Security & Privacy Disclosure, Final Report

Lefun Health for Android (com.tjd.tjdmainS2)

Blood glucose and menstrual cycle data behind a cleartext and user certificate configuration, an ad and Chinese vendor stack that builds before consent, and no reply since the notice.

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

Target	Shenzhen Tengjinda Information Technology Co., Ltd (Lefun Health)
Versions Audited	2.9.8 / versionCode 2026073017 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	12: 2 High, 7 Medium, 3 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`eb7a58ef1f6d6fe454a614205a49f1b3eba564d2859753e1d46353d072d1cf22`

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 7

6.1 C1: Firebase, Google Mobile Ads, Huawei AGConnect, Huawei ML Kit and Vungle construct at process start, before the consent dialog can show 7

6.2 C2: Cleartext traffic permitted for the whole app, user-installed certificate authorities trusted app-wide with overridePins, and no pin-set 8

6.3 H1: At least eight Chinese data collectors are compiled in with live endpoints, and the English policy names no transfer mechanism, no EU representative and does not mention the GDPR 9

6.4 H2: SMS, call log and contacts are read and pushed to the watch, which processes data about people who never installed the app 10

6.5 H3: A system-wide notification listener whose own strings name WeChat and SMS as content that the watch takes over 11

6.6 H4: Blood glucose, blood pressure, uric acid, blood lipids and menstrual cycle data are processed, and the policy states no Article 9 basis 12

6.7 H5: A microphone based AI agent chat module with an iFlytek speech pipeline sits inside a health tracking app 13

6.8 M1: A shake to take a photo remote shutter from the paired watch is built into the camera permission 14

6.9 M2: An AppKey and an AppSecret for the carrier number verification service and an opaque ISP-Config blob are shipped in the manifest 14

6.10 M3: The Firebase project, Google API key, storage bucket and AdMob application ID are hardcoded in the resources 15

6.11 M4: The Eclipse Paho MqttService is exported without a protecting permission 15

6.12 M5: Everyone rating and a policy that sets the minor threshold at 14 for every user 16

7 Impact Analysis 16

8 The Complete Chain 17

9 Chipset SDK Cluster and Fingerprint Keys 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 22

16 Residual Risk & Recommendations 22

Executive Summary

Lefun Health is a companion app for Bluetooth watches and bands published under the developer name TENG JINDA. The operator named in its own privacy policy is Shenzhen Tengjinda Information Technology Co., Ltd ([redacted]), Baoan District, Shenzhen, People's Republic of China. The Google Play listing is rated Everyone and shows 190,424 ratings. A mirror listing gives more than 10 million installs. On 23 August 2026 RFI-IRFOS sent a notice with REF LEFUNHEALTH-2026-R1 to the only contact address, app@ss-tjd.com, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 2.9.8 shows a network security configuration that permits cleartext for the whole app and accepts user-installed certificate authorities for every connection, in an app that handles blood glucose, blood pressure, uric acid, blood lipids and menstrual cycle data (C2, H4). Five SDK providers construct at process start before the consent dialog can show (C1). At least eight Chinese vendors are compiled in with live endpoints, and the English policy never mentions the GDPR, a transfer mechanism or an EU representative (H1). SMS, call log and contacts are pushed to the watch (H2) and a notification listener names WeChat and SMS as content it takes over (H3). A microphone based AI agent module with an iFlytek pipeline sits in the same app (H5). An AppSecret for a carrier verification service is shipped in the manifest (M2).

The package also carries the Bluetrum abpartool and fota class names recorded for HryFine and Wearfit Pro in this programme, and in addition the Realsil and Jieli chipset SDKs, which fits a white label app built for several watch vendors. A reassessment by CVSS v4.0 band puts two findings at High, seven at Medium and three at Low. Both Critical labels and four of the five High labels disclosed on 23 August 2026 move down because the package shows capability and configuration and not runtime behaviour. H4 stays High through a stated blast-radius escalation.

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 2.9.8 (versionCode 2026073017), an APK of 78,410,967 bytes obtained from the APKPure content delivery host and checked against the package name, the developer name TENG JINDA and the developer URL http://www.sz-tjd.com on the live Google Play listing. Work done: manifest and resource decode (apktool, no source decode) and string-pool extraction across the eight classes*.dex files. The package holds no native library. The live Google Play listing and the operator's English 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. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	MEDIUM	Firebase, Google Mobile Ads, Huawei AGConnect, Huawei ML Kit and Vungle construct at process start, before the consent dialog can show
C2	HIGH	Cleartext traffic permitted for the whole app, user-installed certificate authorities trusted app-wide with overridePins, and no pin-set
H1	MEDIUM	At least eight Chinese data collectors are compiled in with live endpoints, and the English policy names no transfer mechanism, no EU representative and does not mention the GDPR
H2	MEDIUM	SMS, call log and contacts are read and pushed to the watch, which processes data about people who never installed the app
H3	MEDIUM	A system-wide notification listener whose own strings name WeChat and SMS as content that the watch takes over
H4	HIGH	Blood glucose, blood pressure, uric acid, blood lipids and menstrual cycle data are processed, and the policy states no Article 9 basis
H5	MEDIUM	A microphone based AI agent chat module with an iFlytek speech pipeline sits inside a health tracking app
M1	LOW	A shake to take a photo remote shutter from the paired watch is built into the camera permission
M2	MEDIUM	An AppKey and an AppSecret for the carrier number verification service and an opaque ISP-Config blob are shipped in the manifest
M3	MEDIUM	The Firebase project, Google API key, storage bucket and AdMob application ID are hardcoded in the resources
M4	LOW	The Eclipse Paho MqttService is exported without a protecting permission
M5	LOW	Everyone rating and a policy that sets the minor threshold at 14 for every user

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Network activity before consent not shown.
C2	CRITICAL	HIGH	No reply. Configuration read in 2.9.8, endpoint use not tested.
H1	HIGH	MEDIUM	No reply. Data reaching each vendor not shown.
H2	HIGH	MEDIUM	No reply. Onward transmission not shown.
H3	HIGH	MEDIUM	No reply. Onward transmission not shown.
H4	HIGH	HIGH	No reply. Features and policy read, no value observed in transit.
H5	HIGH	MEDIUM	No reply. Voice destination not shown.
M1	MEDIUM	LOW	No reply. Trigger origin not shown.
M2	MEDIUM	MEDIUM	No reply. Authorisation scope not shown.
M3	MEDIUM	MEDIUM	No reply. Key restrictions and rules not visible from the package.
M4	MEDIUM	LOW	No reply. Effect of an outside bind not shown.
M5	MEDIUM	LOW	No reply. Age gate not found in resources.

The findings file of 23 August 2026 labels C1 and C2 as Critical, H1 to H5 as High and M1 to M5 as Medium. The report uses the CVSS v4.0 band of each finding. H4 stays High through a blast-radius escalation that the finding states.

Subject & Operator Analysis

The operator named in the live English privacy policy is Shenzhen Tengjinda Information Technology Co., Ltd ([redacted]), Room A607, Donglian Building, Entrepreneurial Road, Dalang Community, Xin'an Street, Baoan District, Shenzhen City, Guangdong. The Play developer name is TENG JINDA with the URL http://www.sz-tjd.com. The signing certificate reads CN=http://www.sz-tjd.com/, OU=tjdSmart, O=Shenzhen TJD Info Technology Co.Ltd, L=shenzhen, ST=guangdong, C=CN. The only contact is app@ss-tjd.com. No phone number, Data Protection Officer or Article 27 representative appears in the package or the policy.

The policy was updated on 6 March 2025 with an effective date of 6 May 2024. It refers twice to a LeDong Health Life account, a product name other than the app. This reads as a template leftover and suggests that the operator or a close affiliate runs a second branded product from the same legal text. A game portal string from the bundled Tenmeter SDK refers to a Shimi membership. Its origin is open.

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

Lefun Health is a native Android app with eight classes*.dex files and no native library. All chipset vendor SDKs are Java or Kotlin class packages. The app drives watches over Bluetooth Low Energy through three vendor stacks, Bluetrum (abpartool and fota), Realsil or Realtek (91 string hits) and Jieli (34 hits). Its own device class com/tjd/common/storage/model/device/DeviceModel has six inner variants.

Phone events reach the watch through the SMS, call log and contacts permissions (H2) and the notification listener NotifyService (H3). Health screens sit under com/tjd/feature/health (H4). The AI module sits under com/tjd/feature/ai (H5). The first-party backend hosts in the strings are api-cluster.sz-tjd.com, api-cluster.ss-tjd.com and aigc.sz-tjd.com. Third-party endpoints are listed in H1. Firebase, AdMob, Vungle, InMobi, Mintegral, Pangle, Huawei AGConnect and ML Kit are bundled (C1). Transport permits cleartext and user certificate authorities (C2). The data model behind the calls was not observed.

Engagement Summary

The notice REF LEFUNHEALTH-2026-R1 was sent on 23 August 2026 at 00:08 UTC from rfi.irfos@gmail.com to app@ss-tjd.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried two critical findings, five high findings, the cluster finding, a statement of what the app does well and three questions. A follow-up of 12 September 2026 restated the findings and asked the three questions with an answer date of 19 September 2026. A second follow-up of 17 October 2026 came from security@rfi-irfos.com under the subject 35 days to publication: Lefun Health. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: Firebase, Google Mobile Ads, Huawei AGConnect, Huawei ML Kit and Vungle construct at process start, before the consent dialog can show

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

AndroidManifest.xml of version 2.9.8 registers five ContentProviders that Android creates when the process starts and before any activity. FirebaseInitProvider is directBootAware with initOrder 100, so it can run before the device is unlocked. MobileAdsInitProvider also has initOrder 100. The Huawei AGConnect and ML Kit providers and the Vungle provider carry no initOrder and also run at application creation. The app does show a first-run privacy dialog (privacy_permissions_tip_content) and bundles the Google User Messaging Platform (ConsentInformation and the IABTCF_CmpSdkID, IABTCF_gdprApplies and IABTCF_TCString keys). A consent platform decides when a dialog is shown and not when these providers construct. Whether any network call or identifier read follows before consent is a code path question and is UNVERIFIED.

```
<provider android:authorities="com.tjd.tjdmainS2.firebaseinitprovider" android:
    directBootAware="true" android:exported="false" android:initOrder="100" android:
    name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.tjd.tjdmainS2.mobileadsinitprovider" android:
    exported="false" android:initOrder="100" android:name="com.google.android.gms.ads.
    MobileAdsInitProvider"/>
<provider android:authorities="com.tjd.tjdmainS2.vungle-provider" android:exported="
    false" android:name="com.vungle.warren.utility.VungleProvider"/>
<provider android:authorities="com.tjd.tjdmainS2.MLInitializerProvider" android:
    exported="false" android:name="com.huawei.hms.mlsdk.common.provider.
    MLInitializerProvider"/>
<provider android:authorities="com.tjd.tjdmainS2.AGCInitializeProvider" android:
    exported="false" android:name="com.huawei.agconnect.core.provider.
    AGConnectInitializeProvider"/>
```

Class package families present at string pool depth in the dex files include Firebase, Google Mobile Ads, Vungle, InMobi, Mintegral (262 hits), Pangle (30 hits), Tencent (143 hits), Huawei HMS and AGConnect (397 hits), Umeng (238 hits), Alipay (263 hits), the Alibaba one-click login stack (271 hits), China Mobile SSO (41 hits) and iFlytek (23 hits).

Impact: A person who opens an app that tracks blood glucose and menstrual cycles for the first time has an ad, analytics and Chinese vendor SDK stack constructed before they have tapped anything. The consent platform changes the moment a dialog appears and does not change when these objects are built.

Fix: Delay SDK initialisation until a recorded consent decision, remove the providers that the product does not need and document which SDK may make a network call before consent.

C2: Cleartext traffic permitted for the whole app, user-installed certificate authorities trusted app-wide with overridePins, and no pin-set

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2 (CVSS-B), disclosed as CRITICAL on 23 August 2026

res/xml/network_security_config.xml has one base-config with cleartextTrafficPermitted set to true and trust anchors for both system and user certificates, each with overridePins set to true. The file has no domain scoping and no pin-set. overridePins tells the platform that certificates from that anchor are exempt from pins declared in the configuration. Since the file declares no pin-set, the flag has no pin to override here, and what the file shows is that user-installed certificate authorities are accepted for every connection, next to a global cleartext allowance. The app targets API level 35, where the platform default refuses cleartext and refuses user authorities for HTTPS. Which endpoints are called over plain HTTP was not tested.

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

The manifest requests READ_SMS, RECEIVE_SMS, READ_CALL_LOG, READ_CONTACTS, location including background location, CAMERA and RECORD_AUDIO, and the dex files hold screens for blood pressure, blood oxygen, blood glucose, uric acid, blood lipids, body temperature and menstrual cycle (H4).

Impact: A person who logs blood glucose, blood pressure or a menstrual cycle in this app uses a transport configuration that allows plain HTTP and accepts any certificate authority that someone installed on the phone. On a hostile network or a phone with an attacker-installed certificate, readings and account traffic can be read or changed.

Fix: Remove the cleartext allowance and the user trust anchor from the base-config, scope any exception to named hosts, add a pin-set for first-party hosts and test every endpoint for HTTPS.

H1: At least eight Chinese data collectors are compiled in with live endpoints, and the English policy names no transfer mechanism, no EU representative and does not mention the GDPR

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 dex string pool holds class packages of Huawei (397 hits), the Alibaba number verification stack (271), Alipay (263), Mintegral (262), Umeng (238), Tencent (143), China Mobile SSO (41), ByteDance and Pangle (30), iFlytek (23) and Alibaba AliAgent (8). Literal endpoint hosts are in the strings, among them alogsus.umeng.com, alogus.umeng.com, ai.login.umeng.com, api.weixin.qq.com, appsupport.qq.com, imgcache.qq.com, h.trace.qq.com, loggw-exsdk.alipay.com, log.wechatpay.cn, log.iflytek.com/log, logconf.iflytek.com/hotupdate, dypnsapi-dualstack.aliyuncs.com, iot-auth.cn-shanghai.aliyuncs.com and api16-access-sg.pangle.io. The Alibaba verification SDK contains the functions PreLoginResultListener, accelerateLoginPage, checkEnvAvailable, getLoginToken and clearCUCCPreLoginCount, the usual structure of a carrier number pre-fetch. Whether the build calls checkEnvAvailable before or after the consent dialog is UNVERIFIED. The English policy of the operator runs to about 90 KB and contains none of the words GDPR, European or representative and names no standard contractual clause.

```
Lcom/huawei/*        397   Lcom/mobile/auth/*    271   Lcom/alipay/sdk/*   263
Lcom/mbridge/msdk/*  262    Lcom/umeng/*         238   Lcom/tencent/*      143
Lcom/cmic/sso/*       41    Lcom/bytedance/sdk/*  30   Lcom/iflytek/*       23
Lcom/alibaba/*         8

alogsus.umeng.com   alogus.umeng.com   ai.login.umeng.com
api.weixin.qq.com   appsupport.qq.com  imgcache.qq.com   h.trace.qq.com
loggw-exsdk.alipay.com   log.wechatpay.cn
log.iflytek.com/log   logconf.iflytek.com/hotupdate
dypnsapi-dualstack.aliyuncs.com   iot-auth.cn-shanghai.aliyuncs.com
api16-access-sg.pangle.io
beian.miit.gov.cn   beian.cac.gov.cn
```

Impact: The user of a health tracker is told nothing about where the data goes. If personal data reaches these vendors, it leaves the Union without any safeguard that the policy names, and the user has no EU contact to turn to.

Fix: Name every recipient and country, state the Chapter V transfer mechanism, appoint and name an Article 27 representative and complete a data protection impact assessment.

H2: SMS, call log and contacts are read and pushed to the watch, which processes data about people who never installed the 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 declares READ_SMS, RECEIVE_SMS, READ_CALL_LOG, PROCESS_OUTGOING_CALLS and READ_CONTACTS. The permission purpose strings say that the data is used to sync contacts and to push call and SMS alerts to the device. The feature is disclosed by the operator in its own words. The data concerns every contact in the address book and every sender and caller, none of whom installed the app. The app also has an account and cloud sync architecture with login, membership and cross-device functions, so a backend path is a live question, and whether content leaves the phone beyond the Bluetooth hop is UNVERIFIED.

```
<string name="permission_name_calllog_info">Call push (alert).</string>
<string name="permission_name_contacts_info">Sync contacts, push calls (alerts)</
    string>
<string name="permission_name_sms_info">SMS push (alert)</string>
<string name="permission_name_phone_info">Call push (alert).</string>

<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
```

Impact: The people who write to or call the wearer are processed without any notice and cannot be informed, because they are not users of the product. Message senders and call counterparts can reveal relationships and routines.

Fix: Limit the data pushed to what the alert needs, state in the policy that content stays on the phone and the watch if that is the case, and remove permissions that no feature uses.

H3: A system-wide notification listener whose own strings name WeChat and SMS as content that the watch takes over

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.tjd.lelife.service.NotifyService with BIND_NOTIFICATION_LISTENER_SERVICE and exported set to true, which is the required form for a listener and is protected by the system permission. The point is scope. The listener sees sender, preview and timing of notifications of every app while the user keeps the access enabled. The strings device_content_dialog_content and dialog_notify_tip_content ask the user to enable it so that the device can take over notification messages (WeChat, SMS, etc.). Whether parsed content is stored, passed to an SDK or sent to the backend is UNVERIFIED.

```
<service android:enabled="true" android:exported="true" android:label="@string/
    app_name" android:name="com.tjd.lelife.service.NotifyService" android:permission="
    android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
    NotificationListenerService"/></intent-filter>
</service>

device_content_dialog_content: It is recommended to enable the notification permission
     of Lefun Health, so that the device can take over the notification message (
    WeChat, SMS, etc.)
```

Impact: A user who enables this access gives an app with ad and analytics SDKs a view onto the notifications of every other app, among them private chats, banking codes and health reminders.

Fix: Limit the listener to the apps the watch feature needs and state in the policy what is stored and what leaves the phone.

H4: Blood glucose, blood pressure, uric acid, blood lipids and menstrual cycle data are processed, and the policy states no Article 9 basis

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 23 August 2026, rated HIGH by blast-radius escalation

The dex files hold activities for blood fat, blood oxygen, blood pressure, blood sugar, heart rate, menstrual cycle (three activities), pressure, sleep, temperature and uric acid under com/tjd/feature/health/home. The operator's own policy lists the data under Health Data Management as sleep, heart rate, weight, blood oxygen, blood pressure, uric acid, blood lipids, menstrual cycle, blood sugar, temperature and other related measurement data. The English policy contains no reference to the GDPR and no Article 9(2) condition. The transport configuration of C2 applies to all of this data. The number of installs is 10M+ on a mirror listing that was not re-confirmed on the live Play page, and the live listing shows 190,424 ratings. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the data covers diabetes related readings, blood pressure and reproductive health of a user base with 190,424 ratings on Google Play, the policy names no Article 9(2) condition and the transport configuration of C2 applies to all of it.

```
com/tjd/feature/health/home/bloodFat/BloodFatActivity
com/tjd/feature/health/home/bloodOxygen/BloodOxygenActivity
com/tjd/feature/health/home/bloodPressure/BloodPressureActivity
com/tjd/feature/health/home/bloodSugar/BloodSugarActivity
com/tjd/feature/health/home/heartRate/HeartRateActivity
com/tjd/feature/health/home/menstrual/MenstrualActivity
com/tjd/feature/health/home/menstrual/MenstruationRecordActivity
com/tjd/feature/health/home/menstrual/MenstrualReminderActivity
com/tjd/feature/health/home/pressure/PressureActivity
com/tjd/feature/health/home/sleep/SleepActivity
com/tjd/feature/health/home/temperature/TemperatureActivity
com/tjd/feature/health/home/uricAcid/UricAcidActivity
```

Impact: People who manage diabetes, blood pressure or metabolic conditions with this watch, and people who log a menstrual cycle, hold data that carries a high risk of harm if it leaks or is misused. The same data travels over the configuration of C2.

Fix: State the Article 9(2) condition, obtain explicit consent in a readable form, name the recipients and complete a data protection impact assessment before processing health data at this scale.

H5: A microphone based AI agent chat module with an iFlytek speech pipeline sits inside a health tracking app

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 dex files hold the package com/tjd/feature/ai with agent creation and list screens, AIChatActivity, AIVoiceHelp, AudioRecordingService, IflytekTts, InitIflytek and OpusConvertUtils. The Opus conversion is consistent with compressed voice transport over a network. The strings hold https://aigc.sz-tjd.com, an AI backend under the operator's own domain, and the iFlytek endpoints log.iflytek.com/log and logconf.iflytek.com/hotupdate. The permission purpose strings do not tie RECORD_AUDIO to this module. Whether recorded voice goes to iFlytek, to aigc.sz-tjd.com, to both or to neither, and whether health context enters the conversations, is UNVERIFIED.

```
com/tjd/feature/ai/agent/ui/CreateAgentActivity
com/tjd/feature/ai/agent/ui/HomeAgentListActivity
com/tjd/feature/ai/agent/ui/MyAgentListActivity
com/tjd/feature/ai/chat/AIChatActivity
com/tjd/feature/ai/chat/AIVoiceHelp
com/tjd/feature/ai/common/voice/AudioRecordingService
com/tjd/feature/ai/common/IflytekTts
com/tjd/feature/ai/common/InitIflytek
com/tjd/feature/ai/common/OpusConvertUtils

https://aigc.sz-tjd.com
https://log.iflytek.com/log
https://logconf.iflytek.com/hotupdate
```

Impact: A user who is managing a health condition with the app has a microphone capable chatbot in the same app and account. If the voice or the conversation reaches a speech vendor in China, the user and anyone talking nearby are exposed to a recipient that the policy does not describe.

Fix: Describe the AI module, its recipients and countries in the policy, separate it from the health data and make it an opt-in feature.

M1: A shake to take a photo remote shutter from the paired watch is built into the camera permission

LOW, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The permission purpose string for the camera reads Shake to take a photo (remote control), change avatar. A remote shutter triggered from the paired watch is therefore a feature that the operator states. The package does not show whether the trigger can come only from the Bluetooth connected watch or also from a network path. That question is UNVERIFIED.

```
<string name="permission_name_camera_info">Shake to take a photo (remote control),
    change avatar.</string>
```

Impact: A photo triggered from the wrist can capture whoever stands in front of the phone, who may not be the account holder.

Fix: State in the policy that the shutter works only from the paired watch and show the camera preview while it is armed.

M2: An AppKey and an AppSecret for the carrier number verification service and an opaque ISP-Config blob are shipped in the manifest

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

AndroidManifest.xml carries the meta-data entries YJYZ-AppKey and YJYZ-AppSecret, a MHttps flag and a long ISP-Config value. A value that is named AppSecret is meant to stay on a server and is not public by design, unlike a Firebase key. YJYZ plausibly abbreviates a carrier one-click verification service, consistent with the com.cmic.sso and com.mobile.auth stack of H1. The ISP-Config value was not decoded and is not plain base64. The authorisation that the secret grants and any restriction by address or request signing could not be tested from the package. Extractability is confirmed and exploitability is UNVERIFIED. The keys were not used.

```
<meta-data android:name="MHttps" android:value="yes"/>
<meta-data android:name="YJYZ-AppKey" android:value="5f18e5f0945b8"/>
<meta-data android:name="YJYZ-AppSecret" android:value="2
    a6262fe61281fcebf78a1696a8f5ed9"/>
<meta-data android:name="ISP-Config" android:value="(one value, wrapped here, see the
    Indicators section)"/>
```

Impact: A secret that anyone can read from a public package gives no protection. If the service accepts the pair, a third party could act under the operator’s account.

Fix: Rotate the AppSecret, move the verification call to a server and restrict the credentials by package and signature.

M3: The Firebase project, Google API key, storage bucket and AdMob application ID are hardcoded in the resources

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 MEDIUM on 23 August 2026

res/values/strings.xml holds the Firebase and Google identifiers listed below, and AndroidManifest.xml holds the AdMob application ID. Firebase keys are not secrets by design. The risk is quota exhaustion and billing abuse if the key is unrestricted, and open data if the Firebase Security Rules and Cloud Storage rules are not locked down. Those settings cannot be seen from the package and were not tested.

```
google_api_key                   AIzaSyC261UUfwL2g-HYniAECJjJ4U-PliZeupA
google_crash_reporting_api_key  AIzaSyC261UUfwL2g-HYniAECJjJ4U-PliZeupA
google_app_id                    1:665800392204:android:6d7f7165f0daa705ea3829
google_storage_bucket            lefun-health-1684317076784.appspot.com
project_id                       lefun-health-1684317076784
gcm_defaultSenderId              665800392204
default_web_client_id            665800392204-kgd7fpl8i72qg05bj0tujmn2pqljl3pc.apps.
    googleusercontent.com
com.google.android.gms.ads.APPLICATION_ID  ca-app-pub-9357120775872721~8402626166
```

Impact: The data of every user who syncs to the cloud depends on rules that the user cannot see and the operator has not described.

Fix: Restrict the key by package name and signature, check the Firebase Security Rules and the storage rules and remove unused identifiers.

M4: The Eclipse Paho MqttService is exported without a protecting permission

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026

AndroidManifest.xml declares org.eclipse.paho.android.service.MqttService with exported set to true and no android:permission attribute. Any other app on the same device can start or bind it. MQTT is a publish and subscribe channel and could carry commands, but what an outside binder can do with this service in this build cannot be seen without a bytecode and runtime pass. That is UNVERIFIED.

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

Impact: Another app on the phone may be able to interact with the app's message channel, with effects that depend on how the library is used.

Fix: Set exported to false unless an outside caller is needed or protect the service with a signature permission.

M5: Everyone rating and a policy that sets the minor threshold at 14 for every user

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 live Google Play listing carries the rating Everyone. The English policy defines children as persons under 14 and says that they may not create their own account without the consent of parents or guardians. Date of birth is a self reported profile field, and no age gate was found in the decompiled resources. The decode covered resources and not the bytecode, so the absence is not asserted for code. Art. 8(1) of the GDPR sets the age of digital consent at 16 and lets a Member State lower it, but not below 13, so the applicable age depends on the child's Member State. The policy applies 14 to every user.

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

Impact: A teenager can install a tracker with SMS, call log, health and microphone features that is rated for everyone, and the policy sets one age for all countries.

Fix: Align the rating with the feature set, apply the age of digital consent of each Member State and add an age gate with a parental consent path.

Impact Analysis

The people affected are the users of a health and fitness companion with a large installed base. They put a watch on the wrist, grant Bluetooth, location, SMS, call log, contacts, camera, microphone and notification access, and record blood glucose, blood pressure, uric acid, blood lipids, body temperature and menstrual cycles. Their contacts, callers and message senders are affected as well.

The weight of the case sits on three points. The transport configuration (C2) lets plain HTTP and user-installed certificate authorities apply to an app with diabetes related and reproductive health data (H4). The policy says nothing about the GDPR, a transfer mechanism or an EU representative while at least eight Chinese vendors are compiled in (H1). A microphone based AI chat module sits inside the health app (H5).

What the package shows is configuration and capability. No health reading, voice recording or personal field was observed leaving a device and the report asserts no such flow.

The Complete Chain

Step 1, install and first start: five SDK providers construct at process creation before the consent dialog can show (C1).

Step 2, consent: the app shows its own first-run dialog and a Google consent platform. The dialog text is a catch-all that covers personal information, account information, sports and health information and location.

Step 3, pairing and use: the user grants SMS, call log, contacts, notification, camera and microphone access. The watch receives callers, messages and notification content (H2, H3). Health screens record glucose, pressure and cycle data (H4).

Step 4, network: calls run under a configuration that permits cleartext and user certificate authorities (C2) towards first-party hosts and the vendors of H1. The AI module can record voice (H5) and a carrier verification SDK is present with an AppSecret in the manifest (M2).

Step 5, rights: a person who wants access or deletion finds one generic address, no phone number and no EU representative. The policy describes an account cancellation path.

Chipset SDK Cluster and Fingerprint Keys

Lefun Health carries the class names Lcom/bluetrum/abpartool/ParTool, Lcom/bluetrum/abpartool/R and Lcom/bluetrum/abpartool/utils/ImageUtils and the Bluetrum fota stack OtaManager, OtaDataProvider, OtaError, ABOtaManager and ABOta, 21 Lcom/bluetrum hits in all. The same namespace is recorded for HryFine and Wearfit Pro in the reports of this programme. The three apps are signed with different certificates and published by different companies, which fits a model in which each reseller signs its own build of a shared chipset reference SDK. Lefun Health goes further by bundling the Realsil or Realtek stack (GlobalGatt, RtkConfigure, BluetoothA2dpManager, SpecScanRecord, FirmwareLoaderX, the Spp and Usb DFU adapters and the bbpro protocol contracts) and the Jieli stack (bluetooth_connect, bmp_convert, jl_bt_ota, jl_fatfs and jl_rcsp). A white label app that drives hardware from three chip vendors is built for re-badging.

```
Signing cert SHA-256   86
    f77c9cd45d8c45c2faca64cfc1c4287fb960bff95d182351a945ef53ad9cea
Signing cert SHA-1     a5ae062f9f3783f8ca01f35df92fc37c12832054
Signing DN             CN=http://www.sz-tjd.com/, OU=tjdSmart, O=Shenzhen TJD Info
    Technology Co.Ltd, L=shenzhen, ST=guangdong, C=CN
BLE vendor SDKs        com.bluetrum.abpartool, com.bluetrum.fota, com.realsil.sdk, com
    .jieli.*
Device field names     device_model, product_id, device_vendor_id, firmware_version,
                       getVendorId, getVendorIdSource, getManufacturerSpecificData,
    getScanRecord
Template leftover      "LeDong Health Life account" (live English policy, two places)
```

Not shown: the numeric BLE manufacturer identifiers and GATT UUIDs, which are bytecode literals and were not extracted, and whether the first-party backend is shared with the HryFine or Wearfit Pro backends. The correlation holds at the chipset SDK layer and not at the backend layer.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H1 to H3 and M1 for the operator's own policy against its code.

Article 5(1)(b), purpose limitation: engaged by H5.

Article 5(1)(c), data minimisation: engaged by H3.

Article 5(1)(f) and Article 32(1)(a) and (b): engaged by C2, M2, M3 and M4.

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

Article 6(1) and Article 7(1): engaged by C1, H2 and H3.

Article 8: engaged by M5.

Article 9(1) and (2): engaged by H4. Article 9 is an open question for H5 and bystander photos in M1.

Article 12(1) and Article 13(1): engaged by H1.

Article 14: engaged by H2 for people in the address book and callers.

Article 25(1): engaged by C2, H3, M1, M3 and M5.

Article 27: no representative is named.

Articles 35, 44 and 46: engaged by H1, H4 and H5.

The policy is silent on Chapter V. The PRC location of the operator and the vendors is established by the policy address and the endpoint hosts and the data flows are not.

Platform Accountability & DSA

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about an inaccurate 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.

The Google Play listing was read on 23 August 2026 and shows the rating Everyone and a free app. The report did not compare a Data Safety declaration field by field with the binary. The policy describes an account cancellation path.

Regulatory & Legal Landscape

Shenzhen Tengjinda Information 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.tjd.tjdmainS2
Version            2.9.8 (versionCode 2026073017), minSdk 26, targetSdk 35, compileSdk
     35
APK size           78,410,967 bytes
APK SHA-256        eb7a58ef1f6d6fe454a614205a49f1b3eba564d2859753e1d46353d072d1cf22
Signing cert SHA-256 86f77c9cd45d8c45c2faca64cfc1c4287fb960bff95d182351a945ef53ad9cea
Signing cert SHA-1   a5ae062f9f3783f8ca01f35df92fc37c12832054
Audit device       none, the app was not installed
Acquisition        APKPure content delivery host (data.winudf.com), checked against
    the Google Play listing, 2026-08-23
```

```
google_api_key / google_crash_reporting_api_key   AIzaSyC261UUfwL2g-HYniAECJjJ4U-
    PliZeupA
google_app_id          1:665800392204:android:6d7f7165f0daa705ea3829
google_storage_bucket  lefun-health-1684317076784.appspot.com
project_id             lefun-health-1684317076784
gcm_defaultSenderId    665800392204
default_web_client_id  665800392204-kgd7fpl8i72qg05bj0tujmn2pqljl3pc.apps.
    googleusercontent.com
AdMob application ID   ca-app-pub-9357120775872721~8402626166
YJYZ-AppKey            5f18e5f0945b8
YJYZ-AppSecret         2a6262fe61281fcebf78a1696a8f5ed9
First-party hosts      api-cluster.sz-tjd.com, api-cluster.ss-tjd.com, aigc.sz-tjd.com
    , app.ss-tjd.com
Contact                app@ss-tjd.com
Policy                 https://app.ss-tjd.com/lelife_privacy_now_EN.html
```

```
GseBo/nfdVxy501ITcLIW3TjSEouMSfQBGwvz1fajSik9+XmsP0peNFlgKbgGW
Na+ta8a6QR8JHASKAGBvsvHMUfbZ5o97xTYdMRll71KBqilcoVkb3LaxHRHmU2
dSMa1BiTtG/PL5seBlZTPulagwlaM3Rdc5t6Pu/SCtH0X8nRUQynYUQdcCBvGN
nlJQEXowJzdiRlfEBJN/F9WR2YrZxkvccaRNCFt52pYitlOv68QnBamuvx42FQ
aDvwihyy2bb4CZUCIofvbDrZBv80fuJIBIhYV9lBlx5PaA6z/UpkUYmNgMspSY
wW1w4neNDvey73GQXfpmLKxv4y32jm9CmzvyXlnEYEfAf6ICz7B2E6vF032Ct7
G9mycuhM/F03TDgci7F7G9vqnbRWVhKZfDHF3uWJYsL3UpUZ7eirQY6i8wFBwg
JykLkiicp7/y/sbA7cowOXTaiW97jyaB7uEZsVq2KKjOxzHAcosJuqunHwVcKj
JPRU3o8fNhIXGcdk+ExsMbaFGKg8Fb/ShRuFBYMhTSYPXFItSN2dbfEs3KE
```

```
C1  AndroidManifest.xml (providers), classes*.dex (SDK packages, ump, IABTCF), res/
    values/strings.xml (privacy_permissions_tip_content)
C2  res/xml/network_security_config.xml
H1  classes*.dex (SDK packages and endpoint strings), English privacy policy
H2  AndroidManifest.xml (permissions), res/values/strings.xml (permission_name_*_info)
H3  AndroidManifest.xml (NotifyService), res/values/strings.xml (
    dialog_notify_tip_content)
H4  classes*.dex (com/tjd/feature/health), English privacy policy
H5  classes*.dex (com/tjd/feature/ai), endpoint strings
M1  res/values/strings.xml (permission_name_camera_info)
M2  AndroidManifest.xml (YJYZ and ISP-Config meta-data)
M3  res/values/strings.xml, AndroidManifest.xml
M4  AndroidManifest.xml (MqttService)
M5  Google Play listing, English privacy policy
```

Reproduction: obtain com.tjd.tjdmainS2 2.9.8 (2026073017), check the SHA-256 value 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 LEFUNHEALTH-2026-R1 at 00:08 UTC to app@ss-tjd.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Two critical and five high findings, the cluster finding and three questions.

2026-09-12 Follow-up to app@ss-tjd.com at 17:04 UTC. It restated the findings and asked three questions on the code path that holds back the SDK providers until consent, the transport configuration and the Chapter V basis, with answers due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:02 UTC, under the subject 35 days to publication: Lefun Health.

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 app disables adb backup of its private data (allowBackup false). It bundles the Google User Messaging Platform next to its own first-run dialog, which names the data categories in plain language. Every dangerous permission has its own purpose string in readable English. The English policy runs to about 90 KB with a per-feature table of purpose, data type, collection method and fields, and it discloses voice information, IMSI, OAID and the HarmonyOS ID. An account cancellation path is described. A string that names Amap has no matching compiled package, which reads as stale template text and not as an additional SDK.

Residual Risk & Recommendations

Open at the date of publication: all twelve findings. The operator has not replied and the build analysed is version 2.9.8. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, remove the cleartext allowance and the user trust anchor and pin first-party hosts (C2). Second, state the Article 9(2) basis and complete a data protection impact assessment for the health data (H4). Third, name every recipient and country, the Chapter V mechanism and an Article 27 representative (H1). Fourth, delay SDK initialisation until a recorded consent decision (C1). Fifth, limit the notification listener and the data pushed to the watch and explain the AI module with its recipients (H2, H3, H5). Sixth, rotate the AppSecret, restrict the Google key, review the Firebase rules, protect the MQTT service and align the rating and age handling (M1 to M5).

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 LEFUNHEALTH-2026-R1.