Security & Privacy Disclosure, Final Report

FlagFit 2.0 for Android (com.yc.flagfit2)

Health profiles shown across accounts, a Chinese cloud stack for special category data and a 1024-bit signing key in a packed app, with no reply since the notice.

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

Target	Youchuangyi Health Technology (Shenzhen) Co., Ltd. (FlagFit 2.0), policy issued by Shenzhen Ultra Easy Technology Co., Ltd.
Versions Audited	1.10.2 / versionCode 102 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 7 Medium, 3 Low, 1 observation (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`328c9adad5da685984f7f47325107e22ecc278c64c0d42b5c69de401770037ae`

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 5

4 Architecture & Data Flow 6

5 Engagement Summary 6

6 Findings 7

6.1 C1: Special category health data of an app with 1 million installs sits behind a PRC cloud and SDK stack, with no transfer mechanism in the policy or the binary 7

6.2 C2: The app is signed with a self-signed 1024-bit RSA certificate issued to a personal name and valid until 2124 8

6.3 H1: Commercial anti-analysis packer around the whole application 9

6.4 H2: Relatives and friends feature shows a person's full health profile to another account, and the profiled person has no consent screen of their own in the description 10

6.5 H3: Three non-matching operator identities and no Article 27 representative . 11

6.6 H4: The policy admits collection of IMEI, IMSI, Mac address and GUID through Umeng and has not changed since July 2023 12

6.7 H5: Google, AMap and Umeng keys and an operator key in the manifest 13

6.8 H6: PEGI 3 rating, a policy clause on children and no age gate found in the resources 13

6.9 H7: The Data Safety label omits contacts, SMS, call log, camera and microphone although permissions and the policy name them 14

6.10 M1: Two parallel notification capture paths, a notification listener and a scoped accessibility service, with the destination of the content not shown 15

6.11 M2: Installed application inventory is read, confirmed in code and in the policy 16

7 Impact Analysis 16

8 The Complete Chain 17

9 Same-Developer Cluster and Chipset Fingerprint 17

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 18

12 Regulatory & Legal Landscape 19

13 Indicators of Compromise & Reproducible Evidence 20

14 Disclosure Timeline & Outcome 21

15 What Was Done Well 21

16 Residual Risk & Recommendations 22

Executive Summary

FlagFit 2.0 (package com.yc.flagfit2) is the companion app of the DB02 smart bracelet. It is published on Google Play as Youchuangyi Health Technology (Shenzhen) Co., Ltd., has more than 1 million installs and carries PEGI 3. Its privacy policy, issued in the name of Shenzhen Ultra Easy Technology Co., Ltd, lists a very broad special category data set: blood pressure, ECG, blood oxygen, body temperature, mood and stress scores and a female health function with menstrual cycle data. On 23 August 2026 RFI-IRFOS sent a notice with REF FLAGFIT20-2026-R1 to support@ute-tech.com.cn, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

The root level code analysis of version 1.10.2 shows hard-coded endpoints for Alibaba Cloud storage in Hangzhou, AMap, Umeng and Tencent connect services behind that data set, with no transfer mechanism in the policy or the binary (C1). The app is signed with a self-signed 1024-bit RSA certificate issued to a personal name and valid until 2124 (C2). The policy describes a relatives and friends feature that shows a person's health data to another account (H2). Three different operator names appear across the listing, the policy and the certificate and no Article 27 representative is named (H3). The policy admits collection of IMEI, IMSI and Mac address through Umeng in a text from July 2023 (H4). The Data Safety label leaves out contacts, SMS, call log and microphone (H7). The whole application is wrapped in a commercial packer that hides the code behind most of these questions (H1).

A reassessment by CVSS v4.0 band puts seven findings at Medium and three at Low, with one observation left unrated. The two findings disclosed as Critical move to Medium because the package shows the endpoints and the weak key and does not show a data flow or an abuse. FlagFit 2.0 shares the signing certificate and the code base with GloryFit (REF GLORYFIT-2026-R1) and does not share the Bluetrum chipset fingerprint of HryFine, Wearfit Pro and Fere Fit.

The operator did not reply to the notice of 23 August 2026, the follow-up of 12 September 2026 or the follow-up of 17 October 2026. No bounce was received. This report is published on the embargo date of 21 November 2026 and records the state of the correspondence on 21 November 2026.

Scope: Root level code analysis of the Google Play release 1.10.2 (versionCode 102, 54.8 MB). Work done: decoded manifest, resources, strings and network security configuration (apktool, no source decode), string extraction across the four unprotected classes*.dex files, the native library inventory, and the signing certificate read with apksigner and keytool. Five further dex payloads under assets/baiduprotect*.dex are encrypted and were not decoded. The Google Play listing, the Data Safety page and the operator privacy policy were read on 23 August 2026. The app was not installed, no account was created, no feature was exercised, no operator server was called and no traffic was captured. No bytecode control-flow pass and no dynamic instrumentation were done. Class-level behaviour that depends on the hidden code is marked as such.

ID	Severity	Title
C1	MEDIUM	Special category health data of an app with 1 million installs sits behind a PRC cloud and SDK stack, with no transfer mechanism in the policy or the binary
C2	MEDIUM	The app is signed with a self-signed 1024-bit RSA certificate issued to a personal name and valid until 2124
H1	INFO	Commercial anti-analysis packer around the whole application
H2	MEDIUM	Relatives and friends feature shows a person's full health profile to another account, and the profiled person has no consent screen of their own in the description
H3	MEDIUM	Three non-matching operator identities and no Article 27 representative
H4	MEDIUM	The policy admits collection of IMEI, IMSI, Mac address and GUID through Umeng and has not changed since July 2023
H5	LOW	Google, AMap and Umeng keys and an operator key in the manifest
H6	LOW	PEGI 3 rating, a policy clause on children and no age gate found in the resources
H7	MEDIUM	The Data Safety label omits contacts, SMS, call log, camera and microphone although permissions and the policy name them
M1	MEDIUM	Two parallel notification capture paths, a notification listener and a scoped accessibility service, with the destination of the content not shown
M2	LOW	Installed application inventory is read, confirmed in code and in the policy

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Routing of a user record to the Hangzhou storage not shown.
C2	CRITICAL	MEDIUM	No reply. Weak key read from the certificate. No forgery shown.
H1	HIGH	INFO	Not rated. Limit of the analysis.
H2	HIGH	MEDIUM	No reply. Rests on the operator policy text.
H3	HIGH	MEDIUM	No reply. Three identities, no representative.
H4	HIGH	MEDIUM	No reply. Policy text dated July 2023.
H5	HIGH	LOW	No reply. Restriction state not visible.
H6	HIGH	LOW	No reply. Age gate not found in resources.
H7	HIGH	MEDIUM	No reply. Label captured 23 August 2026.
M1	MEDIUM	MEDIUM	No reply. Destination of notification content not shown.
M2	MEDIUM	LOW	No reply. Transmission not shown.

Subject & Operator Analysis

FlagFit 2.0 is published as Youchuangyi Health Technology (Shenzhen) Co., Ltd. The privacy policy at ute-tech.com.cn names Shenzhen Ultra Easy Technology Co., Ltd, and the signing certificate names a personal name and the organisation Youchuang in Guilin, Guangxi (H3). The only contact is support@ute-tech.com.cn, which the policy text gives. No data protection officer, press contact, postal address or Article 27 representative was found.

The Google Play listing of FlagFit 2.0 names at least six sibling apps of the same developer account, GloryFit, GloryFitPro, Du Watch, iGloryfit, Glory Note and Glory View, and the original FlagFit. The manifest declares more than 60 activities and services under the internal package com.yc.pedometer and none under com.yc.flagfit2. The application ID is a thin rename over one shared code base. The GloryFit package com.yc.gloryfit carries the same com.yc prefix and the same signing certificate fingerprint, which is documented in the GloryFit report of this package.

A controller without an establishment in the Union is not covered by the one-stop-shop mechanism. The Austrian Datenschutzbehörde receives the notice in copy.

Architecture & Data Flow

FlagFit 2.0 is a native Android app with four unprotected classes*.dex files. The real business logic sits behind a stub Application class (com.sagittarius.v6.StubApplication) that loads five encrypted Baidu Protect dex payloads (H1). All 60 or more activities and services live under com.yc.pedometer.

The band side is built on the Realtek Realsil DFU stack. The manifest declares com.realsil.android.blehub.dfu.DfuService and com.realsil.sdk.dfu.DfuService, and libRtkAesJni.so exports Java_com_realsil_sdk_dfu_utils_AesJni_aes_1encrypt. Phone side features are blood pressure, heart rate, heart rate variability, temperature and physiological monitors, a relatives and friends feature (H2), a notification listener and an accessibility service for message push (M1). Network endpoints in the unprotected dex files point at Alibaba Cloud storage in Hangzhou, AMap, Umeng, QQ and WeChat (C1). The network security configuration has no global cleartext override. Its only cleartext exception is the placeholder host secure.example.com from an SDK template.

Engagement Summary

The notice REF FLAGFIT20-2026-R1 was sent on 23 August 2026 at 04:31 UTC from rfi.irfos@gmail.com to support@ute-tech.com.cn with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried two critical and seven high findings with evidence, a statement of what the app does well and three questions. It asked for a written response within 30 days. A follow-up of 12 September 2026 restated the findings and set a date of 26 September 2026 for the three questions. A second follow-up of 17 October 2026 came from security@rfi-irfos.com. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: Special category health data of an app with 1 million installs sits behind a PRC cloud and SDK stack, with no transfer mechanism in the policy or the binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 23 August 2026

The dex files of version 1.10.2 contain hard-coded endpoints of Alibaba Cloud Object Storage in Hangzhou, AutoNavi AMap, Umeng and the Tencent QQ and WeChat connect services. Two keys in the manifest tie the app to the AMap and Umeng accounts. The operator policy, last updated July 2023 and served against a build for API level 35, describes the same stack and the data categories its SDKs receive, among them device information, network status, location and Wi-Fi information for Amap, and Mac address and unique device identifiers for Umeng. The same policy states that device sync handles activity, sleep, heart rate, blood oxygen saturation, weight, body temperature, blood pressure, body fat, ECG, respiration rate, mood and stress information, and a female health function that records days of menstruation and body condition and mood during menstruation. The manifest declares monitor activities for blood pressure, heart rate, heart rate variability, physiological data and temperature, which shows that the features ship. No Standard Contractual Clauses and no transfer impact assessment is referred to in the policy or the binary. The routing of an individual EU user's record to the Hangzhou bucket was not shown. The packer of H1 hides the request-building code. The score assumes a low confidentiality impact for that reason.

```
http://oss.aliyuncs.com
http://oss-cn-hangzhou.aliyuncs.com     (Alibaba Cloud Object Storage, Hangzhou region
    )
https://apiinit.amap.com/v3/log/init     (AutoNavi AMap)
https://adiu.amap.com/ws/device/adius
https://alogsus.umeng.com               (Umeng)
https://openmobile.qq.com/oauth2.0/m_authorize     (Tencent QQ Connect)
https://open.weixin.qq.com/connect/sdk/qrconnect   (Tencent WeChat)

<meta-data android:name="com.amap.api.v2.apikey" android:value="
    a8772b9da7408d26825410d2c48e03df"/>
<meta-data android:name="UMENG_APPKEY" android:value="5969cb8945297d03c1000233"/>
```

Policy quotes as read on 23 August 2026 from https://www.ute-tech.com.cn/privacy-policy/myprivacypolicy_english.htm. Amap Maps, Amap Positioning: will collect your device information, network status, location information, Wi-Fi information. Umeng: Our products, Umeng integration+ SDK and Umeng+ SDK, are required to collect your device Mac address and unique device identification (IMEI/android ID/IDFA/OPENUDID/GUID, SIM card IMSI information) in order to provide statistical analysis services. Female health function: the number of days of menstruation duration, your body condition and mood during the menstruation.

Impact: The data classes at stake are blood pressure, ECG, blood oxygen, body temperature and the menstrual cycle of people who wear the band every day. A user is told about a list of Chinese cloud and analytics services and given no mechanism that protects the data when it leaves the Union.

Fix: Name each recipient with country and transfer mechanism, publish the transfer impact assessment and state which health data reaches the Hangzhou storage.

C2: The app is signed with a self-signed 1024-bit RSA certificate issued to a personal name and valid until 2124

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), disclosed as CRITICAL on 23 August 2026

apksigner and keytool show a self-signed certificate with a 1024-bit RSA key and the SHA1withRSA signature algorithm, valid from 8 January 2015 until 15 July 2124. Android's own keytool warns that both the signature algorithm and the 1024-bit key are a security risk and that they will be disabled in a future update. The owner is a personal name and a company name in Guilin, Guangxi. The country field reads CH, the ISO code of Switzerland, which does not fit the other fields. Whether this is a typing error or intended is not established and is not asserted. The report found no forged or tampered package and the weakness is one of cryptographic standard for the signing channel. An attacker would need to break a 1024-bit RSA key to sign an update the platform accepts, which explains the high attack complexity in the score. The identical certificate fingerprint appears in the GloryFit package of the same developer (see the GloryFit report of this package).

```
Owner:  CN=Huang Jianchao, OU=Youchuang, O=Youchuang, L=Guilin, ST=Guangxi, C=CH
Issuer: CN=Huang Jianchao, OU=Youchuang, O=Youchuang, L=Guilin, ST=Guangxi, C=CH   (
    self-signed)
Serial number: 54adf9d9
Valid from: 2015-01-08 until: 2124-07-15
SHA-256: F9:0C:BD:89:62:1B:70:E6:DE:E4:CA:CA:3B:C7:14:83:CC:F1:71:63:C6:E3
    :31:32:85:53:5C:CA:91:F4:31:08
Signature algorithm: SHA1withRSA
Subject public key: 1024-bit RSA
Chinese characters of the DN are given in transliteration
```

Impact: The certificate is the identity under which every update of a health app with 1 million installs is accepted. A key of this size and a personal name as owner are weak anchors for that trust, and nothing in the evidence shows that anyone has abused them.

Fix: Replace the signing key with a current key through Play App Signing, name the legal entity in the certificate and rotate with the Play key upgrade path.

H1: Commercial anti-analysis packer around the whole application

INFO, no CVSS v4.0 score assigned, observation, not rated, disclosed as HIGH on 23 August 2026

The declared Application class is com.sagittarius.v6.StubApplication, a stub that loads five further dex payloads of the Baidu Protect hardening product at runtime. The package carries assets/baiduprotect-sec.dex, baiduprotect1 to baiduprotect4 as .i.dex and .jar files and libbaiduprotect.so for three ABIs. The real Application.onCreate(), which decides whether the Umeng, AMap and analytics SDKs initialise before or after the in-app consent screen, is not readable in the decode and cannot be read without unpacking the payload. Every claim about the timing of consent, the code of the relatives and friends feature and the handling of SMS, contacts and call log is therefore marked unverified in this report. The packer is a legal design choice and exposes no data itself. The report records it as a limit of the analysis and as a point for a data protection impact assessment, and does not rate it.

```
<application android:name="com.sagittarius.v6.StubApplication" ...>

assets/baiduprotect-sec.dex
assets/baiduprotect1.i.dex   assets/baiduprotect1.jar
assets/baiduprotect2.i.dex   assets/baiduprotect2.jar
assets/baiduprotect3.i.dex   assets/baiduprotect3.jar
assets/baiduprotect4.i.dex   assets/baiduprotect4.jar
lib/arm64-v8a/libbaiduprotect.so   lib/armeabi-v7a/libbaiduprotect.so   lib/armeabi/
    libbaiduprotect.so
```

Impact: The people affected cannot be told by an outside reviewer what the application does at start-up, because the operator chose to hide it.

Fix: Provide an unpacked build or a code-level description to the supervisory authority on request, and cover the packer in the data protection impact assessment.

H2: Relatives and friends feature shows a person's full health profile to another account, and the profiled person has no consent screen of their own in the description

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026

The manifest declares com.yc.pedometer.FriendsActivity and com.yc.pedometer. ConnectHelp. The operator policy says: Relatives and friends information: You can choose to add other users as your relatives and friends through the relatives and friends functionality. After your relatives and friends are authorized, their data (such as activity, sleep, weight, heart rate, blood pressure, body temperature, body fat, blood oxygen, ECG data, etc.) will be used to show you. That is special category health data about a named third party that another account holder sees. The text describes an authorisation by the relative's own account. It does not describe a separate information step that tells the relative what is shown, to whom and for how long. The server-side data model, whether data is streamed live or cached and whether it is kept after unlinking, is hidden by the packer of H1. The feature and its data scope rest on the operator's own current policy text.

```
Relatives and friends information: You can choose to add other users as your relatives
     and friends through the relatives and friends functionality. After your relatives
     and friends are authorized, their data (such as activity, sleep, weight, heart
    rate, blood pressure, body temperature, body fat, blood oxygen, ECG data, etc.)
    will be used to show you.
```

Impact: A person who agrees to be a relative or friend in the app may share blood pressure, ECG and body temperature readings with someone else. The policy does not say what that person is told when they agree.

Fix: Show the profiled person what is shared, with whom and for how long at the moment of authorisation, allow withdrawal and state the retention after unlinking.

H3: Three non-matching operator identities and no Article 27 representative

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026

The Google Play developer name is Youchuangyi Health Technology (Shenzhen) Co., Ltd. The privacy policy at ute-tech.com.cn is issued in the name of Shenzhen Ultra Easy Technology Co., Ltd. The signing certificate names a personal name and the organisation Youchuang in Guilin, Guangxi. The only contact found is support@ute-tech.com.cn. No data protection officer, press contact or postal address is given in the policy text extracted. No Article 27 representative is named in the policy, the manifest or the resources, although Google Play distribution to Austria was confirmed. The English renderings may be one entity under different names, the domain ute-tech.com.cn reads as Ultra Easy Technology, and no company register was consulted.

Source	Identity given
Google Play developer listing	Youchuangyi Health Technology (Shenzhen) Co., Ltd.
Privacy policy (ute-tech.com.cn)	Shenzhen Ultra Easy Technology Co., Ltd.
APK signing certificate	CN=Huang Jianchao (personal name), OU and O = Youchuang, L=Guilin, ST=Guangxi, C=CH
Contact	support@ute-tech.com.cn

Impact: A person who wants to ask who holds their health data reads three names and finds one mailbox on a .cn domain.

Fix: Name one controller with a postal address, a data protection contact and an Article 27 representative in the Union.

H4: The policy admits collection of IMEI, IMSI, Mac address and GUID through Umeng and has not changed since July 2023

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026

Section 7 of the policy states that the Umeng integration+ SDK and the Umeng+ SDK are required to collect the device Mac address and unique device identification (IMEI, android ID, IDFA, OPENUDID, GUID and SIM card IMSI information). The text is dated July 2023 and is served in 2026 against a build for API level 35, a platform where IMEI and IMSI access has been restricted by the operating system since Android 10. Either the policy claims data the SDK can no longer get on current Android, which misinforms users, or a collection path exists that this decode cannot exclude. The packer of H1 prevents a check. The finding is the textual admission, unrevised for more than two years against an updated binary.

```
Our products, Umeng integration+ SDK and Umeng+ SDK, are required to collect your
    device Mac address and unique device identification (IMEI/android ID/IDFA/OPENUDID
    /GUID, SIM card IMSI information) in order to provide statistical analysis
    services.
Last updated: July 2023
```

Impact: The notice does not match current practice in either direction. A user cannot tell whether persistent identifiers leave the phone.

Fix: Review the policy against the current build, remove claims for data the app cannot get and state the identifiers that are collected.

H5: Google, AMap and Umeng keys and an operator key 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), disclosed as HIGH on 23 August 2026

The manifest of version 1.10.2 carries four keys as plain meta-data values. They can be read with apktool in under a minute. None of the four restriction states can be seen from the package, and the burden of showing the restriction lies with the operator under Art. 5(2). No request was made with any key.

```
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyCSgtyaBMNfU3Utjmgn5dLcLY72xnwGVVE"/>
<meta-data android:name="com.amap.api.v2.apikey" android:value="
    a8772b9da7408d26825410d2c48e03df"/>
<meta-data android:name="UMENG_APPKEY" android:value="5969cb8945297d03c1000233"/>
<meta-data android:name="YCAPPKEY" android:value="12b0cb43454d2cd2f8c0562de71d7157"/>
```

Impact: A key for maps and analytics lets a third party use quota of the operator, which affects availability and cost and not user data.

Fix: Restrict the Google key by package name and signing certificate, set quotas for the AMap and Umeng accounts and rotate the keys.

H6: PEGI 3 rating, a policy clause on children and no age gate found in the resources

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), disclosed as HIGH on 23 August 2026

Google Play lists PEGI 3. Section 6 of the policy says: Children cannot create their own user accounts without the consent of their parents or guardians, and the operator treats anyone under the age of 13 as a child. A search of the decoded resources for birthday, date_of_birth, age_gate, parental, under 13 and COPPA found no match in strings.xml. The registration strings cover phone, email, password and third-party OAuth with QQ, WeChat, Facebook and Twitter. Resource strings only show part of the picture, since an age gate in hidden code or on the server would not appear.

```
Google Play content rating: PEGI 3 (Everyone)
Policy s.6: "Children cannot create their own user accounts without the consent of
    their parents or guardians... we treat anyone under the age of 13 as a child."
```

Impact: A child can register for a product rated for everyone with a phone number or a social login, and the policy promises a parental consent step that the resources do not show.

Fix: Add an age gate with parental consent or state that the app is for adults, and align the rating.

H7: The Data Safety label omits contacts, SMS, call log, camera and microphone although permissions and the policy name them

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026

The developer-submitted label lists as shared with third parties: Location, Health and fitness, Device or other IDs. It lists as collected: Location, Device or other IDs, Photos, Health and fitness, and Personal info (Name, Email address, Other info). It names no Contacts, SMS, Call logs, Camera beyond Photos or Microphone. The package requests READ_CONTACTS, RECEIVE_SMS, READ_CALL_LOG, CAMERA and RECORD_AUDIO, and the policy says: APP will get the incoming calls, SMS and address book data, and with your consent, we will obtain incoming calls, messages and contact information for display. The operator says that it does not save this data. Google's Data Safety guidance covers data that passes through the app, so the statement does not obviously exempt it from the label. Whether the label breaks a Google Play rule is for Google to decide. This report records the gap between the label and the declared permission and policy surface.

```
Shared with third parties: Location, Health and fitness, Device or other IDs
Collected: Location, Device or other IDs, Photos, Health and fitness, Personal info (
    Name, Email address, Other info)

READ_CONTACTS  RECEIVE_SMS  READ_CALL_LOG  CAMERA  RECORD_AUDIO  (manifest)
```

Impact: A person who reads the label is not told that the app reaches contacts, messages, call log and microphone, so they cannot weigh those permissions.

Fix: Align the Data Safety label with the permissions and the policy, including data that passes through the app.

M1: Two parallel notification capture paths, a notification listener and a scoped accessibility service, with the destination of the content not shown

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), disclosed as MEDIUM on 23 August 2026

The manifest declares com.yc.pedometer.remind.StatusbarMsgNotificationListener with BIND_NOTIFICATION_LISTENER_SERVICE and com.yc.pedometer.remind.MessageAccessibilityService with BIND_ACCESSIBILITY_SERVICE. The accessibility configuration limits events to typeNotificationStateChanged for fifteen named messaging packages and sets canRetrieveWindowContent to false, so it cannot read arbitrary screen content. That is a narrower grant than a worst-case use of the API. The listener alone is enough to read notification content system-wide, so the second path is redundant for one stated purpose. The Play listing says the app gets the Accessibility Services to implement a message push function. Whether the captured text is kept, forwarded to a backend or an analytics SDK, or stays on the Bluetooth link as the policy says is not shown, since the packer of H1 hides the code. The policy says that the app will not save incoming call, message, contact and other related information.

```
<service android:name="com.yc.pedometer.remind.StatusbarMsgNotificationListener"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
    NotificationListenerService"/></intent-filter>
</service>
<service android:name="com.yc.pedometer.remind.MessageAccessibilityService" android:
    permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter><action android:name="android.accessibilityservice.
    AccessibilityService"/></intent-filter>
    <meta-data android:name="android.accessibilityservice" android:resource="@xml/
    accessibility_service_message_config"/>
</service>

<accessibility-service android:accessibilityEventTypes="typeNotificationStateChanged"
  android:packageNames="com.kakao.talk, com.skype.polaris, com.facebook.orca, com.
    facebook.Messenger, jp.naver.line.android, jp.naver.line, com.tencent.mobileqq,
    com.skype.raider, com.skype.skype, com.skype.tomskype, com.twitter.android, com.
    tencent.mm, com.facebook.katana, com.skype.rover, com.google.android.talk, com.
    whatsapp"
  android:canRetrieveWindowContent="false" ... />
```

Impact: People who write to the user in WhatsApp, Messenger or WeChat have their names and message previews pass through the app without having agreed to anything.

Fix: Keep one capture path, restrict the listener to the apps the user selects and state that message content stays on the Bluetooth link.

M2: Installed application inventory is read, confirmed in code and in the policy

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), disclosed as MEDIUM on 23 August 2026

The unprotected dex string pool contains the calls getInstalledApplications and getInstalledPackages. Section 1.1 of the policy says: Software installation list: Your software installation list may need to be collected when you use the login function and APP push service, but we do not store your software list information. An installed-app list can reveal health, dating, religious or political app choices. The stated purpose of showing the available software does not obviously need the full list. Transmission was not shown and the policy says the list is not stored.

```
getInstalledApplications
getInstalledPackages
```

Impact: The list of apps on a phone is a profile of the person, and the policy gives only a thin reason for reading it.

Fix: Limit the query to the packages the login and push functions need and state it in the policy.

Impact Analysis

The people affected are the users of a health companion with more than 1 million installs. The app handles blood pressure, ECG, blood oxygen, body temperature and menstrual cycle data, and it shows some of it to other accounts through the relatives and friends feature. Some users are minors, since the Play rating is PEGI 3.

The weight of the case sits on three points. The special category data set meets a Chinese cloud and analytics stack with no transfer mechanism named (C1). A relative or friend can see a person’s health profile and the person has no described information step of their own (H2). The operator wrapped its code in a packer, so neither a user nor an authority can read what the app does at start-up (H1). The weak signing key (C2) matters for the trust of every update.

The package shows endpoints, features, text and a certificate. No health reading was observed leaving a device and the report asserts no such flow.

The Complete Chain

Step 1, install: a user installs the app from Google Play after reading a label that omits contacts, SMS, call log and microphone (H7). Every update is signed with a 1024-bit key (C2).

Step 2, start-up: the stub Application loads hidden code (H1). Whether analytics SDKs start before the consent screen is not shown.

Step 3, pairing and data: the user pairs a DB02 band and the app reads blood pressure, ECG, temperature and menstrual cycle data (C1). Relatives and friends can see it after an authorisation (H2).

Step 4, notifications: two capture paths mirror message previews to the band (M1).

Step 5, recipients: the policy names Alibaba, Umeng and Tencent services with identifiers it says it collects (H4), and no transfer mechanism (C1).

Step 6, rights: a person who wants to ask who holds the data reads three names and one mailbox (H3).

Same-Developer Cluster and Chipset Fingerprint

The cross-developer Bluetrum hypothesis is not confirmed for FlagFit 2.0. A search of all unprotected dex files and all native libraries for bluetrum returned no match and no libab-partool.so or equivalent exists. The band side uses Realtek Realsil instead. The signing certificate matches none of HryFine (923b7186b8811b3b71ae22c2bb506b4e2ab80dd53fb5460c412d6f97a7ae3375), Wearfit Pro or Fere Fit, which each sign their own builds.

What is confirmed is a same-developer cluster. At least seven storefront apps share one Play developer account, and FlagFit 2.0 is a re-skin of a single code base under the com.yc.pedometer package. The GloryFit package carries the identical signing certificate SHA-256 and the identical DN, and GloryFit additionally ships the Bluetrum SDK. The same-developer cluster and the Bluetrum cluster are separate lines. The relationship to other apps was not decompiled in this pass.

```
Signing cert SHA-256
    f90cbd89621b70e6dee4caca3bc71483ccf17163c6e3313285535cca91f43108
Signing DN              CN=Huang Jianchao, OU=Youchuang, O=Youchuang, L=Guilin, ST=
    Guangxi, C=CH
BLE vendor SDK          Realtek Realsil DFU: com.realsil.android.blehub.dfu.DfuService,
     com.realsil.sdk.dfu.DfuService
Native library          libRtkAesJni.so (
    Java_com_realsil_sdk_dfu_utils_AesJni_aes_1encrypt)
Internal package        com.yc.pedometer.* (application ID com.yc.flagfit2)
Packer                  com.sagittarius.v6.StubApplication, Baidu Protect,
    libbaiduprotect.so
Sibling apps            FlagFit, GloryFit (com.yc.gloryfit), GloryFitPro, Du Watch,
    iGloryfit, Glory Note, Glory View
```

Data Protection: Article by Article

Article 4(7), controller: engaged by H3.

Article 4(1), personal data: engaged by M2.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H4, H6 and H7.

Article 5(1)(c), data minimisation: engaged by H2, M1 and M2.

Article 5(2), accountability: engaged by C2, H1 and H5.

Article 6(1) and Article 7: engaged by M1.

Article 8, children: engaged by H6.

Article 9(2): engaged by C1 and H2 for health and menstrual cycle data. No unlawful processing is asserted.

Articles 13 and 14: engaged by C1, H2, H3 and H4. Article 13(1)(f) is engaged by C1.

Article 25: engaged by H1 and H5.

Article 27: engaged by H3. No representative is named.

Article 32(1)(a) and (b): engaged by C2 and H5.

Article 35: engaged by H1 and M2. A data protection impact assessment is not published.

Articles 44 and 46: engaged by C1. The policy and the binary name no mechanism.

Platform Accountability & DSA

The Data Safety label of FlagFit 2.0 says that Location, Health and fitness and Device or other IDs may be shared with third parties. It says that data is encrypted in transit and that users can request deletion. It names no Contacts, SMS, Call logs or Microphone as collected or shared, while the manifest requests the matching permissions and the policy describes them (H7). The label statement on encryption in transit agrees with the absence of a global cleartext override in the network security configuration.

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 and treats the notice as a decision for the publication stage.

Regulatory & Legal Landscape

The developer account and the policy entity offer the app to users in the Union through Google Play, 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 where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) received the notice in copy.

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. 25, 27, 32 and 35 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user’s device.

The notice mentioned the access powers that PRC law gives to PRC-domiciled processors as a risk factor for Chapter V. The report records it as context. The report does not assess PRC law. The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.yc.flagfit2
Version            1.10.2 (versionCode 102), 54.8 MB (57,440,191 bytes)
APK SHA-256        328c9adad5da685984f7f47325107e22ecc278c64c0d42b5c69de401770037ae
Signing cert SHA-256  f90cbd89621b70e6dee4caca3bc71483ccf17163c6e3313285535cca91f43108
Serial number      54adf9d9
Validity           2015-01-08 until 2124-07-15
Key                1024-bit RSA, SHA1withRSA
Audit device       none, the app was not installed
```

```
Google geo API key   AIzaSyCSgtyaBMNfU3Utjmgn5dLcLY72xnwGVVE
AMap API key         a8772b9da7408d26825410d2c48e03df
UMENG_APPKEY         5969cb8945297d03c1000233
YCAPPKEY             12b0cb43454d2cd2f8c0562de71d7157
Storage endpoints    http://oss.aliyuncs.com, http://oss-cn-hangzhou.aliyuncs.com
AMap endpoints       https://apiinit.amap.com/v3/log/init, https://adiu.amap.com/ws/
    device/adius
Umeng endpoint       https://alogsus.umeng.com
Tencent endpoints    https://openmobile.qq.com/oauth2.0/m_authorize, https://open.
    weixin.qq.com/connect/sdk/qrconnect
Policy URL           https://www.ute-tech.com.cn/privacy-policy/
    myprivacypolicy_english.htm
Contact              support@ute-tech.com.cn
Placeholder host     secure.example.com (cleartext exception)
```

```
C1  dex strings (aliyuncs.com, amap.com, umeng.com, qq.com), AndroidManifest.xml (meta
    -data), policy
C2  apksigner verify --print-certs, keytool -printcert
H1  AndroidManifest.xml (StubApplication), assets/baiduprotect*, lib/*/libbaiduprotect
    .so
H2  AndroidManifest.xml (FriendsActivity, ConnectHelp), policy
H3  Google Play listing, policy, signing certificate
H4  policy section 7
H5  AndroidManifest.xml (meta-data)
H6  Google Play listing, res/values/strings.xml, policy section 6
H7  Google Play Data Safety page, AndroidManifest.xml, policy
M1  AndroidManifest.xml, res/xml/accessibility_service_message_config.xml
M2  dex strings (getInstalledApplications, getInstalledPackages), policy section 1.1
```

Reproduction: obtain com.yc.flagfit2 1.10.2 (102), check the SHA-256 values above, decode the manifest and resources with apktool, extract the dex string pools with strings and read the certificate with apksigner and keytool. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF FLAGFIT20-2026-R1 at 04:31 UTC to support@ute-tech.com.cn, CC dsb@dsb.gv.at and edps@edps.europa.eu. Two critical and seven high findings, three questions, response requested within 30 days.

2026-09-12 Follow-up at 16:46 UTC, 20 days after the notice. It restated the findings and asked three questions on the transfer mechanism for the health data, the consent of the profiled relative and the controller and the signing certificate, with answers due on 26 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:04 UTC, 35 days before publication, with the three questions unchanged in substance.

2026-11-14 No reply of any kind and no delivery failure. The mailbox holds no inbound message from the operator.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

What Was Done Well

A working consent screen exists with the strings read_and_agree, user_agreement_agree and user_agreement_disagree, and a Disagree path is present. The network security configuration has no global cleartext override, and the only cleartext exception is a placeholder host from an SDK template. The scoped accessibility service is deliberately narrow, with canRetrieveWindowContent set to false, only notification state events and a fixed list of fifteen messenger packages. An account deletion path is documented as Me, Personal information, Cancel Account and agrees with the Data Safety statement that users can request deletion. The Data Safety label says that data is encrypted in transit. A child protection paragraph exists in the policy, which shows documented intent even though no enforcement is visible in the resources.

Residual Risk & Recommendations

Open at the date of publication: all findings except the observation. The operator has not replied and the build analysed is version 1.10.2. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, name the recipients of the health data with country and transfer mechanism, publish the transfer impact assessment and state which data reaches the Hangzhou storage (C1). Second, show the profiled person what is shared, with whom and for how long, and allow withdrawal (H2). Third, rotate the signing key and name the legal entity in the certificate (C2). Fourth, name one controller with a postal address, a data protection contact and an Article 27 representative (H3). Fifth, review the policy against the current build and align the Data Safety label with the permissions (H4, H7). Sixth, restrict the keys, add an age gate, keep one notification path and trim the installed-package query (H5, H6, M1, M2).

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. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF FLAGFIT20-2026-R1.