Security & Privacy Disclosure, Final Report

Fere Fit for Android (com.czw.freefit)

A speech and text-generation pipeline the policy never names, a licence call into another operator’s backend, and cleartext traffic app-wide, with no reply since the notice.

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

Target	Shenzhen Zhongwei Intelligent Technology Co., Ltd (Fere Fit)
Versions Audited	5.6.49 / versionCode 849 (Play update 2026-05-29, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	9: 1 High, 7 Medium, 1 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`d6bdb810c0cfc4bce4fae0cb126c3f0e086f8f1074a19eb52d58db7e2f9b4c85`

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: Dedicated iFlytek speech recognition and generative text pipeline with its own audio recorder class sits behind RECORD_AUDIO, and the privacy policy never names the microphone . . . 7

6.2 C2: Live licence authentication call to gateway.iwhop.cn, the infrastructure family of another operator, and an embedded com.wakeup.license SDK that no policy text names . . . 8

6.3 C3: Cleartext traffic permitted for the whole app and no certificate pinning anywhere, on an app that handles health, location, call log and contacts data . . . 9

6.4 H1: Three different company names in one binary and a personal QQ mailbox as the only contact . . . 10

6.5 H2: The marketed SMS on the watch feature has no SMS receive permission behind it and runs through a notification listener that reads every app . . . 11

6.6 H3: Two Google API keys in the dex files, one concatenated into a live Google Cloud Translation API request . . . 12

6.7 H4: The SDK table in the privacy policy names seven SDKs and the binary ships more than twenty components . . . 13

6.8 M1: Google Mobile Ads initialises at process start and no consent management platform exists in the binary . . . 14

6.9 L1: PEGI 3 rating, a policy that requires parental consent under 18 and no age gate found in the resources . . . 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Shared Chipset SDK Fingerprint and Cluster 16

10 Data Protection: Article by Article 16

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 18

14 Disclosure Timeline & Outcome 19

15 What Was Done Well 19

16 Residual Risk & Recommendations 20

Executive Summary

Fere Fit is a companion app for Bluetooth wearables with more than 5 million installs on Google Play, published under the developer name Shenzhen Zhongwei Intelligent Technology Co., Ltd. It is rated PEGI 3 and carries the Contains ads and In-app purchases badges. It is meant to sync steps, sleep, heart rate and blood pressure readings from a band to the phone and to relay calls, messages and a remote camera trigger. On 23 August 2026 RFI-IRFOS sent a notice with REF FEREFIT-2026-R1 to the only contact address published for the app, 936160908@qq.com, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 5.6.49 shows a dedicated iFlytek SparkChain speech recognition and text-generation stack with its own audio recorder class behind the RECORD_AUDIO permission, while the bundled privacy policy explains six other permissions and never names the microphone (C1). The app makes a licence authentication call to gateway.iwhop.cn, the infrastructure family of Shenzhen Weike Technology (Wakeup), and embeds that company's com.wakeup.license SDK, with no mention in the policy (C2). Its network security configuration permits cleartext HTTP for every host and pins nothing (C3). Three different company names appear in the same binary and the only contact is a personal QQ mailbox (H1). The marketed SMS feature runs through a notification listener that reads all apps (H2). Two Google API keys are in the dex files, one inside a billed Translation API request (H3). The policy names seven SDKs and the binary ships more than twenty components (H4).

Fere Fit is the fourth app of the programme with the same Bluetrum BLE chipset SDK fingerprint, after HryFine, Wearfit Pro and WearFit2.0. A reassessment by CVSS v4.0 band puts one finding at High and seven at Medium. Every disclosed label that moves down does so because the package shows a capability or a configuration and not the runtime behaviour behind it.

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 5.6.49 (versionCode 849). The package was obtained as an XAPK from the APKPure mirror and verified against the package name, version, permission count, architecture and the signing certificate fingerprint shown on the mirror page. Work done: decoded manifest and resources (apktool, no source decode), string-pool extraction across seven classes*.dex files and the native library inventory of the arm64-v8a split. The Google Play listing was 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. Findings that depend on runtime behaviour are marked as such. The cross-checks against the Wearfit Pro package were made on the archived file of that audit.

ID	Severity	Title
C1	MEDIUM	Dedicated iFlytek speech recognition and generative text pipeline with its own audio recorder class sits behind RECORD_AUDIO, and the privacy policy never names the microphone
C2	MEDIUM	Live licence authentication call to gateway.iwhop.cn, the infrastructure family of another operator, and an embedded com.wakeup.license SDK that no policy text names
C3	HIGH	Cleartext traffic permitted for the whole app and no certificate pinning anywhere, on an app that handles health, location, call log and contacts data
H1	MEDIUM	Three different company names in one binary and a personal QQ mailbox as the only contact
H2	MEDIUM	The marketed SMS on the watch feature has no SMS receive permission behind it and runs through a notification listener that reads every app
H3	MEDIUM	Two Google API keys in the dex files, one concatenated into a live Google Cloud Translation API request
H4	MEDIUM	The SDK table in the privacy policy names seven SDKs and the binary ships more than twenty components
M1	MEDIUM	Google Mobile Ads initialises at process start and no consent management platform exists in the binary
L1	LOW	PEGI 3 rating, a policy that requires parental consent under 18 and no age gate found in the resources

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. Activation and audio destination not shown by the package.
C2	CRITICAL (file), HIGH (follow-up)	MEDIUM	No reply. Content of the licence call not shown.
C3	CRITICAL (file), HIGH (follow-up)	HIGH	No reply. Configuration read in 5.6.49.
H1	HIGH	MEDIUM	No reply. Three names and a personal mailbox.
H2	HIGH	MEDIUM	No reply. Listener and missing SMS permission read in 5.6.49.
H3	HIGH	MEDIUM	No reply. Key restrictions not visible from the package.
H4	HIGH	MEDIUM	No reply. SDK table as read on 23 August 2026.
M1	MEDIUM	MEDIUM	No reply. Not changed by any reply.
L1	LOW	LOW	No reply. Age gate not found in resources.

The findings file of 23 August 2026 labels C2 and C3 as Critical. The follow-up of 17 October 2026 calls the iwhop.cn call and the cleartext configuration high. The report uses the CVSS v4.0 band of each finding.

Subject & Operator Analysis

The Google Play developer field and the company_name string name Shenzhen Zhongwei Intelligent Technology Co., Ltd, Shenzhen, Guangdong, People’s Republic of China. The Play listing shows 5M+ downloads, the category Health & Fitness, PEGI 3 and the badges Contains ads and In-app purchases. The listing was last updated on 29 May 2026. The signing certificate and the privacy policy name two other entities (H1). No postal address, corporate website or Article 27 representative was found. The only contact is 936160908@qq.com. The bundled policy carries the ICP filing number Yue ICP Bei 2022087407 Hao-6.

The app supports devices from at least two Bluetooth chip vendors. The Play description names related equipment as Zhongke Lanxun and Jerry k11 series, which reads as a machine translation of a Jieli device family. The package carries both the Bluetrum and the Jieli SDK.

A controller outside the Union without a main establishment is not covered by the one-stop-shop mechanism. The Austrian Datenschutzbehörde receives the notice in copy and can receive complaints directly.

Architecture & Data Flow

Fere Fit is a native Android shell with seven classes*.dex files, 52 declared permissions, 12 ContentProviders and one BOOT_COMPLETED receiver. The arm64-v8a split carries two BLE chipset SDKs (Bluetrum libabpartool.so and the Jieli libjl family), AMap navigation, the iFlytek SparkChain runtime, Tencent Bugly crash reporting, the Weibo share SDK, ONNX Runtime, FFmpeg, the Opus codec and a ByteDance Zeus plugin stack with dedicated :bytelive, :push and :downloader processes.

The band talks to the app over Bluetooth Low Energy through custom GATT characteristics 0000ff12, 0000ff14 and 0000ff15. Notifications reach the band through NotificationMonitor (H2). The app calls first-party hosts under zwzn-tech.com and aitwszhongwei.mom, a licence endpoint at gateway.iwhop.cn (C2), a Google Cloud Translation endpoint (H3) and the third-party SDK hosts, among them at least five snssdk.com family analytics endpoints. Transport is plain HTTP wherever an http:// address is used, because the network security configuration allows it (C3). The data model behind the calls was not observed.

Engagement Summary

The notice REF FEREFIT-2026-R1 was sent on 23 August 2026 at 04:31 UTC from rfi.irfos@gmail.com to 936160908@qq.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried seven numbered findings, 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: Dedicated iFlytek speech recognition and generative text pipeline with its own audio recorder class sits behind RECORD_AUDIO, and the privacy policy never names the microphone

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 android.permission.RECORD_AUDIO. The dex files of version 5.6.49 carry the iFlytek SparkChain classes listed below, among them a dedicated capture class (com.iflytek.sparkchain.core.asr.AudioRecorder), real-time and file-based speech recognition, online text to speech and generative text output. The arm64-v8a split holds libSparkChain.so and libspark.so. The privacy policy that the app bundles as the string resource privacy_policy explains the purpose of the storage, camera, location, phone, address book and SMS permissions one by one. The words microphone, audio, voice and speech do not occur anywhere in that text. The package shows that the capability exists, that the permission backs it and that the policy is silent. Which in-app feature calls the recorder was not found in the string resources and may sit in a string table that was not fully enumerated or behind remote configuration. No SparkChain host name was isolated from the endpoint list, so the destination of any audio is not shown by the package. iFlytek has been on the US Department of Commerce Entity List since October 2019, which is relevant context for Chapter V of the GDPR and is not a finding about this app. Whether SparkChain here performs speaker identification or plain transcription was not traced.

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

Lcom/iflytek/sparkchain/core/asr/AudioRecorder;
Lcom/iflytek/sparkchain/core/asr/AudioRecorder$AudioDataCallback;
Lcom/iflytek/sparkchain/core/asr/ASR;
Lcom/iflytek/sparkchain/core/asr/AsrCallbacks;
Lcom/iflytek/sparkchain/core/rtasr/RTASR$a;       (real-time ASR)
Lcom/iflytek/sparkchain/core/raasr/RAASR$a;       (file-based ASR)
Lcom/iflytek/sparkchain/core/tts/OnlineTTS;
Lcom/iflytek/sparkchain/core/AiText$Holder;
Lcom/iflytek/sparkchain/core/AiUrl$Builder;
Lcom/iflytek/sparkchain/core/LLMBaseOutput;
Lcom/iflytek/sparkchain/utils/DeviceIdUtil;

lib/arm64-v8a/libSparkChain.so
lib/arm64-v8a/libspark.so
```

Impact: A person who wears the band to count steps and sleep has no way to learn from the operator's own text that a microphone-backed transcription and text-generation component ships in the app. If the component runs, the voice of the user and of people nearby is the data at stake, and the policy gives them no purpose, recipient or country to object to. The score reflects one user action to start a feature and a low confidentiality impact because activation and destination are not shown.

Fix: Name the microphone, the speech pipeline, the feature that triggers it, the recipient and

the country in the permission-purpose section, or remove the SDK and the permission if no feature uses them.

C2: Live licence authentication call to gateway.iwhop.cn, the infrastructure family of another operator, and an embedded com.wakeup.license SDK that no policy text names

---

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, HIGH in the follow-up of 17 October 2026

The dex files contain the URL https://gateway.iwhop.cn/gateway/user/license/api/v1/function/authentication and the Java classes com.wakeup.license.WkLicenseMgr, com.wakeup.license.WkLicenseMgr$activate$1 and com.wakeup.sdk.WkLicense with the Base64, BinaryDecoder and BinaryEncoder helpers. The iwhop.cn domain family is the one documented in the Wearfit Pro report of this programme (api-cluster.iwhop.cn, ad.iwhop.cn, health-monitor.iwhop.cn and others, re-read in the archived Wearfit Pro package on 23 August 2026) as belonging to Shenzhen Weike Technology Co., Ltd, the operator of Wearfit Pro (com.wakeup.howear) and WearFit2.0 (com.wakeup.wearfit2). Fere Fit is published by Shenzhen Zhongwei Intelligent Technology Co., Ltd and is signed with a different certificate (see H1). Neither the Play listing nor the bundled privacy policy names Weike, Wakeup or iwhop.cn. The package cannot show what the call carries, whether a licence key only, device identifiers or user data. The endpoint path reads as a licence or entitlement check and fits a hardware or software licensing arrangement between the two companies, a shared white-label vendor or a data-sharing arrangement. Static analysis cannot tell these apart. No request was sent to the host.

```
https://gateway.iwhop.cn/gateway/user/
https://gateway.iwhop.cn/gateway/user/license/api/v1/function/authentication

com/wakeup/license/WkLicenseMgr
com/wakeup/license/WkLicenseMgr$activate$1
com.wakeup.sdk.WkLicense
Lcom/wakeup/license/binary/Base64;
Lcom/wakeup/license/binary/BinaryDecoder;
Lcom/wakeup/license/binary/BinaryEncoder;
```

Operator infrastructure of Fere Fit itself, also from the dex strings: api.aitwszhongwei.mom, static.zwzn-tech.com, testapi.zwzn-tech.com. Two further host names with an explicit non-default port appear in the same pool and are listed in the Indicators section. Their use by this app was not exercised.

Impact: A user of a Zhongwei branded tracker is told about Zhongwei and nobody else. If the call carries more than a licence key, personal or health data would reach a company that the user cannot find in the policy and has never chosen. That is a recipient the policy hides, not a proven data flow.

Fix: Name Weike, Wakeup and iwhop.cn as recipients if they are recipients, state the role under Art. 26 or Art. 28, and list the data fields that cross the call.

C3: Cleartext traffic permitted for the whole app and no certificate pinning anywhere, on an app that handles health, location, call log and contacts data

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 CRITICAL on 23 August 2026, HIGH in the follow-up of 17 October 2026, rated HIGH by blast-radius escalation

res/xml/network_security_config.xml of version 5.6.49 consists of a base-config with cleartextTrafficPermitted set to true and nothing else. The app targets API level 36, where cleartext HTTP is refused by default, so this file switches that protection off for every host. The file holds no pin-set, no domain-scoped exception and no trust-anchor override, so nothing in the app pins a certificate. The dex strings list dozens of first-party and third-party hosts, among them the gateway.iwhop.cn licence call of C2. Whether a given endpoint is actually 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, GPS position, call log and contacts, it has more than 5 million installs on Google Play and the override covers every host including the licence call of C2.

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

Impact: The app is positioned to handle heart rate, sleep and blood pressure readings from the band, GPS position, call log, contacts and camera-triggered photos. A global cleartext allowance means that a plain HTTP request to any host, first-party or third-party, 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, 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.

H1: Three different company names in one binary and a personal QQ mailbox as the only contact

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 company_name string resource and the Google Play developer field read Shenzhen Zhongwei Intelligent Technology Co., Ltd. The first sentence of the bundled privacy policy speaks for a different company, Shenzhen Chuangzhiwei Technology Co., Ltd, which appears nowhere else in the binary. The signing certificate names CN=zhangguangyao, OU=duozhuo, O=duozhuo, a personal name and a third company name. No postal address was found in the resources or the dex strings. The only contact channel, identical on the live Play listing and in the dex strings, is the personal Tencent QQ mailbox 936160908@qq.com. No Article 27 representative in the Union is named anywhere. The bundled policy carries the ICP filing number Yue ICP Bei 2022087407 Hao-6. No privacy policy URL and no corporate website were found, and the domains zwzn-tech.com and aitwszhongwei.mom from the dex strings were not browsed. The paragraph may be copied boilerplate from a sibling storefront app in the same reseller family or a real failure to name the controller. The package does not decide between the two.

```
company_name string            "Shenzhen Zhongwei Intelligent Technology CO.,Ltd"
privacy_policy string (sentence 1)  "... the promise of Shenzhen Chuangzhiwei
    Technology Co., Ltd. (hereinafter referred to as "us") ..."
Play Store developer name       "SHENZHEN ZHONGWEI INTELLIGENT TECHNOLOGY CO.,Ltd"
Signing certificate DN          CN=zhangguangyao, OU=duozhuo, O=duozhuo, L=shenzhen,
    ST=guangdong, C=86
Contact (Play listing and dex)  936160908@qq.com
ICP filing (bundled policy)     Yue ICP Bei 2022087407 Hao-6
```

Impact: A person who wants to ask what the app holds about them, or have it deleted, cannot tell from the policy which of three companies to address and has only a private mailbox to write to. For a 5M+ install health tracker this is the entry point to every data subject right.

Fix: Name one controller with a postal address and a corporate contact in the policy and the Play listing, and appoint and name an Article 27 representative in the Union.

H2: The marketed SMS on the watch feature has no SMS receive permission behind it and runs through a notification listener that reads every app

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 registers com.czw.freefit.receiver.SmsReceiver for android.provider.Telephony.SMS_RECEIVED. A search of the 52 declared permissions found no READ_SMS, RECEIVE_SMS or SEND_SMS, so the system does not deliver that broadcast to the app. The component that can surface message content to the watch is com.czw.freefit.notification.NotificationMonitor, bound with BIND_NOTIFICATION_LISTENER_SERVICE. That interface is not scoped to SMS. While the listener is enabled by the user it exposes sender, preview text and timing of the notifications of every other app. The Play description lists Send and Receive SMS directly from your smartwatch as a key feature, and the bundled policy explains an SMS permission in the sense of standard Android SMS access. The same pattern is documented in the Wearfit Pro report of this programme. Whether the app forwards non-SMS notifications to the watch or off the device was not traced.

```
<receiver android:enabled="true" android:exported="false" android:name="com.czw.
    freefit.receiver.SmsReceiver">
    <intent-filter><action android:name="android.provider.Telephony.SMS_RECEIVED"/></
    intent-filter>
</receiver>

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

Impact: The listener can see messages from banking apps, one-time passcodes, chat apps and dating apps. A person who grants it for a text preview on the wrist hands over more than the feature description says.

Fix: State in the permission text and the policy that the feature uses notification access for all apps, restrict the listener to the apps the user selects and keep the content on the Bluetooth link.

H3: Two Google API keys in the dex files, one concatenated into a live Google Cloud Translation API request

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

classes5.dex holds the first key and the full request URL that uses it. classes4.dex holds a second key whose service was not isolated. It was found near Google Mobile Ads signal-name strings, which may or may not show its purpose. A key that is part of a billed Google Cloud REST call can be read by anyone who downloads the public APK and can be used for requests billed to the operator's project until it is restricted or rotated. The package cannot show the API restriction, the quota limit or any App Check setting. No request was sent with either key and neither key was tested.

```
classes5.dex   AIzaSyD7C3AP2BpR9z79jkIqR3QdIZsYjsdwZfY
classes5.dex   https://translation.googleapis.com/language/translate/v2?key=
    AIzaSyD7C3AP2BpR9z79jkIqR3QdIZsYjsdwZfY
classes4.dex   AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
```

Impact: If the key is unrestricted, its use against the operator's account is a matter of quota and billing, so the effect falls on availability of the translation feature and on the operator's cost, not on user data.

Fix: Restrict both keys by API and by package name with signing certificate, set quotas, enable App Check where supported and rotate the first key.

Component in the binary	Evidence	In policy table

H4: The SDK table in the privacy policy names seven SDKs and the binary ships more than twenty components

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 bundled policy carries a third-party SDK table that names Baidu Map, Tencent Mobile Analytics (com.tencent.stat), Tencent Bugly, QQ (com.tencent.open), WeChat (com.tencent.mm), Weibo (com.sina.weibo) and Google/Firebase. The dex files, resources and the native library inventory show the further components below. The manifest queries block also lists com.ss.android.ugc.aweme and its lite variant next to com.eg.android.AlipayGphone, which fits the Douyin SDK integration. Several of the missing components are the subject of C1 and C2. The table does not list them.

Component in the binary	Evidence	In policy table
AnyThink / TopOn ad mediation	com/anythink/*	No
ByteDance APM	com/bytedance/apm/*	No
ByteDance Douyin SDK	com/bytedance/android/dy/sdk/api/*	No
ByteDance live-streaming plugin process	com.byted.broadcast.lite (:bytelive)	No
Volcengine Zeus plugin loader	com/volcengine/zeus/*	No
Jieli BLE chipset SDK	com/jieli/jl_bt_ota, jl_rcsp, jl_filebrowse	No
Bluetrum BLE chipset SDK	com/bluetrum/abpartool/*	No
iFlytek SparkChain	com/iflytek/sparkchain/*	No
Wakeup licence SDK	com/wakeup/license/*, com.wakeup.sdk.*	No
AMap (AutoNavi) navigation	libAMapSDK_NAVI_v10_0_700.so	No
Tenmeter SDK, purpose not determined	com.tenmeter.smlib.*, ContentProviders	No
ONNX Runtime	onnxruntime	No
Google Mobile Ads / AdMob	MobileAdsInitProvider	Google/Firebase only

Impact: The user reads a short list and installs an app that talks to a long one. Several of the companies that are not listed are operators of advertising, live-streaming and speech services, so the user cannot judge who receives what.

Fix: List every component that receives or processes personal data with its purpose, its operator and its country, and remove components that no feature uses.

M1: Google Mobile Ads initialises at process start and no consent management platform exists in the binary

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 MEDIUM on 23 August 2026

The manifest declares com.google.android.gms.ads.MobileAdsInitProvider with initOrder 100 and authority com.czw.freefit.mobileadsinitprovider. It is the only ContentProvider in the manifest with an explicit initOrder, so it runs when the process is created and before application code can show a consent screen. A search of the strings.xml and the manifest for OneTrust, Didomi, Usercentrics and IABTCF returned no match. Which identifiers the ad SDK reads at start-up and whether it sends them before a choice was not measured. The Play listing carries the Contains ads badge.

```
<provider android:authorities="com.czw.freefit.mobileadsinitprovider" android:exported
    ="false" android:initOrder="100" android:name="com.google.android.gms.ads.
    MobileAdsInitProvider"/>
```

Impact: Advertising identifiers on a health tracker can be read before the person has made a choice, which links the use of a body-worn health product with an advertising profile.

Fix: Delay ad SDK initialisation until a recorded consent decision and add a consent management platform.

L1: PEGI 3 rating, a policy that requires parental consent under 18 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 LOW on 23 August 2026

The Play listing carries PEGI 3. The bundled policy says: We attach great importance to the protection of minors' personal information. If you are a minor under the age of 18, you should obtain the written consent of your parent or legal guardian before using the service. No date-of-birth field, age gate string or parental consent string was found in strings.xml. The decode covered resources and not the bytecode, so an age gate implemented in code without a resource string would not appear. The absence is therefore not asserted.

```
Google Play content rating: PEGI 3
Policy: "If you are a minor under the age of 18, you should obtain the written consent
     of your parent or legal guardian before using the service."
```

Impact: A child can install a product that is rated for everyone and that can read notifications and, if the speech pipeline runs, the microphone.

Fix: Align the rating and the policy, and add an age gate with a parental consent path or state that the app is for adults.

Impact Analysis

The people affected are the users of a 5M+ install health and fitness companion. They put a band on the wrist, grant Bluetooth, location, phone, contacts, camera and notification access, and trust the product with sleep, heart rate and blood pressure data. Some are minors, since the Play rating is PEGI 3.

The weight of the case sits on three points. The speech stack behind RECORD_AUDIO (C1) would put the voice of users and of nearby people into a pipeline that no policy text describes. The licence call to another company's backend (C2) adds a recipient the user cannot find. The global cleartext allowance (C3) removes the transport protection that the platform sets by default for every host the app talks to.

What the package shows is configuration and capability. No audio, health reading or personal field 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. The ad SDK initialises at process creation before any choice (M1).

Step 2, pairing: the user grants Bluetooth, location, phone, contacts, camera and notification access. The notification listener sees every app (H2).

Step 3, operation: the app calls first-party hosts, the licence endpoint of another operator (C2) and third-party SDK hosts, over a configuration that permits plain HTTP (C3). The SDK table in the policy names seven of more than twenty components (H4).

Step 4, voice: the SparkChain recorder class is present behind RECORD_AUDIO and the policy is silent (C1). The trigger and the destination are not shown.

Step 5, rights: a person who wants access or deletion finds three company names and a personal mailbox (H1).

Shared Chipset SDK Fingerprint and Cluster

Fere Fit ships the Bluetrum abpartool SDK. A class-level comparison against the archived Wearfit Pro package on 23 August 2026 found the same three class names (Lcom/bluetrum/abpartool/ParTool, Lcom/bluetrum/abpartool/R and Lcom/bluetrum/abpartool/utils/ImageUtils) and the same three custom GATT characteristic UUIDs. The same namespace is documented in the HryFine report of this programme. The WearFit2.0 link rests on that report and was not re-read here. Fere Fit differs from the three earlier members in two ways. It is published by another company and signed with another certificate, and it calls the Wakeup licence endpoint and embeds the Wakeup licence SDK (C2). That is a cross-company link at the infrastructure level.

```
Fere Fit signing cert SHA-1    46cc7496de6997085003d5cea12ded0bba209086
Fere Fit signing cert SHA-256  1
    b3ccfbae9a2aaffadd540f513469c3517f504c4d0ff305a87bb8c3b885cc555
Signing DN                     CN=zhangguangyao, OU=duozhuo, O=duozhuo, L=shenzhen, ST
    =guangdong, C=86
BLE vendor SDK                 com.bluetrum.abpartool (Java), lib/arm64-v8a/
    libabpartool.so
Second BLE vendor SDK          com.jieli.jl_bt_ota, jl_rcsp, jl_filebrowse
GATT characteristics           0000ff12-0000-1000-8000-00805f9b34fb
                               0000ff14-0000-1000-8000-00805f9b34fb
                               0000ff15-0000-1000-8000-00805f9b34fb
Licence SDK                    com.wakeup.license, com.wakeup.sdk.WkLicense
```

The signing certificate fingerprint was reproduced with apksigner and matched the value shown on the mirror page. Two open leads from the same pass are recorded and not asserted. The hosts elder.zjjxsoft.com:31000 and oversea.child.zjjxsoft.com:31000 appear in the dex strings and the pair of names suggests a backend module used for elder-care and child-monitoring products. Their use by this app was not corroborated. The Jieli family may form a sub-cluster of its own among white-label apps of this programme.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2, H1, H2 and M1.

Article 5(1)(b), purpose limitation: engaged by C2.

Article 5(1)(c), data minimisation: engaged by L1.

Article 6(1): engaged by H2 and M1.

Article 7(1), conditions for consent: engaged by M1.

Article 8, children: engaged by L1.

Article 9: engaged by C1 and H2 as open questions about voice and notification content. No special category processing is asserted.

Article 12(1) and Article 13(1)(a): engaged by H1. Article 13(1)(c) is engaged by C1 and Article 13(1)(e) by C2 and H4. Article 14 is engaged by H4.

Articles 26 and 28: engaged by C2 as an open question on the role of the two companies.

Article 27: engaged by H1. No representative is named.

Article 32(1)(a) and (b): engaged by C3 and H3. Article 25 is engaged by C3.

Articles 44 and 46: engaged by C1 as an open question on the destination of audio. Both the operator and the licence host are in the People's Republic of China according to the evidence above, which multiplies the recipients and does not create a further transfer.

Platform Accountability & DSA

The Google Play listing carries the badges Contains ads and In-app purchases and a Data Safety declaration that the report read on 23 August 2026 for the account deletion statement. The declaration was not compared field by field with the binary. A deletion path is described in the policy and in the Data Safety panel.

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

Regulatory & Legal Landscape

Shenzhen Zhongwei Intelligent Technology Co., Ltd 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 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 and 32 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 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.czw.freefit
Version            5.6.49 (versionCode 849), minSdk 24, targetSdk 36, compileSdk 36
XAPK SHA-256       8ebcc421ea2b45dc63b7823c595e230fc6527efdd6a84a594daf023e2e80f03b
base APK SHA-256   d6bdb810c0cfc4bce4fae0cb126c3f0e086f8f1074a19eb52d58db7e2f9b4c85
arm64 split SHA-256 59c30379b72fa2aa2774f1c79bece80f68b0637022ace1ca60e0c7c673596f2e
Signing cert SHA-1   46cc7496de6997085003d5cea12ded0bba209086
Signing cert SHA-256 1b3ccfbae9a2aaffadd540f513469c3517f504c4d0ff305a87bb8c3b885cc555
Audit device       none, the app was not installed
Acquisition        APKPure mirror (d.apkpure.com), versionCode 849, 2026-08-23
```

```
Google API key 1   AIzaSyD7C3AP2BpR9z79jkIqR3QdIZsYjsdwZfY   (classes5.dex)
Google API key 2   AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE   (classes4.dex)
Translation URL    https://translation.googleapis.com/language/translate/v2?key=
    AIzaSyD7C3AP2BpR9z79jkIqR3QdIZsYjsdwZfY
Licence URL        https://gateway.iwhop.cn/gateway/user/license/api/v1/function/
    authentication
First-party hosts  api.aitwszhongwei.mom, static.zwzn-tech.com, testapi.zwzn-tech.com
Open-lead hosts    elder.zjjxsoft.com:31000, oversea.child.zjjxsoft.com:31000
Contact            936160908@qq.com
ICP filing         Yue ICP Bei 2022087407 Hao-6
```

```
C1  AndroidManifest.xml (RECORD_AUDIO), classes*.dex (com/iflytek/sparkchain), arm64
    split (libSparkChain.so, libspark.so), strings.xml privacy_policy
C2  classes*.dex (gateway.iwhop.cn, com/wakeup/license, com.wakeup.sdk.WkLicense, com/
    bluetrum/abpartool)
C3  res/xml/network_security_config.xml
H1  strings.xml (company_name, privacy_policy), signing certificate, Google Play
    listing
H2  AndroidManifest.xml (SmsReceiver, NotificationMonitor, permission list)
H3  classes4.dex, classes5.dex
H4  strings.xml privacy_policy SDK table against classes*.dex and lib/arm64-v8a
M1  AndroidManifest.xml (MobileAdsInitProvider)
L1  Google Play listing, strings.xml privacy_policy
```

Reproduction: obtain com.czw.freefit 5.6.49 (849), check the SHA-256 values above, decode the manifest and resources with apktool and extract the dex string pools with strings. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF FEREFIT-2026-R1 at 04:31 UTC to 936160908@qq.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Seven findings, three questions, response requested within 30 days.

2026-09-12 Follow-up to 936160908@qq.com at 16:46 UTC, 20 days after the notice. It restated the findings and asked three questions on the missing microphone purpose, the controller under Art. 4(7) and the transfer to Google Cloud Translation and iFlytek under Art. 44 to 49, with answers due on 26 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:02 UTC, 35 days before publication, with the three questions reframed on the audio path, the controller and the iwhop.cn call.

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 real, detailed privacy policy is bundled in the app and is not a placeholder. It walks through the data categories, gives a per-permission purpose explanation for six permissions and names a third-party SDK table. The operator is traceable through an ICP filing, Yue ICP Bei 2022087407 Hao-6, and is not an anonymous registration. In-app purchases run through standard Google Play Billing and the package holds no third-party payment SDK. The policy describes that data can be deleted on request and the Data Safety declaration says the same.

Residual Risk & Recommendations

Open at the date of publication: all nine findings. The operator has not replied and the build analysed is version 5.6.49 of 29 May 2026. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, remove the global cleartext override and pin the first-party hosts (C3). Second, name the microphone and the speech pipeline in the policy with feature, recipient and country, or remove them (C1). Third, state the relationship with Shenzhen Weike Technology and the data fields behind the iwhop.cn call (C2). Fourth, name one controller with a postal address, a corporate contact and an Article 27 representative (H1). Fifth, restrict the Google keys, complete the SDK list, scope the SMS feature, gate ad SDKs on consent and add an age gate (H2 to L1).

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. 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 FEREFIT-2026-R1.