Security & Privacy Disclosure, Final Report

Wearfit Pro for Android (com.wakeup.howear)

An operator policy that places blood pressure, blood sugar, heart rate and sleep data on servers in China without a named transfer safeguard, in an app with more than 10 million installs.

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

Target	Shenzhen Weike Technology Co., Ltd. (Wearfit Pro, developer account Wakeup)
Versions Audited	hw_5.6.09 / versionCode 2026081417 (Play update 2026-08-14, analysed 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	9: 1 High, 6 Medium, 2 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`0fa1272519b23ec68dec283729b30224d3f73176357c0aac4c0381f5fe12371b`

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 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Findings 7

5.1 C1: Operator states that all collected data, including blood pressure, blood sugar, heart rate and sleep, is stored on servers in the People's Republic of China, with no transfer safeguard named . . . 7

5.2 H1: Chinese speech-cloud library and endpoints bundled next to microphone permissions for a "real-time translation" feature . . . 8

5.3 H2: NotificationListenerService gives access to the notifications of every app on the phone, while the manifest holds no SMS permission . . . 9

5.4 H3: Five SDK ContentProviders initialise at process start before any consent screen can run, and no consent management platform is present . . . 10

5.5 M1: Pinned certificate for bjol.luxhub.top expired on 2025-09-18 and was still the only trust anchor in the August 2026 build . . . 11

5.6 M2: Cleartext traffic permitted for all hosts and user-installed CA certificates trusted globally . . . 12

5.7 M3: Device identifier bundle with IMEI, IMSI, SIM serial, hardware serial and OAID, plus the installed apps inventory . . . 13

5.8 M4: Policy describes third-party applications that can read sensor, sleep, exercise and location data from the paired wearable . . . 14

5.9 L1: PEGI 3 rating, an under-14 parental-consent statement and a date-of-birth field, with no age gate located . . . 15

6 Impact Analysis 15

7 The Complete Chain 16

8 Operator Cluster and Shared SDK Choices 16

9 Data Protection: Article by Article 17

10 Regulatory & Legal Landscape 17

11 Indicators of Compromise & Reproducible Evidence 18

12 Disclosure Timeline & Outcome 19

13 What Was Done Well 19

14 Residual Risk & Recommendations 19

Executive Summary

Wearfit Pro is the Android companion app of smartwatches and wearables, published on Google Play by the developer account Wakeup with more than 10 million downloads. The operator is Shenzhen Weike Technology Co., Ltd. in Shenzhen. People use the app to record sleep, heart rate, blood pressure and blood sugar, to receive notifications on a wearable and to use a translation feature.

The most serious finding is written by the operator itself. Its English privacy policy says that the collected information "will be transmitted and stored on servers within the People's Republic of China" and calls sleep, heart rate, blood pressure and blood sugar "personal sensitive information". The build contains .cn backend hostnames that match those data categories. Neither the policy nor the build names Standard Contractual Clauses, a transfer impact assessment or an EU representative (C1).

Further findings cover a Chinese speech-cloud library and endpoints next to microphone permissions (H1), a notification listener that reads every app's notifications while the manifest holds no SMS permission (H2), five SDKs that initialise before any consent screen can run (H3), an expired pinned certificate (M1), a global cleartext override (M2), a wide device identifier set (M3), a policy that lets unnamed third-party applications read wearable data (M4) and a PEGI 3 rating without a located age gate (L1).

The notice went to the four addresses found for the operator, one of which rejected it. A follow-up with three written questions and a second reminder followed. As of 14 November 2026 no reply or acknowledgment has arrived. The publication date of 20 November 2026 stands independent of any reply.

Scope: Root level code analysis of the Google Play release hw_5.6.09 (versionCode 2026081417) as an XAPK bundle: decoded manifest and resources, strings extraction across 16 dex files, native library inventory of the armeabi-v7a split, and the operator's public privacy policy and corporate site. The React Native JavaScript bundle was scanned for plain-text domains only. No traffic was captured, the app was not installed and no third-party system was tested. Statements that need runtime evidence are marked UNVERIFIED.

ID	Severity	Title
C1	HIGH	Operator states that all collected data, including blood pressure, blood sugar, heart rate and sleep, is stored on servers in the People’s Republic of China, with no transfer safeguard named
H1	MEDIUM	Chinese speech-cloud library and endpoints bundled next to microphone permissions for a ”real-time translation” feature
H2	MEDIUM	NotificationListenerService gives access to the notifications of every app on the phone, while the manifest holds no SMS permission
H3	MEDIUM	Five SDK ContentProviders initialise at process start before any consent screen can run, and no consent management platform is present
M1	LOW	Pinned certificate for bjol.luxhub.top expired on 2025-09-18 and was still the only trust anchor in the August 2026 build
M2	MEDIUM	Cleartext traffic permitted for all hosts and user-installed CA certificates trusted globally
M3	MEDIUM	Device identifier bundle with IMEI, IMSI, SIM serial, hardware serial and OAID, plus the installed apps inventory
M4	MEDIUM	Policy describes third-party applications that can read sensor, sleep, exercise and location data from the paired wearable
L1	LOW	PEGI 3 rating, an under-14 parental-consent statement and a date-of-birth field, with no age gate located

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

The Disclosed column shows the label used in the first notice. The This report column shows the rating after the CVSS v4.0 reassessment in this report.

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Policy wording and hostnames as recorded in version hw_5.6.09. Data flow on the wire is UNVERIFIED.
H1	HIGH	MEDIUM	No reply. Reassessed down because transmission of audio is UNVERIFIED.
H2	HIGH	MEDIUM	No reply. Use of notification content is UNVERIFIED.
H3	HIGH	MEDIUM	No reply. Reassessed down because collection by each provider is UNVERIFIED.
M1	MEDIUM	LOW	No reply. Attribution of the domain is UNVERIFIED.
M2	MEDIUM	MEDIUM	No reply. Plaintext use on the wire is UNVERIFIED.
M3	MEDIUM	MEDIUM	No reply. Runtime reads of the identifiers are UNVERIFIED.
M4	MEDIUM	MEDIUM	No reply. The authorisation screen was not observed.
L1	LOW	LOW	No reply. Enforcement of the age check is UNVERIFIED.

Subject & Operator Analysis

Wearfit Pro is the Android companion app for smartwatches and wearables sold under the Wearfit label, published on Google Play under the package com.wakeup.howear by the developer account Wakeup. The Google Play listing shows more than 10 million downloads, a rating of 2.9 from 127,000 reviews, PEGI 3 and the category Health & Fitness. The reviewed build is hw_5.6.09 (versionCode 2026081417).

The privacy policy and the corporate site iwhop.com name the operator as Shenzhen Weike Technology Co., Ltd., trading as WAKE UP Technology, with its address at Room 4208, Tower A, Hongrongyuan North Station Center, Beistation Community, Minzhi Street, Longhua District, Shenzhen, People's Republic of China (ICP filing Yue ICP Bei 16118838). The corporate site markets WEARFIT OS, WEARFIT Cloud Services and a one stop hardware solution service. The app therefore looks like a client for a platform that the operator also sells to third parties.

No EU establishment, no EU address and no Art. 27 representative appear in the binary, the Google Play listing, the privacy policy or the corporate site. The privacy contact in the policy is common@iwhop.com.

Architecture & Data Flow

Wearfit Pro is a native Android shell of 16 dex files with an embedded React Native module (Hermes engine, assets/index.android.bundle). It ships a large native stack in the armeabi-v7a split: FFmpeg, OpenCV, ONNX Runtime, ncnn, the Agora real-time communication SDK, VLC and the libmsc.so speech library. The target SDK is 35 and the minimum SDK is 26. The manifest declares 80 permissions.

The location and push layer combines Baidu, Alibaba Amap, Huawei HMS, Honor Push, Xiaomi MiPush and JPush. Payment and login SDKs from Tencent are present. The advertising layer includes Google Mobile Ads, AppLovin, ByteDance Pangle, Mintegral, BIGO Ads and AnyThink/TopOn. The backend estate is a set of .cn hostnames under iwhop.cn.

Which fields leave the phone toward which host is UNVERIFIED. The review decoded the manifest and resources and extracted strings from the dex files and the native library names. It made no bytecode control-flow pass and no traffic capture.

Findings

C1: Operator states that all collected data, including blood pressure, blood sugar, heart rate and sleep, is stored on servers in the People's Republic of China, with no transfer safeguard named

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7 (CVSS-B)

Section 5 of the operator's own English privacy policy says that the information described in the policy "will be transmitted and stored on servers within the People's Republic of China". The same policy calls sleep, heart rate, blood pressure and blood sugar "personal sensitive information" and lists a device identifier bundle that includes IMEI, IMSI, Android advertising ID and hardware serial number. The dex files hold backend hostnames on the .cn top-level domain whose names match those data categories. The policy and the build name no Standard Contractual Clauses, no transfer impact assessment and no other Art. 46 safeguard.

```
5. Data Storage Location and Duration

The above information will be transmitted and stored on servers within the
People's Republic of China.
```

```
Health Data Management... we need to collect your sleep, heart rate, blood pressure,
blood sugar, MET, etc. Health data is personal sensitive information
```

```
api-cluster.iwhop.cn      gateway.iwhop.cn          howear.iwhop.cn
health-monitor.iwhop.cn   health-pro.iwhop.cn       health-news.iwhop.cn
gps.iwhop.cn              city-checkin.iwhop.cn     hkcos-material.iwhop.cn
mall.iwhop.cn             medal.iwhop.cn            micro-life.iwhop.cn
```

Every host in the list is a .cn name, and health-monitor, health-pro and gps match the data categories that the policy enumerates. No .eu host, no region-scoped endpoint and no second storage region appears in the manifest, the resources or the dex strings. The policy is linked from the Google Play listing under App support.

The controller discloses the storage location, so the transparency element of Art. 5(1)(a) is partly met. The legal basis for the transfer is the gap. The People's Republic of China has no EU adequacy decision, and Art. 7 of the PRC National Intelligence Law obliges organisations to support national intelligence work. A transfer impact assessment under Art. 46 has to address that access risk. Whether any such assessment exists is not stated anywhere in the material reviewed.

What data actually leaves the phone on which request is UNVERIFIED, because no traffic was captured. The finding rests on the operator's own written statement and on the hostnames in the build.

Impact: People who wear a Wearfit Pro device and track blood pressure, blood sugar, heart

rate and sleep keep that health record on servers in China. The operator's own policy says so. The person who lives with hypertension or diabetes has no means in the app or the policy to learn which safeguard protects it.

Fix: Name the Art. 46 mechanism and the transfer impact assessment for EU users in the policy. Offer an EU storage region for health data or stop transferring it. Appoint an Art. 27 representative in the Union.

H1: Chinese speech-cloud library and endpoints bundled next to microphone permissions for a "real-time translation" feature

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

The manifest declares RECORD_AUDIO, CAPTURE_AUDIO_OUTPUT and FOREGROUND_SERVICE_MICROPHONE. The armeabi-v7a split holds libmsc.so, the standard file name of the iFlytek Mandarin Speech Cloud SDK. The dex strings hold three speech-cloud hostnames. An asset folder named MaxLingo sits in the package. The Google Play description names "real-time translation patches".

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.CAPTURE_AUDIO_OUTPUT"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE_MICROPHONE"/>
```

```
iss.openspeech.cn   openapi.openspeech.cn   dev.voicecloud.cn
lib/armeabi-v7a/libmsc.so   assets/MaxLingo/
```

The hostname openspeech.cn belongs to the speech services of ByteDance's Volcano Engine according to the findings file for this target. The owner of voicecloud.cn was not identified. The package therefore contains a native Chinese speech recognition library, strings for two or more Chinese speech-cloud endpoints and the permissions that capture microphone and playback audio, all in one shipped build. No consent management platform sits in front of any of it (see H3).

Whether audio is transmitted on every install, only while the translation feature is active or only after an in-app toggle is UNVERIFIED. The review made no traffic capture and no bytecode control-flow pass. If audio does leave the phone, it compounds C1. Whether the speech data qualifies under Art. 9 depends on whether the speech SDK performs speaker identification, which was not traced.

Impact: A person who talks to the app's translation feature may have the voices of everyone in the conversation sent to speech services in China. The people spoken to never installed the app and see no notice.

Fix: State in writing whether microphone audio leaves the phone for the translation feature and where it is processed. Offer on-device translation or a clear opt-in before the first recording.

H2: NotificationListenerService gives access to the notifications of every app on the phone, while the manifest holds no SMS permission

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B)

MyNotificationListenerService is declared with the BIND_NOTIFICATION_LISTENER_SERVICE permission. The Google Play description says the app "offers SMS core functionality". The 80 declared permissions contain no RECEIVE_SMS, READ_SMS or SEND_SMS. A receiver filters on android.provider.Telephony.SMS_RECEIVED but cannot receive that broadcast without the dangerous permission.

```
<service android:exported="false" android:label="@string/app_name"
    android:name="com.wakeup.howear.service.MyNotificationListenerService"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action
           android:name="android.service.notification.NotificationListenerService"/>
    </intent-filter>
</service>
```

Only the operating system can bind to the service. The capability remains: a notification listener reads sender, source app, preview text and time of every notification that arrives while the listener is enabled, from any app. The listener is the only mechanism in the build that can carry message content to a wearable. It is not limited to SMS.

The operator's policy discusses an "SMS Permission" as if the Android SMS permission model were in use and does not mention notification access. Whether the content is stored or transmitted is UNVERIFIED.

Impact: The people who write to a Wearfit Pro user, such as family members, partners and doctors, have their message previews pass through the app. The same holds for one-time passcodes from banks. None of the senders installed the app or saw a notice.

Fix: Limit the listener to the apps and categories that the wearable shows. State in the policy that notification content is neither stored nor passed to any SDK. Align the Google Play description with the real mechanism.

H3: Five SDK ContentProviders initialise at process start before any consent screen can run, and no consent management platform is present

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B)

The manifest declares ContentProviders for Google Mobile Ads, AppLovin, Firebase, Tramini (AnyThink/TopOn) and Huawei HMS with initOrder values between 100 and 500. Android runs ContentProviders during Application.onCreate, before any Activity. FirebaseInitProvider is directBootAware. A search of strings.xml and the manifest for OneTrust, Didomi, Usercentrics and IABTCF returned no match.

```
<provider android:authorities="com.wakeup.howear.mobileadsinitprovider"
   android:exported="false"
    android:initOrder="100"
       android:name="com.google.android.gms.ads.MobileAdsInitProvider"/>
<provider android:authorities="com.wakeup.howear.applovininitprovider"
   android:exported="false"
    android:initOrder="101" android:name="com.applovin.sdk.AppLovinInitProvider"/>
<provider android:authorities="com.wakeup.howear.firebaseinitprovider"
   android:directBootAware="true"
    android:exported="false" android:initOrder="100"
       android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.wakeup.howear.initprovider"
   android:exported="false"
    android:initOrder="100"
       android:name="com.tramini.plugin.api.TraminiContentProvider"/>
<provider android:authorities="com.wakeup.howear.aaidinitprovider"
   android:exported="false"
    android:initOrder="500" android:name="com.huawei.hms.aaid.InitProvider"/>
```

The class prefix identifies TraminiContentProvider as the com.anythink.sdk.tramini_sdk component, which is part of the AnyThink/TopOn ad mediation platform. The only consent-like string in the resources is applovin_agree_message: ”Please press \”Continue\” if you choose to start using our app”. It is a single acknowledgement and offers no choice per purpose.

Construction of an SDK object does not by itself prove data collection. What each provider collects before the first screen is UNVERIFIED. The finding is the architecture: the app has no mechanism that holds the five providers back until a consent decision exists.

Impact: Every user of an app with more than 10 million installs starts a process in which advertising and analytics SDKs are initialised before the user has seen a choice, including people who log blood pressure and blood sugar.

Fix: Disable the auto-init providers in the manifest and start each SDK from code after a granular consent decision. Add a certified consent management platform and test the gating against each provider.

M1: Pinned certificate for bjol.luxhub.top expired on 2025-09-18 and was still the only trust anchor in the August 2026 build

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B)

network_security_config.xml scopes a domain-config for bjol.luxhub.top with res/raw/dd.pem as the only trust anchor. The certificate has a validity ending on 2025-09-18. The build is versionCode 2026081417 and was updated on Google Play on 14 August 2026.

```
<domain-config>
    <domain includeSubdomains="true">bjol.luxhub.top</domain>
    <trust-anchors>
        <certificates src="@raw/dd" />
    </trust-anchors>
</domain-config>
```

```
subject=CN=bjol.luxhub.top
issuer=C=AT, O=ZeroSSL, CN=ZeroSSL ECC Domain Secure Site CA
notBefore=Jun 20 00:00:00 2025 GMT
notAfter=Sep 18 23:59:59 2025 GMT
```

The name bjol.luxhub.top follows no naming pattern of the operator’s iwhop.cn and iwhopodm.com estate. It may belong to a partner or vendor backend. That attribution is UNVERIFIED. Either the app no longer relies on the pin and falls back to another trust path, or connections to this domain fail validation and run through an unaudited code path. Which of the two applies was not determined.

Impact: A pinning rule that nobody maintains for eleven months gives users and reviewers a false picture of how well traffic is protected.

Fix: Rotate or remove the expired trust anchor and document which backend uses the domain. Add a build check that fails on expired pin material.

M2: Cleartext traffic permitted for all hosts and user-installed CA certificates trusted globally

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), rated MEDIUM by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from LOW/2.3 to MEDIUM because the setting applies to the whole application and removes the platform default for an app with more than 10 million installs whose own policy says it sends health and location data to .cn backends (C1). The base-config of network_security_config.xml sets cleartextTrafficPermitted=”true” and lists both system and user certificate sources as trust anchors. Hosts without a domain-config, which includes the .iwhop.cn and .iwhopodm.com backend estate, fall under that base-config.

```
<base-config cleartextTrafficPermitted="true">
    <trust-anchors>
        <certificates src="system" />
        <certificates src="user" />
    </trust-anchors>
</base-config>
```

With targetSdkVersion 35 Android denies cleartext by default. The app opts back in for every host that has no own rule and also accepts certificates that a user or an administrator installed. Together with the transfer of C1 this widens the exposure on a hostile network or on a device with an installed CA. Whether any API traffic travels in plaintext is UNVERIFIED because no traffic was captured.

Impact: People who track their health on public Wi-Fi depend on a transport setting that the app has told Android to relax for the whole application.

Fix: Remove cleartextTrafficPermitted from the base-config, drop the user trust anchor and define per-domain rules that permit HTTPS only for the first-party hosts.

M3: Device identifier bundle with IMEI, IMSI, SIM serial, hardware serial and OAID, plus the installed apps inventory

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B)

The operator's policy lists IMEI, IMSI, Android ID, Android advertising ID, OAID, hardware serial number and SIM card identifier six times. The manifest declares QUERY_ALL_PACKAGES. The Google Play Data safety panel lists installed apps under App activity as collected.

```
...device identification information (system basic information, device name, device
identifier, IMEI, Mac address, system log, system usage information, device usage
information, IMSI, AndroidID, Android advertising ID, OAID, hardware serial number,
SIM card identifier, etc.)...
```

```
<uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
```

IMEI, IMSI and the SIM identifier have no technical link to Bluetooth Low Energy pairing or to fitness tracking. OAID is a Chinese advertising identifier designed to work without Google Play Services. The set supports a device fingerprint that survives a reset of the advertising ID. Whether the app reads each identifier at runtime is UNVERIFIED.

Impact: A wearer who resets the advertising ID to stay unlinked can still be recognised through the other identifiers, and the list of installed apps shows which health, dating or banking apps sit on the phone.

Fix: Remove identifiers that pairing and fitness functions do not need. Justify QUERY_ALL_PACKAGES to Google Play or replace it with targeted queries.

M4: Policy describes third-party applications that can read sensor, sleep, exercise and location data from the paired wearable

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 (CVSS-B)

Section 1.3.2 of the operator's policy says that after pairing, third-party applications that interact with the wearable through Wearfit Pro can obtain a device identifier, device name, hardware information and status. According to the policy and "your explicit authorization" they can access sensor data, sleep status, exercise type, wearing status, logs, location and device information. They can also send messages and notifications to the wearable.

```
"After Weike wearable devices are successfully paired, third-party applications that
interact with the paired Weike wearable devices through 'Wearfit Pro' can obtain the
random identifier of your device (pairing can be reset and unique to each
   application),
device name, device hardware information and status (charging or in use) and other
   data.
Third-party applications can also send messages or notifications to your paired
   wearable
devices. According to your explicit authorization, these third-party applications
   can
access the device's sensor data, sleep status, exercise type (walking, running),
   wearing
status data, log information, location information, device information"
```

The policy names no third-party application and no controller for any of them. The authorisation step in the app was not observed because the onboarding screens render from the React Native bundle, which this review scanned only for plain-text domains. The roles of these third parties as joint controllers, processors or independent controllers under Art. 26 and 28 are undetermined.

Impact: A person who pairs a wearable agrees to an authorisation whose recipients are not named, so sleep, movement and location data can reach applications the person has never heard of.

Fix: Name every third-party application class and controller that can read wearable data, state the roles under Art. 26 and 28 and show the authorisation screen with its purposes.

L1: PEGI 3 rating, an under-14 parental-consent statement and a date-of-birth field, with no age gate located

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B)

Google Play lists the app as PEGI 3. The policy defines children as individuals under 14 and says they may not create accounts without a guardian's consent. The account profile includes a date of birth. strings.xml holds no age gate or parental consent string.

```
The children referred to in this statement are individuals under 14 years of age.
Without the consent of parents or guardians, children may not create their own user
accounts.
```

The negative result is not treated as proof of absence. The account and onboarding screens are built in React Native, so their text most likely sits in assets/index.android.bundle, which was not parsed for interface strings. The date-of-birth field is real because the policy describes it. Whether an enforced check follows it is UNVERIFIED.

The policy also describes a Family Space feature that shares health data among family and friends. A parent registering a child's watch or a minor seeing a relative's health data are paths that the policy does not close.

Impact: A child with a watch from a parent may be able to use an app that reads notifications, logs health values and shares them in a family space, behind a rating that says suitable for everyone.

Fix: Align the content rating with the features, add an age screen with a parental consent route and document how Family Space limits what minors can see.

Impact Analysis

Wearfit Pro has more than 10 million installs. People who use it record sleep, heart rate, blood pressure and blood sugar, receive their phone notifications on a wearable, talk to a translation feature and pair the device to other applications. The operator says that the resulting data is stored in China and names no transfer safeguard.

Four groups carry the consequences. Wearers with hypertension or diabetes keep a health record in a store that sits outside the Union without a named mechanism (C1). People who write to a wearer, and people spoken to through the translation feature, are processed without a notice (H1, H2). Every user starts advertising and analytics SDKs before a consent choice (H3). Children can reach the app behind a rating of PEGI 3 (L1).

The harm demonstrated is a harm of declared architecture and of missing safeguards. Observed exposure on the wire is not claimed because no traffic was captured.

The Complete Chain

Step 1, install: a user finds an app rated PEGI 3 with more than 10 million downloads and a policy in English (L1).

Step 2, first launch: five SDK ContentProviders construct during process start, before any consent screen can run (H3).

Step 3, pairing and features: the user pairs a wearable, grants notification access and starts logging blood pressure, blood sugar and sleep. Third-party applications can read wearable data after pairing (H2, M4).

Step 4, storage: the policy states that the data is stored on servers in China, and the build contains .cn backend hostnames with health and gps in their names (C1).

Step 5, the user tries to find the safeguard: the policy names no Standard Contractual Clauses, no transfer impact assessment and no EU representative (C1).

Operator Cluster and Shared SDK Choices

The developer account Wakeup publishes at least five apps on Google Play: Wearfit Pro, WearFit2.0, Wearfit, Tband and OCECCA. The findings file for this target records that count from the Google Play developer page. The operator's own policy describes a platform in which third-party applications access wearable data (M4).

A comparison with WearFit2.0 (package com.wakeup.wearfit2) found the same Tramini ContentProvider pattern and a NotificationListenerService in both apps. The native library sets and the Bluetooth stack did not match, so a binary level cluster claim between the two is NOT CONFIRMED. The shared elements are one publisher and one SDK integration choice. WearFit2.0 has its own report under REF WEARFIT20-2026-R1.

The findings file for HryFine (REF HRYFINE-2026-R1) records that Wearfit Pro contains the Bluetrum abpartool and fota classes at class level. A hostname lenovo-api.idours.cn in the dex strings sits in a different domain family from iwhop.cn and may point to a Lenovo-branded product line. That relationship is UNVERIFIED and is recorded as an open lead.

Data Protection: Article by Article

Article 5(1)(a), (b) and (c), transparency, purpose limitation and minimisation: engaged by C1, M3 and M4.

Articles 6(1) and 7(1), lawfulness and conditions for consent: engaged by H2 and H3. Processing by SDKs that construct at process start precedes any consent decision, and ePrivacy Art. 5(3) applies to access to the terminal equipment.

Article 8, a child's consent: engaged by L1.

Article 9, special categories: engaged by C1. Sleep, heart rate, blood pressure and blood sugar are health data. Voice data in H1 is engaged only if speaker identification is used, which was not traced.

Article 13(1)(e), recipients: engaged by M4.

Article 25, data protection by design and by default: engaged by H1, H2, M2 and M3.

Articles 26 and 28, joint controllers and processors: engaged by M4. The roles are undetermined.

Article 27, EU representative: engaged. None found.

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

Articles 44 and 46, transfers: engaged by C1 and, if audio leaves the phone, by H1.

Regulatory & Legal Landscape

Shenzhen Weike Technology Co., Ltd. offers the app to users in the Union, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State can receive a complaint. The Austrian Datenschutzbehörde and the EDPS were in copy of the first notice.

Infringements of Art. 5, 6, 7 and 9 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 8, 25, 26, 27, 28 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82.

The privacy contact common@iwhop.com is the only privacy channel found. The address hr01@iwhop.com rejected the first notice with a permanent failure.

Indicators of Compromise & Reproducible Evidence

Every point is reproducible from the public build and from the public policy page read by plain HTTP GET.

```
Package            com.wakeup.howear
Version            hw_5.6.09 (versionCode 2026081417), Play update 14 Aug 2026
Bundle size        324 MB XAPK (base.apk 200 MB, armeabi-v7a split 113 MB, 21
   language splits)
XAPK SHA-256       0fa1272519b23ec68dec283729b30224d3f73176357c0aac4c0381f5fe12371b
base.apk SHA-256   5c2067a107ea5c36dc928665acc605adcdb369369dddad7313e38f9071c06e62
native split       535870b9210b6d311fa768a85bd51d5bd04e8faaf9460965c82b4d183e7e8ffe
minSdk / target    26 / 35
Permissions        80
Obtained from      APKPure mirror, matched on package name, version, version code
   and
                   permission count against the mirror listing before download
```

```
api-cluster.iwhop.cn  gateway.iwhop.cn  howear.iwhop.cn  health-monitor.iwhop.cn
   health-pro.iwhop.cn
health-news.iwhop.cn  gps.iwhop.cn  city-checkin.iwhop.cn  hkcos-material.iwhop.cn
   mall.iwhop.cn
medal.iwhop.cn  micro-life.iwhop.cn  iss.openspeech.cn  openapi.openspeech.cn
   dev.voicecloud.cn
bjol.luxhub.top  lenovo-api.idours.cn  common@iwhop.com
res/raw/dd.pem  res/xml/network_security_config.xml  lib/armeabi-v7a/libmsc.so
   assets/MaxLingo/
```

```
https://h5.iwhop.com/login/privacy_policy/privacy_policy_en.html  (sections 1.2.3,
   1.2.5, 1.3.2, 3, 5)
```

Disclosure Timeline & Outcome

2026-08-22 First notice, REF WEARFITPRO-2026-R1, sent at 14:19 UTC to common@iwhop.com, chenxia@iwhop.com, br@iwhop.com and hr01@iwhop.com with the Austrian DSB and the EDPS in copy. hr01@iwhop.com rejected the message at 14:19 UTC with the permanent failure 554 and was removed from later correspondence.

2026-09-12 First follow-up to the three working addresses, 21 days after the notice, restating C1, H1 and H3 and asking three written questions with a response date of 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com, 34 days before publication, with the three questions unchanged and the embargo stated as 20 November 2026 independent of any reply.

2026-11-14 No reply of any kind. None of the three addresses bounced. A search of the mailbox for inbound mail from the operator’s domain returned nothing.

2026-11-20 Publication date as stated in the second follow-up and equal to 90 days from the notice of 22 August 2026.

What Was Done Well

allowBackup is set to false, so app data is not part of Android’s automatic cloud backup. A detailed privacy policy exists, is linked from the Google Play listing, names the responsible entity with a physical address and states retention periods per data category. The policy names two integrated SDKs (Umeng+ and JPush) with a stated purpose. The operator discloses the storage location in the People’s Republic of China in plain words instead of using vague wording about partners worldwide.

Residual Risk & Recommendations

Open at the date of publication: all nine findings. The operator has not replied, and the build analysed is hw_5.6.09 of 14 August 2026. A final APK diff before 20 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, name the Art. 46 safeguard and the transfer impact assessment, offer an EU storage region for health data and appoint an Art. 27 representative (C1). Second, state whether microphone audio leaves the phone and where it is processed (H1). Third, hold every advertising and analytics SDK behind a granular consent decision (H3). Fourth, narrow the notification listener and correct the Google Play description (H2). Fifth, remove the global cleartext permission and the user trust anchor and fix the expired pin (M1, M2). Sixth, cut the identifier set and name the third-party applications that can read wearable data (M3, M4). Seventh, add an age gate (L1).

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 RFI-IRFOS research focus institute · ZVR 1015608684 · GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. CVSS-B is the CVSS v4.0 base score. REF WEARFITPRO-2026-R1.