardian consent flow: the guardian states that they are the child's legal guardian and consents together with the child to the access and storage of the child's health data. This is a real safeguard and the report credits it. The findings above apply to child profiles as well, because the pre-consent SDK start (H1) and the aggregation of data (M3) are properties of the app as a whole.

Data Protection: Article by Article

Article 5(1)(a) and Article 13(1)(e): engaged by H1 and M2. Firebase, ML Kit, the Huawei provider and RudderStack are not named as recipients in the policy text for the app.

Article 5(1)(c): engaged by M3. The breadth of data under one account is a minimisation question.

Article 5(2): engaged by H1 and H2. The operator carries the burden of showing consent gating, key restrictions and server-side rules.

Article 6(1), Article 7(1) and ePrivacy Directive Article 5(3): engaged by H1. Processing and access to terminal equipment begin before a consent screen can exist.

Article 9: engaged by H1 and M3. ECG, AFib, blood pressure, urine biomarkers and reproductive-health records are health data.

Article 25 and Article 32(1)(a) and (b): engaged by H2 and M1. Project keys ship in every install and no certificate pinning exists at the configuration layer.

Article 35: engaged by M3. A DPIA should cover the aggregate risk, including the U-Scan launch.

Not engaged: Article 27, because Withings SAS is established in France, and Article 44 and 46 on the evidence found, because the backend hostnames sit under the operator's own domains and named processors.

Regulatory & Legal Landscape

The CNIL is the lead supervisory authority under Art. 56 because the main establishment is in France, and the policy directs data subjects to it. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the first notice in copy. The U-Scan device and other measuring devices may fall under the Medical Device Regulation, which is enforced by other authorities. This report makes no claim about the regulatory classification of any Withings device.

The pre-consent initialisation pattern in H1 recurs across health and consumer apps in the RFI-IRFOS programme, which treats every operator under the same rules regardless of size. Compared with that corpus, Withings has a leaner SDK stack and a more specific AI disclosure than most, and the same structural gap.

Indicators of Compromise & Reproducible Evidence

Every point below can be checked against the public Google Play build, the mirror release page and the public privacy policy.

```
Package         com.withings.wiscale2
Version         8.10.0 / versionCode 8100001
base.apk        SHA-256 12
    d62eda5d6804152dc0ab31a5a8a192b636b0e486177f30d43235328e9704c4
                72.07 MB, from the split bundle (26 splits, 205.97 MB)
Source          APKMirror, apk/withings/nokia-health-mate/withings-8-10-0-release
Min/target SDK  32 / 36
Code base       native Kotlin and Java, four classes*.dex
```

```
Firebase project   new-healthmate
App ID             1:655894465677:android:23d5a0248490faa7e066c4
Sender ID          655894465677
Realtime Database  https://new-healthmate.firebaseio.com
Storage bucket     new-healthmate.appspot.com
API key and Maps key: present in res/values/strings.xml, values as extracted:
    AIzaSyBb5H_6VVbr_DP4s2MFc2DYjc-ybZ7opcw and
    AIzaSyCNTrDQOaCmax6b2N8iHGYpwROhP647N18
```

```
com.google.mlkit.common.internal.MlKitInitProvider       initOrder 99
com.google.firebase.provider.FirebaseInitProvider        initOrder 100,
    directBootAware
com.huawei.hms.aaid.InitProvider                          initOrder 500
com.rudderstack.android.sdk.core (e-commerce events), config https://static.withings.
    com/content/app/healthmate/rudderstack
Wpa02* class family (U-Scan), 35 android.permission.health.* strings
Policy   https://www.withings.com/legal/privacy-policy (read 2026-08-21)
Contact  privacy@withings.com
```

```
apktool d on the base APK: AndroidManifest.xml, res/values/strings.xml, res/xml
strings and grep over classes*.dex
search for onetrust, didomi, usercentrics, consentmanager, iabtcf, cmpsdk, sourcepoint
    , cookiebot: 0 matches
res/xml: 18 files, no network_security_config.xml
```

Disclosure Timeline & Outcome

2026-08-21 First notice (REF WITHINGS-2026-R1) to privacy@withings.com, CC dsb@dsb.gv.at and edps@edps.europa.eu, with three questions and a 14-day reply request.

2026-09-04 The 14-day reply window closed with no answer.

2026-09-12 Follow-up to privacy@withings.com restating the three questions.

2026-09-14 Reply from Withings Customer Service (request 3025447) directing RFI-IRFOS to the YesWeHack public program.

2026-09-15 RFI-IRFOS replied that a bug bounty platform does not change the addressee of a GDPR notice, restated the three questions and asked for routing to the data protection and security teams.

2026-10-17 Reminder to privacy@withings.com, 33 days before publication.

2026-10-18 Automatic message from privacy@withings.com that the support request was already closed and there would be no reply.

2026-11-14 No substantive reply to any of the three questions.

2026-11-19 Publication date, unchanged since the first notice.

What Withings Got Right

No ad-mediation, attribution or session-replay SDK exists in the binary, and a sweep for 25 common SDKs of that kind, including AppLovin, AdMob, Meta Audience Network, AppsFlyer, Adjust, Amplitude, Mixpanel, ContentSquare and Clarity, returned nothing. No PRC-linked SDK was found, and the China-market code path has its own consent strings and policy URL. No hardcoded endpoint routes traffic to a non-EU cloud region.

The Health Assistant disclosure is specific. It says data is pseudonymised before it is sent to Google, that Google receives only a technical ID, that Google does not keep the data or use it for training, that Google Vertex AI processes the data exclusively within the European Union, that no decision with legal or medical significance is taken by the AI alone, and that consent can be withdrawn in Settings with immediate effect.

The child profile has a guardian declaration. Cardio Check-Up has three independent consents. The ECG feature enforces a US age gate of 22 and the Cardio Check-Up uses different named processors by region. Android backup is disabled, targetSdkVersion is 36 and privacy@withings.com is a working data protection channel.

Residual Risk & Recommendations

Everything in the findings table is open at the date of publication. A final APK diff before 19 November 2026 determines the state the published report records.

What remains unknown and matters most: whether a first-launch consent choice governs MlKitInitProvider, FirebaseInitProvider and the Huawei provider in practice, which host receives RudderStack events, whether the Firebase database and project rules and the Maps key restrictions are tight, and whether the DPIA covers the aggregate risk since U-Scan.

Recommendations: gate Firebase, ML Kit and the Huawei provider behind a recorded consent choice and name them as recipients in the app privacy policy. Restrict both Google Cloud keys, enforce App Check and keep database and storage rules at deny-by-default. Add a network security configuration with pinning for the API domains. Name RudderStack or its actual recipient and the data-plane location. Update the DPIA for the aggregate profile, including U-Scan and the Health Connect categories.

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 a public privacy policy read by plain HTTP GET. No Withings server, key or account was used. Final report, published 21 November 2026. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG and GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF WITHINGS-2026-R1.