Security & Privacy Disclosure, Final Report

GloryFit for Android (com.yc.gloryfit)

A built-in Chinese voice cloning toolkit, a tracking stack with no consent platform and global cleartext in a health wearable app with 10 million installs, 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. (GloryFit), policy issued by Shenzhen Ultra Easy Technology Co., Ltd.
Versions Audited	4.0.10 / versionCode 277 (updated 2026-08-21, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 1 High, 5 Medium, 4 Low, 1 observation (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`0c26ec567c3db97161a84717de3d3641325251b5eeccae3b22e0d6b805eef83d`

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: Tracking and login SDK stack with no consent platform in the package . . 7
- 6.2 C2: Volcengine voice cloning and speech SDK with a microphone service, not disclosed 8
- 6.3 H1: Cleartext traffic permitted for the whole app, 10 million installs 10
- 6.4 H2: Bluetrum and Realtek chipset SDKs, third Bluetrum cluster member 11
- 6.5 H3: Chinese infrastructure against a policy naming only affiliated companies . 12
- 6.6 H4: Notification listener next to call log, contacts and SMS permissions 13
- 6.7 M1: MQTT client on Alibaba Cloud IoT Hub gives the backend a channel 14
- 6.8 M2: Camera remote control and photo access with an object storage SDK . . . 14
- 6.9 M3: Two operator names, no Article 27 representative, odd certificate country 15
- 6.10 M4: Parental consent promised for under 13, no age gate in the resources . . . 16
- 6.11 M5: Kakao app key in the resource table 16

7 Impact Analysis 17

8 The Complete Chain 17

9 Shared Chipset or Platform Fingerprint 18

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 19

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 21

Executive Summary

GloryFit (package com.yc.gloryfit) is the companion app of a line of Bluetooth fitness bands. It is published on Google Play as Youchuangyi Health Technology (Shenzhen) Co., Ltd., has more than 10 million installs, a rating of 3.8 stars from 171 thousand reviews and PEGI 3. On 23 August 2026 RFI-IRFOS sent a notice with REF GLORYFIT-2026-R1 to jc.huang@ute-tech.com.cn and support@ute-tech.com.cn, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

The root level code analysis of version 4.0.10 shows a compiled ByteDance Volcengine toolkit for voice chat, speech recognition, speech synthesis, voice cloning and language model streaming, declared with a microphone foreground service (C2). Neither the Play description nor the privacy policy text mentions it. The package carries a dense Chinese and global tracking and login stack and no consent management platform (C1). Cleartext traffic is permitted for the whole app on a product that handles health data, which makes this the one finding that stays at High (H1). The endpoints of the stack sit on Chinese infrastructure against a policy that names only affiliated companies (H3). A notification listener sits next to call log, contacts and SMS permissions (H4). The package also ships the Bluetrum chipset SDK found in HryFine and Wearfit Pro, which makes GloryFit the third member of that fingerprint cluster (H2).

A reassessment by CVSS v4.0 band puts five findings at Medium, four at Low and one at High, with one observation left unrated. The two findings disclosed as Critical move to Medium because the package shows the toolkit and the stack and does not show activation, start order or a data flow. GloryFit shares its signing certificate and code base with FlagFit 2.0 (REF FLAGFIT20-2026-R1).

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 4.0.10 (versionCode 277), obtained as an XAPK bundle from a download mirror and matched to the live Google Play listing on package ID, developer name, version and update date. Work done: manifest, resources, strings and network security configuration decoded without a source decode (apktool), a string pass across all eight classes dex files, the native library inventory from the armeabi-v7a split and the signing certificate. 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. Anything that depends on runtime behaviour is marked as such.

ID	Severity	Title
C1	MEDIUM	Tracking and login SDK stack with no consent platform in the package
C2	MEDIUM	Volcengine voice cloning and speech SDK with a microphone service, not disclosed
H1	HIGH	Cleartext traffic permitted for the whole app, 10 million installs
H2	INFO	Bluetrum and Realtek chipset SDKs, third Bluetrum cluster member
H3	MEDIUM	Chinese infrastructure against a policy naming only affiliated companies
H4	MEDIUM	Notification listener next to call log, contacts and SMS permissions
M1	LOW	MQTT client on Alibaba Cloud IoT Hub gives the backend a channel
M2	LOW	Camera remote control and photo access with an object storage SDK
M3	MEDIUM	Two operator names, no Article 27 representative, odd certificate country
M4	LOW	Parental consent promised for under 13, no age gate in the resources
M5	LOW	Kakao app key in the resource table

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Start order of the SDKs not traced.
C2	CRITICAL	MEDIUM	No reply. Reachability of voice features in the user interface not established.
H1	HIGH	HIGH	No reply. Kept at High by blast-radius escalation, computed band Medium.
H2	HIGH	INFO	Not rated. Shared chipset SDK fingerprint.
H3	HIGH	MEDIUM	No reply. Data flow per host not traced.
H4	HIGH	MEDIUM	No reply. Destination of notification content not shown.
M1	MEDIUM	LOW	No reply. Capability only, command vocabulary not reconstructed.
M2	MEDIUM	LOW	No reply. Upload of photos not shown.
M3	MEDIUM	MEDIUM	No reply. Two names, no representative.
M4	MEDIUM	LOW	No reply. Server side age check not excluded.
M5	LOW/MEDIUM	LOW	No reply. Hygiene only.

Subject & Operator Analysis

GloryFit is published as Youchuangyi Health Technology (Shenzhen) Co., Ltd. with a registered address in Xixiang, Baoan, Shenzhen. The privacy policy at app.help-document.com names Shenzhen Ultra Easy Technology Co., Ltd. and the website is ute-tech.com.cn. The contacts are jc.huang@ute-tech.com.cn on the operator domain, support@ute-tech.com.cn and the mobile number +86 185 6575 8972. No data protection officer and no Article 27 representative was found (M3).

The same developer account publishes at least six sibling storefront apps beside GloryFit, namely GloryFitPro, Du Watch, iGloryfit, Glory Note, Glory View and FlagFit, and FlagFit 2.0 is one of them. The signing certificate SHA-256 is identical to the one of FlagFit 2.0, and both apps carry the internal package com.yc.pedometer. The cluster of this operator is therefore a same-developer white-label family.

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

Architecture & Data Flow

GloryFit is a native Android app with eight classes dex files of about 61 MB, targeting API level 36 with a minimum of API level 26. The Application class is com.yc.pedometer.MyApplication. The band side combines the Bluetrum OTA stack (libabpartool.so, Lcom/bluetrum/fota) with the Realtek DFU service, so the app can serve more than one hardware batch (H2).

On the network side the package holds the operator backend at www.ute-tech.com.cn, a WeChat linked authorisation host, an Alibaba Cloud IoT Hub MQTT client (M1), Alibaba Object Storage, iFlytek speech interfaces and the Volcengine host of the Starburst toolkit (C2, H3). Umeng, Tencent, Alibaba, Sobot, Facebook, Twitter and Google Sign-In classes complete the stack (C1). The network security configuration permits cleartext for all hosts (H1). The manifest sets allowBackup to false.

The device facing features are a notification listener (H4), a camera remote control (M2) and AI generated diet plans with a daily limit (C2).

Engagement Summary

The notice REF GLORYFIT-2026-R1 was sent on 23 August 2026 at 00:28 UTC from rfi.irfos@gmail.com to jc.huang@ute-tech.com.cn and support@ute-tech.com.cn with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried eleven findings, two critical, four high and five medium or low, with evidence and three questions. A follow-up of 12 September 2026 restated the open findings and set 19 September 2026 as the date 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: Tracking and login SDK stack with no consent platform in the package

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), disclosed as CRITICAL on 23 August 2026

The dex files of version 4.0.10 contain the class namespaces of Umeng (analytics, common, commonsdk, pagesdk, powersdk, umcrash, vt), Tencent (WeChat, QQ Connect, tauth, MMKV), Alibaba (aliagentsdk, fastjson), ByteDance Starburst, Sobot chat, Facebook, Twitter and Google Sign-In, with the native libraries libumeng-spy.so, libAMapSDK_MAP_v10_0_700.so and libcrashsdk.so. The Application class is com.yc.pedometer.MyApplication and the application element sets usesCleartextTraffic to true. A search of all resource files and the manifest for onetrust, didomi, usercentrics, iabtcf and consentmanager returned no hit. The androidx.startup list in the manifest holds only four unrelated initialisers (Net, EmojiCompat, ProcessLifecycle, LogX), so the SDK start points are not in that list. Calls placed directly in MyApplication.onCreate() would run before any screen. The call order was not traced, because no bytecode control-flow pass was done, and the report therefore asserts the stack and the absence of a consent platform and does not assert the order. The vector models a local, pre-consent collection with a low confidentiality impact for that reason.

```
Lcom/umeng/analytics/*   Lcom/umeng/common/*   Lcom/umeng/commonsdk/*   Lcom/umeng/
    pagesdk/*   Lcom/umeng/powersdk/*   Lcom/umeng/umcrash/*   Lcom/umeng/vt/*
Lcom/tencent/mm/* (WeChat)   Lcom/tencent/connect/*   Lcom/tencent/tauth/* (QQ)   Lcom
    /tencent/mmkv/*
Lcom/alibaba/aliagentsdk/*   Lcom/alibaba/fastjson/*   Lcom/starburst/sdk/*
Lcom/sobot/chat/*   Lcom/sobot/gson/*   Lcom/sobot/network/*
Lcom/facebook/*   Lcom/twitter/sdk/*   Lcom/google/android/gms/auth/api/signin/*

libumeng-spy.so   libAMapSDK_MAP_v10_0_700.so   libcrashsdk.so

<application android:allowBackup="false" android:name="com.yc.pedometer.MyApplication"
    android:networkSecurityConfig="@xml/network_security_config" android:
    usesCleartextTraffic="true" ...>
```

Impact: The app measures steps, sleep and heart rate, which are health data. A person who installs it meets an analytics and social login stack from several Chinese and US vendors in the binary and no consent platform that would let them say no before it runs.

Fix: Add a consent management platform, start analytics and login SDKs only after the choice and document the start order in the data protection impact assessment.

C2: Volcengine voice cloning and speech SDK with a microphone service, not disclosed

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 CRITICAL on 23 August 2026

The manifest declares the service com.starburst.sdk.core.keepalive.KeepAliveManager$KeepAliveService with foregroundServiceType connectedDevice, dataSync and microphone. The dex files hold the Starburst classes for voice chat recording (VoiceChatManager), speech recognition (AsrWsRequest), speech synthesis (TextToSpeechWs, VolcTtsWsFrame), voice cloning (VoiceCloneWs, IVoiceCloneCallback), image generation (ImageToImageRequest, ITextToImageManager), podcast generation (PodcastManager) and feed handling. Eight endpoint literals point to a Volcengine host in Beijing, the cloud platform of ByteDance. Native libraries for voice activity detection, on-device inference, the Microsoft Cognitive Services Speech SDK and Opus and Speex codecs sit beside it. A feature for AI generated diet plans, with a daily generation limit, is confirmed in the resource strings. The Play description names step counting, sleep, heart rate, message and call reminders and camera control and no voice or AI feature. The privacy policy text read on 23 August 2026 contains no mention of AI processing, machine learning or voice data collection. Whether the voice chat, recognition and cloning entry points are reachable from the user interface of this build or are shared code from the operator’s other storefront apps is not established, and the audio content that would be sent is not known. The score therefore models a user-activated, low impact exposure.

```
<service android:enabled="true" android:exported="false"
    android:foregroundServiceType="connectedDevice|dataSync|microphone"
    android:name="com.starburst.sdk.core.keepalive.KeepAliveManager$KeepAliveService
    "/>

Lcom/starburst/sdk/business/
    VoiceChatManager$voiceChatRecorderStateListener$1$audioListener$1;
Lcom/starburst/sdk/core/asr/AsrWsRequest$1;   Lcom/starburst/sdk/core/asr/
    AsrWsRequest$2;
Lcom/starburst/sdk/core/tts/TextToSpeechWs;   Lcom/starburst/sdk/core/tts/
    VolcTtsWsFrame;
Lcom/starburst/sdk/core/clone/VoiceCloneWs;   Lcom/starburst/sdk/api/
    IVoiceCloneCallback;
Lcom/starburst/sdk/api/ImageToImageRequest;   Lcom/starburst/sdk/api/
    ITextToImageManager;
Lcom/starburst/sdk/business/PodcastManager;   Lcom/starburst/sdk/core/feed/FeedManager
    ;   Lcom/starburst/sdk/api/IGuiControlCallback;
```

```
https://ainf.tis.cn-beijing.volces.com/tis/ai/audio/device/asr/byfile/create
https://ainf.tis.cn-beijing.volces.com/tis/ai/audio/device/asr/byfile/query
https://ainf.tis.cn-beijing.volces.com/tis/ai/device/llm/stream
https://ainf.tis.cn-beijing.volces.com/tis/ai/device/podcast/stream
https://ainf.tis.cn-beijing.volces.com/starburst/ai/tts
https://ainf.tis.cn-beijing.volces.com/starburst/ai/aigc/create/async
https://ainf.tis.cn-beijing.volces.com/starburst/ai/aigc/create/sync
https://ainf.tis.cn-beijing.volces.com/tis/device/register

libimsl_vad.so   libonnxruntime.so   libMicrosoft.CognitiveServices.Speech.*
    libst_opus.so   libst_speex.so   libjl_opus.so   libjl_speex.so
```

```
generate_recipes            (Chinese string, meaning: Generating recipe...)
diet_plan_reset_tip         (Chinese string, meaning: Confirm regenerating the weight-
    loss recipe?)
today_generation_limit      (Chinese string, meaning: Today's generation limit reached
    )
```

Impact: A person who wears the band and talks near the phone has no way to learn from the app description or the policy that a voice recognition and voice cloning toolkit of a Chinese cloud provider is built in. The audio and the voice model of a person are biometric in character once they are used to clone a voice.

Fix: State in the policy whether voice, speech or language processing is active in the app, name the recipient and the legal basis, publish the data protection impact assessment and remove the SDK parts the product does not use.

H1: Cleartext traffic permitted for the whole app, 10 million installs

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as HIGH on 23 August 2026, rated HIGH by blast-radius escalation

res/xml/network_security_config.xml sets cleartextTrafficPermitted to true in the base-config, and the application element of the manifest sets usesCleartextTraffic to true. A domain-config repeats the allowance for android.bugly.qq.com, a Tencent Bugly crash reporting domain, and for the placeholder host secure.example.com, which points to a template that was never hardened. The app targets API level 36, where cleartext HTTP is refused by default, so both settings switch that protection off for every host. No pin-set was found. Whether a given endpoint is called over plain HTTP was not tested and no traffic was captured. The score reflects an attacker on the same network path and the need for the app to use an http:// address. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the app is positioned to carry health readings, location, call log, contacts and messages, it has more than 10 million installs on Google Play and the allowance covers every host in the dex strings including the operator backend.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">secure.example.com</domain>
        <domain includeSubdomains="true">android.bugly.qq.com</domain>
    </domain-config>
</network-security-config>
```

Impact: The app handles heart rate and sleep readings from the band, location, call log, contacts and messages. A plain HTTP request to any host travels in the open on a shared Wi-Fi network or a hostile access point. For a person who wears the band all day, the data at stake is the most personal kind a phone holds.

Fix: Remove the base-config override and the application flag, allow cleartext only for named hosts that need it, pin the first-party hosts and verify that every endpoint in the dex strings uses https.

H2: Bluetrum and Realtek chipset SDKs, third Bluetrum cluster member

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

The package ships libabpartool.so and the class namespaces Lcom/bluetrum/abpartool and Lcom/bluetrum/fota with the ABOta class. The same Bluetrum reference SDK was found in the HryFine package com.lianhezhuli.hyfit and in the Wearfit Pro package com.wakeup.howear, which are signed with different certificates and published by different developer accounts. A second chipset vendor toolkit is bundled, the Realtek DFU service com.realsil.sdk.dfu.DfuService with libRtkAesJni.so and libRtkMediaCodec.so, which points to more than one hardware batch behind the storefront. The shared SDK shows a common hardware platform behind several consumer brands. It does not show that the three apps share a backend, and each app's own findings rest on its own evidence. No exposure follows from the shared library itself, so the report records it as an observation and does not rate it.

```
libabpartool.so   SHA-256 3012
    eaf67be421437561f4771ea491f5d8c9de8f67470b9d03c34a11fc90fc2b
Lcom/bluetrum/abpartool/R;
Lcom/bluetrum/fota/abota/ABOta;
Lcom/bluetrum/fota/BuildConfig;
Lcom/bluetrum/fota/log/ILogger;
Lcom/bluetrum/fota/log/Logger;
Lcom/bluetrum/fota/R;

<service android:enabled="true" android:exported="false" android:name="com.realsil.sdk
    .dfu.DfuService"/>
libRtkAesJni.so   libRtkMediaCodec.so   MANUFACTURER_ID_REALTEK
```

Impact: A user or an authority who looks at one brand in isolation does not see that the same hardware platform sits behind several apps, so the question of who processes the data on that platform stays open.

Fix: Name the party that controls the processing on the shared platform and list the chipset vendor SDKs in the policy.

H3: Chinese infrastructure against a policy naming only affiliated companies

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 HIGH on 23 August 2026

The dex files hold endpoints on Alibaba Cloud IoT Hub (MQTT) and IoT authorisation in Shanghai, Alibaba Cloud Object Storage in Shanghai and Hangzhou, the iFlytek speech interfaces iat-api.xfyun.cn and tts-api.xfyun.cn, the operator's own backend at www.ute-tech.com.cn and a WeChat linked device authorisation host at tt-smartband-weixin.ute-tech.com.cn, in addition to the Volcengine host of C2. The manifest declares an MQTT client service. The policy states that information may be disclosed to affiliated companies in the communications, social media, technology and cloud businesses, and it names no jurisdiction, no entity and no transfer mechanism. The report does not assess PRC law. The finding is the absence of a named mechanism for a stack that is Chinese by its endpoints. Which user data reaches which host was not traced.

```
tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com        (Alibaba Cloud IoT Hub, MQTT
    )
https://iot-auth.cn-shanghai.aliyuncs.com                  (Alibaba Cloud IoT auth)
https://oss-cn-shanghai.aliyuncs.com   https://oss-cn-hangzhou.aliyuncs.com   https://
    oss.aliyuncs.com   (Alibaba Object Storage)
https://iat-api.xfyun.cn/v2/iat   https://tts-api.xfyun.cn/v2/tts   (iFlytek speech)
https://www.ute-tech.com.cn/ci3/index.php/api/*            (operator backend)
https://tt-smartband-weixin.ute-tech.com.cn/foyal_wechat/index.php/app/device/
    authorize   (WeChat linked device authorisation)

<service android:enabled="true" android:name="org.eclipse.paho.android.service.
    MqttService"/>
```

Policy wording as read on 23 August 2026 at https://app.help-document.com/privacy-policy/gloryfit_en.html: information may be disclosed to affiliated companies (which are in the communications, social media, technology and cloud businesses).

Impact: The people who use the band are told that data goes to affiliated companies in several industries. They are not told which countries, which companies or which safeguards apply.

Fix: Name each recipient with country and transfer mechanism, publish the transfer impact assessment per platform and state which data reaches which host.

H4: Notification listener next to call log, contacts and SMS permissions

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 HIGH on 23 August 2026

The manifest declares com.yc.pedometer.remind.StatusbarMsgNotificationListener with BIND_NOTIFICATION_LISTENER_SERVICE and requests READ_CALL_LOG, READ_CONTACTS, RECEIVE_SMS, SEND_SMS, CALL_PHONE, ANSWER_PHONE_CALLS, READ_PHONE_STATE and ACCESS_BACKGROUND_LOCATION. Mirroring notifications to a watch is the advertised use and is not the finding. The combination is, because a listener sees sender, source app and text of every notification, and the call log and contacts permissions add who the user talks to. Whether notification content is kept, sent off the device or only rendered on the watch is not shown, since no bytecode control-flow pass was done.

```
<service android:exported="false" android:label="@string/app_name"
    android:name="com.yc.pedometer.remind.StatusbarMsgNotificationListener"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE"/>

android.permission.READ_CALL_LOG        android.permission.READ_CONTACTS
android.permission.RECEIVE_SMS          android.permission.SEND_SMS
android.permission.CALL_PHONE           android.permission.ANSWER_PHONE_CALLS
android.permission.READ_PHONE_STATE     android.permission.ACCESS_BACKGROUND_LOCATION
```

Impact: People who write to the user receive no notice that their message previews, including banking alerts and codes, pass through a health app. Notification text reveals health and religious information about third parties who never agreed.

Fix: Restrict the listener to the apps the user selects, drop the call log and contacts permissions that the notification feature does not need and state in the policy that message content stays on the Bluetooth link.

M1: MQTT client on Alibaba Cloud IoT Hub gives the backend a channel

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The manifest declares org.eclipse.paho.android.service.MqttService, and the dex strings hold the Alibaba Cloud IoT Hub address iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com. MQTT is a two-way channel, so a backend can push messages to an installed app at any time. The topic structure, the command vocabulary and whether any command changes device behaviour beyond sync and firmware update were not reconstructed. This is a capability and no abuse is shown.

```
<service android:enabled="true" android:name="org.eclipse.paho.android.service.
    MqttService"/>
tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
```

Impact: A user cannot tell from the policy that the operator can reach the app after installation.

Fix: Describe the remote command channel in the policy and list the commands it carries.

M2: Camera remote control and photo access with an object storage SDK

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 Play description says that the app supports device control through the app for taking photos, saving and reading photos. The manifest requests CAMERA and READ_MEDIA_IMAGES, the Alibaba Object Storage SDK is in the dex files and the Data Safety label lists Photos as collected. Whether the read and save function covers only photos taken through the remote shutter or the whole gallery, and whether any photo is uploaded to the buckets of H3, is not established. A person who appears in a photo taken this way is not the account holder and sees no consent screen.

```
"Supports device control through App for taking photos, saving, and reading photos;
    supports submitting videos and providing feedback on application issues."
CAMERA   READ_MEDIA_IMAGES   (manifest)
Data Safety label: Photos listed as collected
```

Impact: A passer-by in a photo taken through the band remote has no notice and no way to ask what happens to the picture.

Fix: State whether photos leave the device, limit gallery access to the captured photos and cover bystanders in the policy.

M3: Two operator names, no Article 27 representative, odd certificate country

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 MEDIUM on 23 August 2026

The Google Play developer record reads Youchuangyi Health Technology (Shenzhen) Co., Ltd. with an address in Xixiang, Baoan, Shenzhen. The privacy policy names the controller Shenzhen Ultra Easy Technology Co., Ltd. The signing certificate is the one documented in the FlagFit 2.0 report of this package (identical SHA-256) and names a personal name and the organisation Youchuang in Guilin, Guangxi, with the country code CH, which is the code of Switzerland. The domain ute-tech.com.cn reads as Ultra Easy Technology, so the names may be one entity, and no company register was consulted. No Article 27 representative in the Union is named in the listing, the policy or the package, and no data protection officer was found.

Source	Identity given
Google Play developer listing	Youchuangyi Health Technology (Shenzhen) Co., Ltd., Building A, Room 503, Xicheng Longqiukou Industrial Park beside National Road 107, Xixiang, Baoan District, Shenzhen 518000
Privacy policy (app.help-document.com)	Shenzhen Ultra Easy Technology Co., Ltd.
APK signing certificate (SHA-256 f90cbd89621b70e6dee4caca3bc71483ccf17163c6e3313285535cca91f43108)	CN=Huang Jianchao, OU and O = Youchuang, L=Guilin, ST=Guangxi, C=CH (Chinese characters transliterated)
Contacts	jc.huang@ute-tech.com.cn, support@ute-tech.com.cn, +86 185 6575 8972

Impact: A person who wants to ask who holds their health data finds two company names, a mobile number and no representative in the Union.

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

M4: Parental consent promised for under 13, no age gate 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 MEDIUM on 23 August 2026

Google Play lists PEGI 3. The policy says that children cannot create their own user accounts without the consent of their parents or guardians, treats anyone under 13 as a child and commits to deleting data collected from minors without verifiable parental consent. A search of the resources and the dex strings for birthday, date_of_birth, parental, coppa, age_gate and under 13 returned one match, please_select_birthday, a birth date field used for a sleep metric. It has no blocking or parental consent step. An age check on the server would not appear in the package.

```
Google Play content rating: PEGI 3 (Everyone)
please_select_birthday = "APP will calculate your sleep habits according to age."
```

Impact: A child can register for a product rated for everyone, and the written promise of parental consent has no visible counterpart in the app.

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

M5: Kakao app key in the resource table

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 LOW/MEDIUM on 23 August 2026

res/values/strings.xml carries a Kakao app key. Client side app keys of social login platforms are not secrets by SDK design, so the entry is hygiene. It shows a Kakao login integration that the Play description does not mention. No Google, AWS or Stripe style secret was found, and no Firebase API key is in strings.xml. The Firebase Crashlytics build tooling class names in the dex are consistent with leftover symbol upload artefacts. No request was made with the key.

```
<string name="kakao_app_key">483d818d7beeabab0f45a5be89f8f028</string>
```

Impact: The key lets a third party use the operator’s Kakao quota. It does not expose user data.

Fix: Restrict the Kakao key to the package and signing certificate and remove the integration if it is unused.

Impact Analysis

The people affected are the users of a health companion app with more than 10 million installs, which includes minors under the PEGI 3 rating. The app records steps, sleep and heart rate, reads notifications, call log and contacts and relays photos from a camera control.

The weight of the case sits on three points. A toolkit for voice recognition and voice cloning from a Chinese cloud provider is built into the package, and the description and the policy text do not mention it (C2). A tracking and login stack ships with no consent platform (C1). Cleartext traffic is permitted for every host (H1). The infrastructure named in the package is Chinese throughout, against a policy that names only affiliated companies (H3).

The package shows classes, endpoints, permissions and text. No voice recording and 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 description that names step counting, sleep, heart rate and reminders, and a Data Safety label that is more candid than most peers.

Step 2, start-up: the application class starts and the SDK stack of C1 is present with no consent platform. The order of calls was not traced.

Step 3, pairing: the user pairs a band. The app speaks to chipsets of Bluetrum and Realtek (H2).

Step 4, features: notifications are mirrored (H4), a camera control reaches the phone camera (M2) and an AI diet plan feature calls a language model (C2).

Step 5, network: traffic goes to Alibaba, iFlytek, Volcengine and operator hosts in China (H3) and cleartext is allowed for all of them (H1). An MQTT client keeps a channel open to the backend (M1).

Step 6, rights: a person who wants to ask who holds the data reads two company names and finds no representative (M3).

Shared Chipset or Platform Fingerprint

The package ships the Bluetrum reference SDK as the same class namespace that was found in HryFine (com.lianhezhuli.hyfit) and Wearfit Pro (com.wakeup.howear). All three apps are signed with different certificates and published by different developer accounts. The Fere Fit report of this package documents a fourth member with the same fingerprint. The shared SDK shows one hardware platform behind several brands and is scoped in this report to that fingerprint. It makes no claim that the apps share a backend.

```
Bluetrum SDK          libabpartool.so SHA-256 3012
    eaf67be421437561f4771ea491f5d8c9de8f67470b9d03c34a11fc90fc2b
Bluetrum classes      Lcom/bluetrum/abpartool/R, Lcom/bluetrum/fota/abota/ABOta, Lcom
    /bluetrum/fota/BuildConfig, Lcom/bluetrum/fota/log/ILogger, Lcom/bluetrum/fota/log
    /Logger, Lcom/bluetrum/fota/R
Realtek DFU           com.realsil.sdk.dfu.DfuService, libRtkAesJni.so,
    libRtkMediaCodec.so, MANUFACTURER_ID_REALTEK
Signing cert SHA-256
    f90cbd89621b70e6dee4caca3bc71483ccf17163c6e3313285535cca91f43108 (identical to
    FlagFit 2.0)
Internal package      com.yc.pedometer.* (application ID com.yc.gloryfit)
Sibling apps          FlagFit, FlagFit 2.0, GloryFitPro, Du Watch, iGloryfit, Glory
    Note, Glory View
```

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, M3 and M4.

Article 5(1)(b) and (c), purpose limitation and data minimisation: engaged by H4, M1 and M2.

Article 5(1)(f), integrity and confidentiality: engaged by H1.

Article 5(2), accountability: engaged by C1 and H2.

Articles 6(1) and 7(1): engaged by C1 for the stack that precedes a consent choice. No unlawful processing is asserted.

Article 8, children: engaged by M4.

Article 9: engaged by C2 for voice data and by H4 for notification content.

Articles 13 and 14: engaged by C2 and H3. Articles 13(1)(f) and 14(1)(f) are engaged by H3.

Article 25: engaged by C2 and M1.

Article 27: engaged by M3. No representative is named.

Article 28: engaged by H2 and M2.

Article 32(1)(a) and (b): engaged by H1, M1 and M5.

Article 35: engaged by C2 and H3. A data protection impact assessment is not published.

Articles 44 and 46: engaged by C2 and H3. The policy names no mechanism.

Platform Accountability & DSA

The Data Safety label of GloryFit says that Health and fitness, Location and Device or other IDs may be shared with third parties and that Location, Personal info, Photos, Health and fitness and Device or other IDs may be collected. It says that data is encrypted in transit and that deletion can be requested. The label is more candid than many peers. It names no microphone or voice data, although the manifest requests RECORD_AUDIO and declares a microphone foreground service (C2). The statement on encryption in transit sits against a package that permits cleartext for every host (H1). The label was not re-read after 23 August 2026.

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about the Data Safety declaration under Art. 16 of that Regulation. RFI-IRFOS records the contradictions here and treats the notice as a decision for the publication stage.

Regulatory & Legal Landscape

The operator offers 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, 8 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, 28, 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 raised the access powers that PRC law gives to PRC-domiciled processors as a risk factor for Chapter V. The report records it as context and 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.gloryfit
Version            4.0.10 (versionCode 277), updated 2026-08-21, minSdk 26, targetSdk
    36
XAPK SHA-256       316e555eda64ecbd7b8d6973f4eaec51f7be866c12c508ab03c530b765761f5c
Base APK SHA-256   0c26ec567c3db97161a84717de3d3641325251b5eeccae3b22e0d6b805eef83d
armeabi-v7a split  43e2a04a08f960fdb31b9a8bfae2b305538f743351aeae84a101d0cd7e5c643f
libabpartool.so    3012eaf67be421437561f4771ea491f5d8c9de8f67470b9d03c34a11fc90fc2b
Signing cert SHA-256  f90cbd89621b70e6dee4caca3bc71483ccf17163c6e3313285535cca91f43108
Audit device       none, the app was not installed
```

```
Kakao app key        483d818d7beeabab0f45a5be89f8f028
Volcengine base    https://ainf.tis.cn-beijing.volces.com/
Alibaba IoT        tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com, https://iot-
    auth.cn-shanghai.aliyuncs.com
Alibaba storage    https://oss-cn-shanghai.aliyuncs.com, https://oss-cn-hangzhou.
    aliyuncs.com, https://oss.aliyuncs.com
iFlytek            https://iat-api.xfyun.cn/v2/iat, https://tts-api.xfyun.cn/v2/tts
Operator backend   https://www.ute-tech.com.cn/ci3/index.php/api/*
WeChat linked auth https://tt-smartband-weixin.ute-tech.com.cn/foyal_wechat/index.php/
    app/device/authorize
Bugly domain       android.bugly.qq.com (cleartext allowed)
Placeholder host   secure.example.com (cleartext allowed)
Policy URL         https://app.help-document.com/privacy-policy/gloryfit_en.html
Contacts           jc.huang@ute-tech.com.cn, support@ute-tech.com.cn, +86 185 6575
    8972
```

```
C1  dex namespaces, AndroidManifest.xml, res/values and manifest search for consent
    platforms
C2  AndroidManifest.xml (KeepAliveService), dex string pool (Starburst), res/values/
    strings.xml, policy
H1  res/xml/network_security_config.xml, AndroidManifest.xml (usesCleartextTraffic)
H2  lib/armeabi-v7a/libabpartool.so, dex (Lcom/bluetrum), AndroidManifest.xml (Realtek
     DfuService)
H3  dex string pool (endpoints), AndroidManifest.xml (MqttService), policy
H4  AndroidManifest.xml (StatusbarMsgNotificationListener and permissions)
M1  AndroidManifest.xml (MqttService), dex string pool
M2  Google Play description, AndroidManifest.xml, Data Safety page
M3  Google Play developer record, policy, signing certificate
M4  Google Play listing, res/values/strings.xml, policy
M5  res/values/strings.xml
```

Reproduction: obtain com.yc.gloryfit 4.0.10 (277), 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. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF GLORYFIT-2026-R1 at 00:28 UTC to jc.huang@ute-tech.com.cn and support@ute-tech.com.cn, CC dsb@dsb.gv.at and edps@edps.europa.eu. Eleven findings, three questions.

2026-09-12 Follow-up at 16:36 UTC, 20 days after the notice, with the open findings restated and the three questions due on 19 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

The manifest sets allowBackup to false, which blocks backup extraction of local app data. The Data Safety label is more candid than most peers and names health and fitness, location and device identifiers as shared with third parties and photos and personal information as collected. A deletion request path is stated on the label and the policy names a contact on the operator domain, not a private mailbox. The policy commitment on minors is specific in its wording. The app targets API level 36 and was updated two days before the analysis.

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 4.0.10. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, state whether voice, speech and language processing is active, name the recipient and the legal basis and publish the impact assessment, or remove the toolkit (C2). Second, remove the global cleartext allowance (H1). Third, add a consent management platform and start the SDKs after the choice (C1). Fourth, name each Chinese recipient with country and transfer mechanism (H3). Fifth, restrict the notification listener and drop unneeded call log and contacts permissions (H4). Sixth, name one controller with an Article 27 representative, describe the MQTT channel, cover bystanders in photos, add an age gate and restrict the Kakao key (M1 to M5). Seventh, name the party that controls the shared chipset platform (H2).

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 GLORYFIT-2026-R1.