Security & Privacy Disclosure, Final Report

WearFit2.0 for Android (com.wakeup.wearfit2)

No consent tooling, a global cleartext override and ECG and blood pressure data stored in China, in an app rated PEGI 3 with more than 5 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. (WearFit2.0, developer account Wakeup)
Versions Audited	zh_5.2.5 / versionCode 2024070215 (mirror build, Google Play listing dated 2024-05-08, analysed 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	11: 2 High, 4 Medium, 5 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`f34e9535b15d3e8289adcf26aafd90fa15f2ef59f685044046f2d088bb4ea241`

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: No consent management code anywhere in the build, a ContentProvider that initialises at process start, and a stack of at least eight tracking and advertising SDKs . . . 7

5.2 C2: Global cleartext traffic override without pinning on an app that logs ECG, blood glucose, blood pressure, contacts and SMS content . . . 8

5.3 C3: Operator states that health data and a device identifier bundle with IMSI and IMEI are stored in the People's Republic of China, with no transfer safeguard named . . . 9

5.4 H1: Circle feature lets one named user view the health data of another named person . . . 10

5.5 H2: ECG and other clinical-type health measurements on an app rated PEGI 3 with no age gate located . . . 11

5.6 H3: ByteDance Zeus plugin loading framework with a live-streaming plugin and an embedded signing certificate . . . 12

5.7 H4: Chinese SDK cluster (AMap, Jiguang and JPush, Umeng, Baidu, Tencent, ByteDance and Kuaishou) with literal endpoints, corroborating C3 . . . 13

5.8 M1: Five third-party API keys and application identifiers hardcoded in the manifest 14

5.9 M2: allowBackup is true on an app that stores health measurements and contacts 14

5.10 M3: BLE connection service and firmware update service exported without a protecting permission . . . 15

5.11 M4: One APK carries three brand names, and the Polish locale shows a different app name . . . 15

6 Impact Analysis 16

7 The Complete Chain 16

8 Operator Cluster and Shared SDK Choices 17

9 Data Protection: Article by Article 17

10 Platform Accountability & DSA 18

11 Regulatory & Legal Landscape 18

12 Indicators of Compromise & Reproducible Evidence 18

13 Disclosure Timeline & Outcome 19

14 What Was Done Well 19

15 Residual Risk & Recommendations 20

Executive Summary

WearFit2.0 is the Android companion app of Bluetooth smartwatches and bracelets, published on Google Play by the developer account Wakeup with more than 5 million downloads and a PEGI 3 rating. The operator is Shenzhen Weike Technology Co., Ltd. in Shenzhen. The listing promises monitoring of mental health, heart rate, blood pressure and blood tests, and the app contains an ECG result screen.

The most serious finding is written by the operator itself. Its English privacy policy says that the user's data "will be stored in the territory of the People's Republic of China", calls sleep, heart rate, blood pressure and blood sugar "sensitive personal information" and lists IMEI and IMSI among the collected identifiers. Neither the policy nor the build names Standard Contractual Clauses, a transfer impact assessment or an EU representative (C3).

The build contains no consent management code of any kind, while at least eight tracking and advertising SDKs are configured and a ContentProvider starts at process launch (C1). The network security configuration permits plaintext for the whole app, although the Google Play panel says that data is encrypted in transit (C2). A Circle feature shows the health values of one named person to another (H1). Further findings cover the ECG and PEGI 3 mismatch (H2), a ByteDance dynamic plugin framework (H3), the Chinese SDK cluster (H4), hardcoded keys (M1), allowBackup (M2), two exported services (M3) and three brand names in one APK (M4).

The notice went to the only developer contact found, a Gmail address. A follow-up with three written questions and a second reminder followed. As of 14 November 2026 no reply, acknowledgment or bounce has arrived. The publication date of 20 November 2026 stands independent of any reply.

Scope: Root level code analysis of the mirror build zh_5.2.5 (versionCode 2024070215): decoded manifest and resources, strings extraction across five dex files, native library inventory, and the operator's public privacy policy. The Google Play listing showed an update date of 8 May 2024 while the version code of the analysed file corresponds to 2 July 2024, and package name, developer name and icon match across both sources. 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	MEDIUM	No consent management code anywhere in the build, a ContentProvider that initialises at process start, and a stack of at least eight tracking and advertising SDKs
C2	HIGH	Global cleartext traffic override without pinning on an app that logs ECG, blood glucose, blood pressure, contacts and SMS content
C3	HIGH	Operator states that health data and a device identifier bundle with IMSI and IMEI are stored in the People's Republic of China, with no transfer safeguard named
H1	MEDIUM	Circle feature lets one named user view the health data of another named person
H2	LOW	ECG and other clinical-type health measurements on an app rated PEGI 3 with no age gate located
H3	MEDIUM	ByteDance Zeus plugin loading framework with a live-streaming plugin and an embedded signing certificate
H4	MEDIUM	Chinese SDK cluster (AMap, Jiguang and JPush, Umeng, Baidu, Tencent, ByteDance and Kuaishou) with literal endpoints, corroborating C3
M1	LOW	Five third-party API keys and application identifiers hardcoded in the manifest
M2	LOW	allowBackup is true on an app that stores health measurements and contacts
M3	LOW	BLE connection service and firmware update service exported without a protecting permission
M4	LOW	One APK carries three brand names, and the Polish locale shows a different app name

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	MEDIUM	No reply. Reassessed down because network activity of each SDK at process start is UNVERIFIED.
C2	CRITICAL	HIGH	No reply. Cleartext configuration as recorded. Plaintext use on the wire is UNVERIFIED.
C3	CRITICAL	HIGH	No reply. Policy wording as recorded. The consent step in the app was not observed.
H1	HIGH	MEDIUM	No reply. Reassessed down because the second person's consent step is UNVERIFIED.
H2	HIGH	LOW	No reply. Reassessed down because age gate enforcement is UNVERIFIED.
H3	HIGH	MEDIUM	No reply. Reassessed down because activation of the plugin is UNVERIFIED.
H4	HIGH	MEDIUM	No reply. Reassessed down because the fields sent to each host are UNVERIFIED.
M1	MEDIUM	LOW	No reply. Key restrictions are not testable without third-party tests.
M2	MEDIUM	LOW	No reply. Backup content is UNVERIFIED.
M3	MEDIUM	LOW	No reply. Behaviour of the exported services is UNVERIFIED.
M4	MEDIUM	LOW	No reply.

Subject & Operator Analysis

WearFit2.0 is the Android companion app of Bluetooth Low Energy smartwatches and bracelets, published on Google Play under the package com.wakeup.wearfit2 by the developer account Wakeup. The Google Play listing shows more than 5 million downloads, a rating of 2.3 from 58,900 reviews, PEGI 3 and the category Health & Fitness. The listing markets the app with the words ”Mental health, heart rate, blood pressure measurement, blood tests, statistical exercise step, sleep time”.

The Google Play developer entry and the privacy policy name the operator as Shenzhen Weike Technology Co., Ltd., with its address at Room 4208, Tower A, Hongrongyuan North Station Center, Minzhi Subdistrict, Longhua District, Shenzhen, Guangdong, China 518000. The developer contact is the Gmail address developer.wakeup@gmail.com and a Hong Kong telephone number. The same operator publishes Wearfit Pro (REF WEARFITPRO-2026-R1).

No EU establishment and no Art. 27 representative appear in the build, the Google Play listing or the privacy policy at http://h5.iwhop.com/wearfit-2/privacy_policy_en.html, which is served over plain HTTP. The policy mentions a personal information protection department and names no person or direct channel.

Architecture & Data Flow

WearFit2.0 is a native Android and Java app with five dex files, minSdkVersion 23 and targetSdkVersion 33. The firmware update path uses the Nordic Semiconductor DFU protocol. The native libraries cover AMap, JPush core, Pangle, Umeng, ByteDance Zeus and a WGS84 to GCJ02 coordinate conversion, which is a mapping compliance routine specific to China.

The SDK stack is almost entirely operated from mainland China (see H4). A Circle module lets connected accounts view each other’s health values (H1). Network access is governed by a base-config that permits cleartext for the whole app (C2).

Which fields leave the phone toward which host is UNVERIFIED. The review decoded the manifest and resources and extracted the dex string pool without a bytecode control-flow pass and without traffic capture.

Findings

C1: No consent management code anywhere in the build, a ContentProvider that initialises at process start, and a stack of at least eight tracking and advertising SDKs

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)

A search across all five dex files for Google UMP, IAB TCF, OneTrust, Didomi and Usercentrics signatures returned no match. The dex files carry JPush and Jiguang (858 class hits), AMap (645), Umeng (244), Kuaishou (1,612), ByteDance Pangle (129), Tencent (95) and Baidu Mobile Ads. The manifest tells the Baidu SDK to collect GPS, cell tower and WiFi location for advertising. TraminiContentProvider (AnyThink/TopOn) is declared with initOrder 100.

```
ConsentInformation / ConsentForm (Google UMP) : 0
IABTCF_* (IAB TCF strings)                    : 0
OneTrust / Didomi / Usercentrics              : 0
```

```
<provider android:authorities="com.wakeup.wearfit2.initprovider"
   android:exported="false"
          android:initOrder="100"
             android:name="com.tramini.plugin.api.TraminiContentProvider"/>
BaiduMobAd_STAT_ID="4f986d59aa"  BaiduMobAd_GPS_LOCATION="true"
BaiduMobAd_CELL_LOCATION="true"  BaiduMobAd_WIFI_LOCATION="true"
```

Android runs ContentProviders during Application.onCreate, before any Activity can render, so no consent screen can come first. With no consent tool in the build, no code path exists that asks for a decision before the SDKs act. Whether the advertising and analytics SDKs send network requests at process start, as opposed to constructing their objects, is UNVERIFIED because no bytecode control-flow pass and no traffic capture was made.

The Play listing shows no billing permission, so the app appears to rely on advertising. The SDK inventory is almost entirely operated from mainland China. Firebase, Audience Network, AppLovin, Vungle, Mintegral, InMobi and Unity Ads returned no hit in a targeted search.

Impact: Users who track blood pressure, ECG and sleep with the app, many of them on a phone shared with family, start a process that holds eight tracking and advertising SDKs before anyone asks them for a choice.

Fix: Add a consent management platform. Start every advertising and analytics SDK from code only after a granular consent decision and disable the auto-init ContentProvider until then. Turn off GPS, cell and WiFi location collection in the Baidu advertising configuration.

C2: Global cleartext traffic override without pinning on an app that logs ECG, blood glucose, blood pressure, contacts and SMS content

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), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from LOW/2.3 to HIGH because the setting applies to the whole application and removes the platform default for an app with more than 5 million installs that processes Art. 9 health data including ECG and blood glucose, and the Play Data safety label contradicts it. res/xml/network_security_config.xml sets cleartextTrafficPermitted="true" in the base-config and the application element sets android:usesCleartextTraffic="true". There is no pin-set and no per-domain rule anywhere in res/xml. The Google Play Data safety panel says the data is encrypted in transit.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

With targetSdkVersion 33 Android denies cleartext by default. The app opts back in twice for the whole application. The configuration permits plaintext for any endpoint, present or future, without a code change. Which endpoints use plain HTTP today is UNVERIFIED because no traffic was captured. The operator's privacy policy is itself served over plain HTTP.

The app processes ECG results, blood glucose, blood pressure, sleep, contacts, call logs and SMS content according to its activity inventory and its policy (see H2).

Impact: A person who tracks an ECG, blood pressure or blood glucose with this app relies on a transport setting that the app has told Android to run in plaintext, while the Google Play panel tells that person the data is encrypted in transit.

Fix: Remove cleartextTrafficPermitted and usesCleartextTraffic, define per-domain rules that permit HTTPS only and pin the first-party hosts. Correct the Data safety declaration if any endpoint stays on HTTP.

C3: Operator states that health data and a device identifier bundle with IMSI and IMEI are stored 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)

The operator's English privacy policy says twice that the data "will be stored in the territory of the People's Republic of China". Section 5 repeats that the information "will be transmitted and stored to servers in the People's Republic of China". The policy calls sleep, heart rate, blood pressure and blood sugar "sensitive personal information" and lists IMEI, IMSI, Android ID, advertising ID, OAID and hardware serial number six times. It names no Standard Contractual Clauses, no transfer impact assessment and no other Art. 46 safeguard.

```
"Your Wearfit2.0 information contains sensitive personal information, and we
will upload it to the Weike server only after you express your consent in the
application, and your above data will be stored in the territory of the
People's Republic of China."

(Section 5) "The above information will be transmitted and stored to servers
in the People's Republic of China."
```

```
"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
identification, etc."
```

The policy says that upload happens after the user consents in the application. The consent step in the app was not observed. The storage location is stated without qualification either way. The policy also quotes two of its SDKs collecting IMEI, IMSI, MAC and OAID: the AutoNavi positioning SDK and the Jiguang push service.

IMSI and IMEI have no technical link to step counting, heart rate or sleep. 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. The endpoint evidence in H4 corroborates the policy statement.

Impact: People who track an ECG, blood pressure, blood sugar or sleep with this app keep that record on servers in China. The operator's own policy says so. The person has no means in the app or the policy to learn which safeguard protects it.

Fix: Name the Art. 46 mechanism and publish the transfer impact assessment for EU users. Offer an EU storage region for health data or stop the transfer. Remove IMSI and IMEI collection. Appoint an Art. 27 representative.

H1: Circle feature lets one named user view the health data of another named person

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

The app ships a social module (packages ui.quanzi and ui.Circle) built around QR code friend adding. Activities such as GroupMemberHealthDataDetailActivity and per-metric screens show step, heart rate, blood oxygen, blood pressure, body temperature and sleep data of a connected person.

```
com.wakeup.wearfit2.ui.quanzi.scan.ScanActivity
com.wakeup.wearfit2.ui.quanzi.activity.VerificationActivity
com.wakeup.wearfit2.ui.Circle.HealthDataActivity
com.wakeup.wearfit2.ui.Circle.HealthDataDetailActivity
com.wakeup.wearfit2.ui.Circle.GroupMemberHealthDataDetailActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.StepDataActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.HeartRateDataActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.BloodOxygenDataActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.BloodPressureDataActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.BodyTempDataActivity
com.wakeup.wearfit2.ui.quanzi.activity.data.SleepDataActivity
```

The class inventory shows a designed feature in which an account holder can see health values of a second identifiable person. The consent step that the second person sees before this becomes visible was not observed and is UNVERIFIED. Whether the shared data also reaches the operator's backend is UNVERIFIED. Sharing Art. 9 data of a second person requires its own condition under Art. 9(2) and its own basis under Art. 6(1) for that person, and information to that person under Art. 13 and 14.

Impact: A relative, partner or friend who connects through the Circle can see another person's heart rate, blood pressure and sleep. For an older parent or a partner this is an intimate view into daily health, and the app does not show what the second person was told.

Fix: Show the second person a specific consent screen before any metric becomes visible, let them withdraw per metric and document the Art. 9(2) condition.

H2: ECG and other clinical-type health measurements on an app rated PEGI 3 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)

The manifest declares screens for heart rate, blood oxygen, blood pressure, ECG (EcgMeasureResultActivity), fatigue, sleep and weekly health reports. Google Play lists the app as PEGI 3 and Everyone and markets ”mental health, heart rate, blood pressure measurement, blood tests”. No date-of-birth field, age screen or parental gate was found in the resources.

```
HeartRateFragmentActivity  HeartRateDetActivity  OxygenActivity
   OxygenMeasureResultActivity
BloodpressureFragmentActivity  BloodpressureMeasureResultActivity
EcgMeasureResultActivity  FatigueMeasureResultActivity  SleepActivity
HealthWeeklyActivity  HealthWeeklyHrActivity  HealthWeekly10Activity
```

```
"we need to collect your sleep, heart rate, blood pressure, blood sugar, [body
   temperature], etc.
Health data is sensitive personal information."
"If you are a minor, your guardian is required to agree to your use of this
   application"
```

The minors sentence is advice and not a technical control. The feature set (ECG, blood pressure, blood sugar, mental health framing) points to adults managing their own health. Whether an age check sits behind account creation is UNVERIFIED. No data protection impact assessment is published.

Impact: A child who receives a watch from a parent can use an app rated suitable for everyone that records ECG and blood pressure, and the policy asks only for a guardian’s agreement.

Fix: Align the content rating with the features, add an age screen with a parental consent route, and document and publish a data protection impact assessment for the health measurements.

H3: ByteDance Zeus plugin loading framework with a live-streaming plugin and an embedded signing certificate

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

AndroidManifest.xml carries Zeus plugin metadata for Pangle, a Pangle extension and a live-streaming plugin (com.byted.live.lite) with an internal path plugins/zeusliveplugin.apk and a signature. libzeus_direct_dex.so is present and a Douyin authorisation proxy activity is exported.

```
<meta-data android:name="ZEUS_PLUGIN_PANGLE" android:value="{apiVersionCode:5709,
   packageName:com.byted.pangle.m, ...}"/>
<meta-data android:name="ZEUS_PLUGIN_LIVE" android:value="{apiVersionCode:2112,
   packageName:com.byted.live.lite,
   minPluginVersion:211200, maxPluginVersion:211999, isSupportLibIsolate:true,
   internalPath:'plugins/zeusliveplugin.apk', internalVersionCode:5,
      signature:'MIIDSTCCAjGgAwIBAgIEaLy5tzANBgkqhkiG9w0BAQsF...'}"/>
<activity android:exported="true"
android:name="com.bytedance.android.openliveplugin.stub.activity.
    DouyinAuthorizeActivityProxy"/>
```

Zeus is a dynamic plugin loading framework. An app built with it can load additional native code after installation without a store update. The integration is wired up, as the Douyin proxy activity shows. Nothing in the Google Play description of a smartwatch app explains a live-streaming plugin, so it reads as inherited from a shared advertising SDK bundle. This is a capability finding. Whether the plugin was ever downloaded or activated for users of this app is UNVERIFIED.

Impact: Users of a health app have no way to know that a third party can extend the code running next to their health records after installation.

Fix: Remove the live-streaming plugin and the dynamic loading capability if the app does not need them, or document what they load, from where and under which integrity checks.

H4: Chinese SDK cluster (AMap, Jiguang and JPush, Umeng, Baidu, Tencent, ByteDance and Kuaishou) with literal endpoints, corroborating C3

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 dex string pool holds class references for AMap (645), Jiguang (461), JPush (397), Umeng (244), Kuaishou (1,612), ByteDance (129), Tencent (95) and Baidu (3), and literal request hosts at each operator, among them a named Alibaba Cloud storage bucket in Shenzhen.

```
apilocate.amap.com  abroad.apilocate.amap.com  adiu.amap.com  apiinit.amap.com
   restapi.amap.com
wap.amap.com  mpsapi.amap.com  ce3e75d5.jpush.cn  oss.iwhop.cn
shenzhen-file-bucket.oss-cn-shenzhen.aliyuncs.com  adash.man.aliyuncs.com
api.weixin.qq.com  open.weixin.qq.com  long.open.weixin.qq.com  cgi.connect.qq.com
apps.bytesfield.com  apps.oceanengine.com  i.snssdk.com  sf6-ttcdn-tos.pstatp.com
open.e.kuaishou.com  p1-lm.adkwai.com  static.yximgs.com
union.baidu.com  cpro.baidustatic.com
aaid.umeng.com  ai.login.umeng.com  ulogs.umeng.com  c.umsns.com  log.umsns.com
```

The AMap host abroad.apilocate.amap.com is a dedicated endpoint for locations outside China, so location queries of users in the Union can reach Alibaba's mapping backend. Personal data that reaches Alibaba, Tencent, ByteDance, Kuaishou, Baidu and Jiguang infrastructure engages Chapter V of the GDPR. A transfer impact assessment has to address Art. 7 of the PRC National Intelligence Law. No Art. 46 mechanism is named. Which fields reach which host is UNVERIFIED.

Impact: Location, device identifiers and usage data of EU users reach several Chinese technology companies, and the person using the app learns about only two of them from the policy.

Fix: Name every SDK vendor, its country and the Art. 46 safeguard in plain English in the policy, and document a transfer impact assessment.

M1: Five third-party API keys and application identifiers hardcoded in the manifest

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

The manifest carries keys for AMap, Google Maps, Umeng, Baidu Mobile Ads and JPush, and a Facebook application ID. No key was tested or used.

```
<meta-data android:name="com.amap.api.v2.apikey"
   android:value="fde45ba5371f01c25323af71c587507d"/>
<meta-data android:name="com.google.android.geo.API_KEY"
   android:value="AIzaSyDAajNhc31YDaICVsLhMKbW8XumXxlD5vU"/>
<meta-data android:name="UMENG_APPKEY" android:value="586480df1c5dd01e4700155d"/>
<meta-data android:name="BaiduMobAd_STAT_ID" android:value="4f986d59aa"/>
<meta-data android:name="JPUSH_APPKEY" android:value="d2241211099ec3f7e5dbe3bf"/>
facebook_app_id = 1333853393320181
```

The platforms document such keys as identifiers. The finding concerns quota and billing exposure and depends on the key restrictions that the operator configured, which cannot be tested without third-party tests. No Facebook Audience Network class was found, so the Facebook ID is either leftover template configuration or a login-only integration. Which of the two applies is UNVERIFIED.

Impact: The operator carries quota and billing risk, and users could lose map or push features if a quota is exhausted.

Fix: Restrict each key to the package name and signing certificate and remove identifiers that the app does not use.

M2: allowBackup is true on an app that stores health measurements and contacts

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4 (CVSS-B)

The application element sets allowBackup=”true”. The app stores health measurements, friend and group data and contacts synchronised for wearable push.

```
<application android:allowBackup="true" ... />
```

With targetSdkVersion 33 the adb backup route no longer exports private data of apps that target API level 31 or higher, so the relevant routes are the automatic cloud backup and device-to-device transfer. What the backup contains is UNVERIFIED.

Impact: Health measurements and contacts that the app stores can travel into device backups.

Fix: Set allowBackup to false or define backup rules that exclude health and contact data.

M3: BLE connection service and firmware update service exported without a protecting permission

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)

WearfitService and DfuService are exported with no android:permission attribute.

```
<service android:enabled="true" android:exported="true"
   android:label="@string/app_name"
         android:name="com.wakeup.wearfit2.ble.WearfitService"/>
<service android:exported="true"
   android:name="com.wakeup.wearfit2.ui.duf.DfuService"/>
```

Any app on the device can start or bind to both services without holding a permission. What they do when invoked from outside could not be determined from this review and is UNVERIFIED. The notification listener AlertService is correctly not exported and carries the system permission.

Impact: Another app on the phone may be able to reach the component that talks to the wearable and the one that updates its firmware.

Fix: Set exported to false or protect both services with a signature-level permission.

M4: One APK carries three brand names, and the Polish locale shows a different app name

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)

The resource table labels the app ”Somatik Fit” for the Polish locale and ”WearFit2.0” for the other locales. The English privacy policy calls the operator ”Microgram” in one passage and Shenzhen Weike Technology Co., Ltd. elsewhere. The Google Play developer field shows only ”Wakeup”.

```
application-label-pl:'Somatik Fit'       application-label-pl-PL:'Somatik Fit'
application-label (other locales, e.g. -en, -de, -zh, -ru, -ja): 'WearFit2.0'
```

The Chinese company name Weike translates as microgram, so the policy appears to render the operator’s own name literally. The brand strings WearFit2.0, Somatik Fit, Microgram, Weike and Wakeup all refer to one legal entity, one package and one signing key.

Impact: A Polish-speaking user who installs Somatik Fit cannot tell from the name that it is the same product and company as WearFit2.0 and Wakeup.

Fix: Present one product name and the controller’s full legal name consistently in the app, the store listing and the policy.

Impact Analysis

WearFit2.0 has more than 5 million installs. Its users record ECG results, blood pressure, blood oxygen, blood glucose and sleep, synchronise contacts and notifications with a wearable and can share health values with connected persons. The operator says that the data is stored in China and names no transfer safeguard.

Four groups carry the consequences. People with cardiac, blood pressure or metabolic conditions keep a health record in a store outside the Union without a named mechanism and in an app that permits plaintext transport (C2, C3). Relatives and friends in the Circle have their health values visible to others without a consent step that anyone observed (H1). Every user starts tracking and advertising SDKs before any choice (C1). Children can reach an ECG app behind a rating of PEGI 3 (H2).

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 with more than 5 million downloads, PEGI 3, a Data safety label that says data is encrypted in transit and a listing that promises blood pressure and mental health monitoring (C2, H2).

Step 2, first launch: a ContentProvider of AnyThink/TopOn starts with the process and no consent tool exists in the build for any of the eight SDKs (C1).

Step 3, use: the user pairs a wearable, records ECG, blood pressure and sleep and can add friends through a QR code so that they see the values (H1, H2).

Step 4, transmission and storage: the network security configuration permits plaintext for every host, literal Chinese endpoints sit in the dex files and the policy says that the data is stored in China (C2, C3, H4).

Step 5, the user tries to understand: the policy is served over plain HTTP, names no safeguard and refers to the operator under different names (C3, M4).

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 operator's corporate site iwhop.com markets WEARFIT OS, WEARFIT Cloud Services and a one stop hardware solution service. The privacy policy of WearFit2.0 and the policy of Wearfit Pro use near-identical wording about storage in the People's Republic of China.

Both apps declare the same TraminiContentProvider and both declare a NotificationListenerService component. The two apps differ in the Bluetooth stack. WearFit2.0 has no Bluetrum classes and no libabpartool.so and uses Nordic DFU, so a hardware level cluster claim with Wearfit Pro or HryFine is NOT CONFIRMED. The shared elements are one operator and one SDK integration choice.

Data Protection: Article by Article

Article 5(1)(a), (b) and (c) and Article 5(2), transparency, minimisation and accountability: engaged by C1, C3 and H1.

Articles 6(1) and 7(1), lawfulness and conditions for consent: engaged by C1 and H1. ePrivacy Art. 5(3) applies to access to the terminal equipment.

Article 8, a child's consent: engaged by H2.

Article 9, special categories: engaged by C3, H1 and H2. ECG, blood pressure, blood oxygen, blood glucose and sleep data are health data.

Articles 12(1), 13 and 14, information duties: engaged by H1 and M4.

Article 25, data protection by design and by default: engaged by C2, H3 and M2.

Article 27, EU representative: engaged. None found.

Article 32(1)(a) and (b), security of processing: engaged by C2, H3, M1, M2 and M3.

Article 35, impact assessment: engaged by C3, H2 and H4. None is published.

Articles 44 and 46, transfers: engaged by C3 and H4.

Platform Accountability & DSA

The Google Play Data safety panel of WearFit2.0 says that the app may share device or other IDs with third parties, may collect location and app info and performance and that data is encrypted in transit. The global cleartext configuration of C2 contradicts the last statement.

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about the Data safety declaration under the notice and action mechanism of Art. 16 of that Regulation. RFI-IRFOS records the contradiction here.

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, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 8, 25, 27, 32 and 35 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82.

The only contact channel for the operator is a personal Gmail address and a Hong Kong telephone number, so no corporate privacy or security contact exists for supervisory authorities or users.

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.wearfit2
Version            zh_5.2.5 (versionCode 2024070215)
APK size           61,228,988 bytes
APK SHA-256        f34e9535b15d3e8289adcf26aafd90fa15f2ef59f685044046f2d088bb4ea241
Signing cert
   90:3A:ED:B9:D9:AE:0D:5D:10:6C:41:34:BD:AF:21:89:4F:B5:CA:67:44:C8:1B:1F:67:8A:89:F6
    :90:19:52:66
Signing DN         CN=wakeup, OU=wakeup, O=wakeup, L=sz, ST=gd, C=81
minSdk / target    23 / 33
Obtained from      APKPure mirror, matched on package name, developer name and icon
   against the
                   Google Play listing
```

```
com.amap.api.v2.apikey        fde45ba5371f01c25323af71c587507d
com.google.android.geo.API_KEY  AIzaSyDAajNhc31YDaICVsLhMKbW8XumXxlD5vU
UMENG_APPKEY                  586480df1c5dd01e4700155d
BaiduMobAd_STAT_ID            4f986d59aa
JPUSH_APPKEY                  d2241211099ec3f7e5dbe3bf
facebook_app_id               1333853393320181
```

```
apilocate.amap.com  abroad.apilocate.amap.com  ce3e75d5.jpush.cn  oss.iwhop.cn
   api.weixin.qq.com
shenzhen-file-bucket.oss-cn-shenzhen.aliyuncs.com  apps.oceanengine.com
   open.e.kuaishou.com  union.baidu.com
developer.wakeup@gmail.com  http://h5.iwhop.com/wearfit-2/privacy_policy_en.html
```

```
res/xml/network_security_config.xml  AndroidManifest.xml  libzeus_direct_dex.so
   libpangleflipped.so  libjcore332.so  libJni_wgs2gcj.so
```

Disclosure Timeline & Outcome

2026-08-22 First notice, REF WEARFIT20-2026-R1, sent at 17:12 UTC to developer.wakeup@gmail.com with the Austrian DSB and the EDPS in copy.

2026-09-12 First follow-up to developer.wakeup@gmail.com, 21 days after the notice, restating the open findings 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, no automated acknowledgment and no bounce. A search of the mailbox for inbound mail from the operator’s address 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

A detailed privacy policy exists, is linked from the app, names the responsible entity with a physical address and names two integrated SDKs (AutoNavi and Jiguang) with a stated purpose. The notification listener AlertService is not exported and carries the system permission. The microphone use traces to conventional features. A second-pass check found AudioRecord and MediaRecorder references tied to the video capture audio track and the operator’s voice and call functions, and found no audio classification model or feature extraction code. The policy states concrete retention periods per data category.

Residual Risk & Recommendations

Open at the date of publication: all eleven findings. The operator has not replied. The build analysed is zh_5.2.5 (versionCode 2024070215). The Google Play listing showed an update date of 8 May 2024 on 22 August 2026 while the mirror file is dated 2 July 2024 by its version code, so the relation between the analysed file and the current Google Play release is not independently confirmed. 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 and appoint an Art. 27 representative (C3). Second, remove the global cleartext permission, pin the first-party hosts and correct the Data safety declaration (C2). Third, add a consent management platform and hold every SDK behind it (C1). Fourth, add a consent step for the second person in the Circle (H1). Fifth, add an age gate and a data protection impact assessment (H2). Sixth, remove or document the Zeus plugin loading (H3) and name every SDK vendor and its country (H4).

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 WEARFIT20-2026-R1.