Security & Privacy Disclosure, Final Report

HryFine for Android (com.lianhezhuli.hyfit)

Advertising SDKs that start before consent and a global cleartext override on a blood glucose logging app with more than 50 million installs.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED 20 NOVEMBER 2026. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Shenzhen United Power Technology Co., Ltd. (HryFine)
Versions Audited	3.8.12 / versionCode 216 (Play update 2026-08-10, analysed 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	11: 2 High, 4 Medium, 5 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`a462666229d46dd20911159abd4b75f32912492e31caf85b6b017df7c0768e6f`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Findings 7
- 5.1 C1: Advertising, analytics and mediation SDKs that construct at process start, before any consent screen can render . . . 7
- 5.2 C2: Global cleartext traffic override without pinning on an app that logs blood glucose, blood pressure and SMS content . . . 8
- 5.3 H1: Chinese SDK cluster (ByteDance Pangle, Tencent Beacon, GDT and Cloud, Mintegral) named only in untranslated Chinese brand names . . . 9
- 5.4 H2: Contacts, call log and SMS content pushed to a second physical device . . . 10
- 5.5 H3: NotificationListenerService with system-wide notification access and a queries block that names eight messaging apps . . . 11
- 5.6 H4: Special category health data including blood glucose, blood pressure, blood oxygen, temperature and sleep . . . 12
- 5.7 M1: Remote camera trigger from the paired bracelet . . . 12
- 5.8 M2: Firebase and Google Maps keys and identifiers hardcoded . . . 13
- 5.9 M3: allowBackup is true and the FileProvider covers the whole external storage root . . . 14
- 5.10 M4: MessageService is exported without a protecting permission . . . 14
- 5.11 M5: PEGI 3 rating with no age gate and an advisory paragraph for minors under 18 . . . 15

6 Impact Analysis 15

7 Advertising and Analytics Stack 16

8 The Complete Chain 17

9 Shared Chipset SDK Fingerprint 17

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 18

12 Regulatory & Legal Landscape 19

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 21

Executive Summary

HryFine is the Android companion app of Bluetooth smartwatches and bracelets, published on Google Play by Shenzhen United Power Technology Co., Ltd. with more than 50 million downloads. It forwards calls, SMS and contacts to a bracelet and logs heart rate, blood pressure, blood oxygen, temperature, blood glucose and sleep. On 22 August 2026 RFI-IRFOS (ZVR 1015608684, GISA 39261441) disclosed eleven findings from a root level code analysis of version 3.8.12 under REF HRYFINE-2026-R1.

The two most serious findings are structural. At least seven ContentProviders of advertising and analytics SDKs run at process start, before any consent screen can render, and the dex files hold at least 15 advertising networks (C1). The network security configuration permits cleartext traffic for the whole application with no pinning, while the Google Play Data safety panel tells every installer that data is encrypted in transit (C2). The app bundles Google's consent SDK, so the problem of C1 is timing and not the absence of consent tooling.

Further findings cover a Chinese SDK cluster that the in-app text names only in untranslated Chinese brand names (H1), contacts, call log and SMS content pushed to a second device (H2), a notification listener that names eight messaging apps (H3), the glucose and other health data (H4) and five findings of lower rating on the camera trigger, hardcoded keys, backup and FileProvider scope, an unprotected exported service and the PEGI 3 rating.

The only contact channel found for the operator is a personal Gmail address. The notice went there and a follow-up with three written questions and a second reminder followed. As of 14 November 2026 no reply, acknowledgment or bounce has arrived. The publication date is 20 November 2026 and does not depend on a reply. A final APK diff before that date determines the state this report records.

Scope: Root level code analysis of the Google Play release 3.8.12 (versionCode 216): decoded manifest and resources, dex string-pool extraction across seven primary dex files and two embedded Audience Network dex files, native library inventory. Public listing and policy pages read by plain HTTP GET. No bytecode control-flow pass, no dynamic instrumentation, no traffic capture, no account, no backend call and no key test. Findings that depend on runtime behaviour are marked UNVERIFIED.

ID	Severity	Title
C1	HIGH	Advertising, analytics and mediation SDKs that construct at process start, before any consent screen can render
C2	HIGH	Global cleartext traffic override without pinning on an app that logs blood glucose, blood pressure and SMS content
H1	MEDIUM	Chinese SDK cluster (ByteDance Pangle, Tencent Beacon, GDT and Cloud, Mintegral) named only in untranslated Chinese brand names
H2	MEDIUM	Contacts, call log and SMS content pushed to a second physical device
H3	MEDIUM	NotificationListenerService with system-wide notification access and a queries block that names eight messaging apps
H4	MEDIUM	Special category health data including blood glucose, blood pressure, blood oxygen, temperature and sleep
M1	LOW	Remote camera trigger from the paired bracelet
M2	LOW	Firebase and Google Maps keys and identifiers hardcoded
M3	LOW	allowBackup is true and the FileProvider covers the whole external storage root
M4	LOW	MessageService is exported without a protecting permission
M5	LOW	PEGI 3 rating with no age gate and an advisory paragraph for minors under 18

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

The Disclosed column shows the label used in the first notice. The This report column shows the rating after the CVSS v4.0 reassessment in this report.

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Provider declarations are as recorded in version 3.8.12. Runtime gating is UNVERIFIED.
C2	CRITICAL	HIGH	No reply. Cleartext configuration as recorded.
H1	HIGH	MEDIUM	No reply. Presence of Amap and Umeng is UNVERIFIED.
H2	HIGH	MEDIUM	No reply. Off-device transmission is UNVERIFIED.
H3	HIGH	MEDIUM	No reply. Use of notification content is UNVERIFIED.
H4	HIGH	MEDIUM	No reply. Consent capture for health screens is UNVERIFIED.
M1	MEDIUM	LOW	No reply. Origin of the camera command is UNVERIFIED.
M2	MEDIUM	LOW	No reply. Key restrictions are not testable without third-party tests.
M3	MEDIUM	LOW	No reply. Backup rules are UNVERIFIED.
M4	MEDIUM	LOW	No reply. Behaviour of the exported service is UNVERIFIED.
M5	MEDIUM	LOW	No reply.

Subject & Operator Analysis

HryFine is the Android companion app of Bluetooth Low Energy smartwatches and bracelets, published on Google Play under the package com.lianhezhuli.hyfit. The Play listing shows more than 50 million downloads, a rating of 3.67 from 224,574 ratings, PEGI 3, the Contains ads badge, a last update on 10 August 2026 and the website http://www.lhzl666.com. The listing and independent mirror listings give the developer as Shenzhen United Power Technology Co., Ltd.

The developer entry names an address in the Hedong Second Industrial Village, Xin'an subdistrict, Bao'an, Shenzhen 518000, a Gmail address (hdtapp2016@gmail.com) and a mobile number. That Gmail address is the only contact channel found anywhere. The package is signed with the certificate subject CN=hy, OU=hy, O=huayan, L=sz, ST=gd, C=cn. Three brand strings therefore appear: Shenzhen United Power, the domain lhzl666 and the certificate name huayan, which points to an operator that runs several storefront names.

No data protection officer and no Art. 27 representative appear in the binary, the Play listing or the privacy policy at https://privacy.lhzl666.com/static/hryfine/privacypolicy_gp.html.

Architecture & Data Flow

HryFine is a native Android and Java app with seven primary dex files plus two embedded Meta Audience Network dex files, minSdkVersion 24 and targetSdkVersion 35. Its Bluetooth stack combines the Bluetrum abpartool SDK with the open-source Blessed GATT library. Health measurements flow from the bracelet over Bluetooth to the phone. Contacts, call and SMS data flow from the phone to the bracelet.

In parallel the app compiles in at least 15 advertising and mediation networks and three analytics or attribution stacks, listed in the next section. Their ContentProviders start with the process. Network access is governed by a base-config that permits cleartext for every host. Firebase (project hryfine-85cf2) and Google Maps are present, and Tencent and ByteDance endpoints appear as literal hosts in the dex.

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

Findings

C1: Advertising, analytics and mediation SDKs that construct at process start, before any consent screen can render

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), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the defect applies to every user on every cold start regardless of jurisdiction, spans more than 15 advertising networks including companies in China and Russia, and sits in an app that processes health data of 50 million installs. At least seven ContentProviders from Firebase, AppLovin, Vungle, Meta Audience Network, ironSource and Mintegral are declared in the manifest. Android runs ContentProviders during Application.onCreate, before any Activity. FirebaseInitProvider is also directBootAware. The dex files contain at least 15 ad and mediation networks and 3 analytics or attribution stacks.

```
<provider android:authorities="com.lianhezhuli.hyfit.firebaseinitprovider"
   android:directBootAware="true"
          android:exported="false" android:initOrder="100"
             android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.lianhezhuli.hyfit.applovininitprovider"
   android:exported="false"
          android:initOrder="101"
             android:name="com.applovin.sdk.AppLovinInitProvider"/>
<provider android:authorities="com.lianhezhuli.hyfit.vungle-provider"
   android:exported="false"
          android:initOrder="102" android:name="com.vungle.ads.VungleProvider"/>
AudienceNetworkContentProvider   FacebookInitProvider   IronsourceLifecycleProvider
   MBComponentLifecycleProvider
```

The app bundles the Google User Messaging Platform SDK (ConsentInformation, ConsentForm) and IAB TCF constants (IABTCF_CmpSdkID, IABConsent_SubjectToGDPR), so consent tooling exists. A bundled consent SDK does not show that the providers above wait for it. They construct their SDK objects at process start whether or not a consent dialog appears later. Whether the app code also holds back SDK network activity until a consent decision is UNVERIFIED because no code-path or runtime analysis was done.

The full SDK inventory is in the section on the advertising and analytics stack below. It includes companies in mainland China, Japan and Russia.

Impact: Every user of an app with 50 million installs, including people who log blood glucose, starts a process in which more than a dozen advertising companies are initialised before the user has seen a choice.

Fix: Gate every advertising and analytics provider behind the consent decision, for example by disabling the auto-init providers in the manifest and starting each SDK from code after consent. Document and test the gating against each network.

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

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), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the setting applies to the whole application and removes the platform default for an app with 50 million installs that processes Art. 9 health data including blood glucose, and the Play Data safety label contradicts it. res/xml/network_config.xml sets cleartextTrafficPermitted="true" in the base-config. The manifest references it through android:networkSecurityConfig. There is no domain-config and no pin-set anywhere in res/xml.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

With targetSdkVersion 35 Android denies cleartext by default. The app opts back in for the whole application. The configuration permits plaintext for any endpoint, present or future, without a code change. Which endpoints use plain HTTP today is UNVERIFIED because no traffic was captured.

The app requests READ_SMS, READ_CALL_LOG, READ_CONTACTS, ACCESS_FINE_LOCATION and CAMERA, and it drives dedicated screens for heart rate (HrMeasureActivity), blood pressure (BpMeasureActivity), blood oxygen (BoMeasureActivity), temperature (TempMeasureActivity), blood glucose (GluRecordActivity, GluInputActivity, HistoryGluActivity) and sleep. The Google Play Data safety panel states "Data is encrypted in transit."

Impact: A person who manages diabetes with this app logs glucose values over a connection that the app has told Android may run in plaintext, and the Play listing tells that person the opposite.

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

H1: Chinese SDK cluster (ByteDance Pangle, Tencent Beacon, GDT and Cloud, Mintegral) named only in untranslated Chinese brand 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)

The dex files hold thousands of class references for ByteDance (4,051), Tencent (4,834) and Mintegral (4,145 and 76) and native libraries for Pangle and ByteDance APM Insight. Literal endpoint hosts at Tencent and Pangle are present. The in-app privacy text names the SDKs with Chinese brand names and no English gloss.

```
Lcom/bytedance/adsdk/...  Lcom/bytedance/pag/...  Lcom/bytedance/pcc/...
   Lcom/pgl/ssdk/...      4,051 hits "Lcom/bytedance"
Lcom/tencent/beacon/...  Lcom/tencent/cos/...  Lcom/tencent/qcloud/...
   Lcom/qq/e/...            4,834 hits "Lcom/tencent"
Lcom/mbridge/msdk/...  Lcom/mintegral/msdk/...
   4,145 and 76 hits
libpglarmor.so  libbuffer_pgl.so  libfile_lock_pgl.so  libtt_ugen_layout.so
   libapminsighta.so  libapminsightb.so

otheve.beacon.qq.com  mqqeve.beacon.qq.com  othstr.beacon.qq.com  h.trace.qq.com
api16-access-sg.pangle.io  redirector.gvt1-cn.com
```

The policy strings user_privacy_content44 to 48 list the third-party SDK statements as Pangle (Chuanshanjia, ByteDance), Tencent GDT (Youliangtong), Amap (AutoNavi, Alibaba) and Umeng (Alibaba), each with a link, under the heading Third-party SDK privacy statement. Amap and Umeng are named in the text but no class package for either was found in this build, apart from a single attribution enum string for Umeng. The text therefore reads as a template that was not adapted to this build. Whether Amap or Umeng are present is UNVERIFIED. Which data each SDK sends from EU devices is also UNVERIFIED.

Personal data that reaches infrastructure of Tencent and ByteDance engages Chapter V of the GDPR. A transfer impact assessment has to address Art. 7 of the PRC National Intelligence Law, which obliges organisations to support national intelligence work. No Art. 46 mechanism is named in the policy material.

Impact: EU users meet a list of data recipients that is written in Chinese brand names without translation, so most of them cannot tell which companies receive their data or in which country.

Fix: Name every SDK vendor, its country and the Art. 46 safeguard in plain English, remove Amap and Umeng from the text if they are not in the build, and document a transfer impact assessment.

H2: Contacts, call log and SMS content pushed to a second physical device

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)

The in-app privacy notice describes reading the address book to send caller details to the bracelet, synchronising the address book and writing new contacts to the phone, reading missed calls and pushing new SMS to the bracelet. The manifest declares READ_CONTACTS, WRITE_CONTACTS, READ_CALL_LOG, READ_SMS and RECEIVE_SMS.

```
(2) Address book permissions: When a call comes in, read the contact's address book
   and send the corresponding information to the bracelet to remind the user,
   synchronize the address book and write the new contact to the phone.
(3) Call log permissions: When the app is connected to the bracelet, it reads missed
   calls and pushes the information to the bracelet to remind the user.
(4) Read SMS permission: When there is a new SMS, the SMS message will be pushed to
   the bracelet to remind the user.
```

The feature is disclosed and is common in this product class. The concern is the data subjects. The address book holds the details of every contact, and a call or message push involves the person who called or wrote. None of them installed HryFine or saw a consent screen. ContactActivity and SelectContactActivity manage which contacts are pushed. The app also has account and cloud architecture (AccountActivity, AccountBindActivity, ThirdPartyBindActivity), so whether address book, call or SMS content also reaches a backend beyond the Bluetooth link is UNVERIFIED.

Impact: Every person in the address book of a HryFine user, and every caller and texter, has their details processed without a notice reaching them.

Fix: State in writing that address book, call and SMS content stays on the phone and the Bluetooth link. If any part goes to a backend, name the legal basis and the Art. 14 information route for the contacts.

H3: NotificationListenerService with system-wide notification access and a queries block that names eight messaging apps

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)

NPNotificationService is declared with the BIND_NOTIFICATION_LISTENER_SERVICE permission. The queries block names WeChat, QQ, WhatsApp, Messenger, Line, KakaoTalk, Instagram, Skype and the Samsung and default SMS apps.

```
<service android:enabled="true" android:exported="true"
   android:foregroundServiceType="connectedDevice"
         android:name="com.lianhezhuli.hyfit.aider.NPNotificationService"
         android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action
           android:name="android.service.notification.NotificationListenerService"/>
    </intent-filter>
</service>
```

Only the operating system can bind to the service. The capability remains: a listener can read sender, source app and text of every notification, which allows a picture of who writes to the user, how often and through which app without storing content. Whether parsed notification content stays on the Bluetooth link or reaches a local database, the backend or an analytics SDK is UNVERIFIED.

Impact: Messages from family, partners, doctors and colleagues across eight named messaging apps pass the listener, and the policy text describes only calls, contacts and SMS.

Fix: Limit the listener to the apps and categories that the bracelet displays and state in the policy that notification content is neither stored nor sent to any SDK.

H4: Special category health data including blood glucose, blood pressure, blood oxygen, temperature and sleep

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.8 (CVSS-B)

The manifest declares measurement and history screens for heart rate, blood pressure, blood oxygen, body temperature, blood glucose (with manual input) and sleep. ACTIVITY_RECOGNITION is declared and described in the privacy text.

```
HrMeasureActivity  BpMeasureActivity  BoMeasureActivity  TempMeasureActivity
GluRecordActivity  GluInputActivity  HistoryGluActivity
HistoryOfSleepActivity  HistoryOfHrActivity  HistoryOfBpActivity
```

The glucose screens give a longitudinal log with manual entry. Combined with heart rate and sleep history this is a detailed health picture. The data sits inside the architecture of C1 and C2. This review located no separate Art. 9(2) condition and no data protection impact assessment in the material. Consent capture for the health screens was not examined at runtime, which is UNVERIFIED.

Impact: People with diabetes, hypertension or sleep problems keep a longitudinal health record in an app that initialises advertising SDKs at start and permits plaintext transport.

Fix: Document the Art. 9(2) condition for each measurement type, run and publish a data protection impact assessment and separate health data from the advertising initialisation.

M1: Remote camera trigger from the paired bracelet

LOW, CVSS v4.0 AV:A/AC:H/AT:N/PR:L/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B)

The app discloses that the bracelet can remotely trigger the phone camera. OldTakePhotoActivity, BaseCameraTakePhotoActivity and PhotoPreviewActivity implement it.

```
permission_title_camera_des:  "Function for scanning code connection and remote
   camera"
permission_detail_camera_des: "We visited your camera permission to scan code, and
   the bracelet is remotely Selfie."
```

A remoteCaptureServiceUrl field that appears in the dex belongs to the Google Mobile Ads SDK feature-flag namespace and is not part of this feature. Whether the camera command can originate only from the paired bracelet or also from a backend path is UNVERIFIED. A camera released from the wrist captures whoever stands in front of the phone.

Impact: Bystanders in front of a phone can be photographed by a command from someone else's wrist.

Fix: Confirm that only the paired bracelet can release the shutter and that no network path arms the feature.

M2: Firebase and Google Maps keys and identifiers hardcoded

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)

strings.xml carries the Firebase project values and one Google API key. The manifest carries a separate Maps key. No key was tested or used.

```
<string name="google_api_key">AIzaSyBSIswUuEEh8NqHAOUKTCCA2TC_hkZc6-w</string>
<string
   name="google_crash_reporting_api_key">AIzaSyBSIswUuEEh8NqHAOUKTCCA2TC_hkZc6-w</
    string>
<string name="google_app_id">1:769389742827:android:c717b6939ce16cbeed0cae</string>
<string name="google_storage_bucket">hryfine-85cf2.appspot.com</string>
<string name="project_id">hryfine-85cf2</string>
<string name="gcm_defaultSenderId">769389742827</string>
<string
   name="default_web_client_id">769389742827-aftqmvfg93n028q62e1d2thkua50p366.apps.
    googleusercontent.com</string>
<meta-data android:name="com.google.android.geo.API_KEY"
   android:value="AIzaSyBckbG6Lmnc88g3MsGub4Nu7udMHdfwM5U"/>
```

Google documents Firebase API keys as identifiers and not as secrets. The finding concerns quota and billing exposure, and it depends on whether Firebase security rules and Cloud Storage rules are locked down. The burden of proof lies with the operator and the rules cannot be tested without calling the service.

Impact: The operator carries quota and billing risk, and users could lose app features if quota is exhausted.

Fix: Restrict the keys to the package name and signing certificate and verify that the Firebase and Cloud Storage rules deny unauthenticated access.

M3: allowBackup is true and the FileProvider covers the whole external storage root

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

The application element sets allowBackup=”true”. file_paths.xml declares download_path with path /storage/emulated/0/ and camera_photos with path ”.”.

```
<application android:allowBackup="true" ... />
<paths>
    <external-path name="download_path" path="/storage/emulated/0/" />
    <external-path name="camera_photos" path="." />
    <external-path name="share_pic" path="/storage/emulated/0/HryFine/ScreenShot/"
       />
    <files-path name="update" path="./updateFile/" />
</paths>
```

allowBackup=”true” makes the private data directory eligible for Android backup. On current Android versions adb backup no longer exports the private data of apps that target API level 31 or higher, so the relevant route is the automatic cloud backup. Which files the backup includes depends on backup rules that were not recorded in the review material, which is UNVERIFIED. The download_path entry grants URI scope over the whole external storage root, while the share_pic entry already covers the disclosed screenshot sharing.

Impact: Contacts, health measurements and photos that the app caches could travel into device backups, and a shared URI could open more storage than the user intended.

Fix: Set allowBackup to false or define backup rules that exclude health and contact data, and remove the root download_path and the camera_photos root entry.

M4: MessageService is exported without a protecting permission

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B)

com.lianhezhuli.hyfit.service.MessageService is exported with no android:permission attribute.

```
<service android:enabled="true" android:exported="true"
   android:name="com.lianhezhuli.hyfit.service.MessageService"/>
```

NPNotificationService is protected by a system permission and the other services are unexported or run in a private process. MessageService can be started or bound by any app on the device. What it does when invoked from outside could not be determined from resources, which is UNVERIFIED. It is recorded as an improperly protected component under OWASP MASVS-PLATFORM.

Impact: Another app on the phone may be able to reach a messaging component of the app without holding any permission.

Fix: Set exported to false or protect the service with a signature-level permission.

M5: PEGI 3 rating with no age gate and an advisory paragraph for minors under 18

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)

Google Play lists the app as PEGI 3 and Everyone. The privacy text asks minors under 18 to seek parental guidance. No date-of-birth field, age screen or parental gate was found in the resources.

```
5. Use of our services by minors. We encourage parents or guardians to guide minors
   under the age of 18 to use our services. We recommend that minors encourage their
   parents or guardians to read this Privacy Policy and advise minors to seek
   parental or guardian consent and guidance before submitting personal information.
```

The paragraph imposes no technical control. The feature set (SMS and call forwarding, blood glucose logging, location, camera trigger) points to adult users managing their own communications and, for glucose, a chronic condition.

Impact: A child whose parent saw PEGI 3 can use an app that reads contacts and messages and logs health data.

Fix: Align the content rating with the features and add an age screen with a parental consent route.

Impact Analysis

HryFine has more than 50 million installs. People who use it log glucose, blood pressure, blood oxygen and sleep, forward their calls, messages and contacts to a bracelet and allow notification access. The same app starts more than a dozen advertising companies at launch.

Four groups carry the consequences. People who manage diabetes, hypertension or sleep problems keep a health record in an app that permits plaintext transport (C2, H4). Every user is subject to advertising and analytics initialisation before a consent screen can appear (C1). Contacts, callers and message senders who never installed the app are processed without notice (H2, H3). Children whose parents read PEGI 3 find an app that reads contacts and messages and logs health data (M5).

The harm demonstrated is a harm of default configuration and of opacity. Observed exposure on the wire is not claimed because no traffic was captured.

Advertising and Analytics Stack

The table lists the networks that the dex string pool shows at class level. The inventory includes companies in mainland China (Pangle, Tencent, Mintegral), Russia (MyTarget) and Japan (Maio, FiveAd). Whether each network is active in a given release is UNVERIFIED.

Network	Class evidence
AppLovin MAX	Lcom/applovin/
Vungle / Liftoff	Lcom/vungle/
Meta Audience Network	Lcom/facebook/ads/ (plus two embedded dex in assets/audience_network/)
ironSource / Unity LevelPlay	Lcom/ironsource/ (30+ obfuscated sub-packages)
InMobi	Lcom/inmobi/
Unity Ads	Lcom/unity3d/ads/
Mintegral / Mobvista	Lcom/mbridge/msdk/, Lcom/mintegral/msdk/
Pangle / ByteDance	Lcom/bytedance/adsdk/, Lcom/pgl/ssdk/
Tencent GDT (Youliangtong)	Lcom/qq/e/
MyTarget (VK / Mail.ru)	Lcom/my/target/
Ogury	Lcom/ogury/
Smaato	Lcom/smaato/sdk/
Tapjoy	Lcom/tapjoy/
Moloco	Lcom/moloco/sdk/
Chartboost	Lcom/chartboost/
Fyber / Digital Turbine	Lcom/fyber/inneractive/
Verve / PubNative	Lnet/pubnative/lite/
Amazon Publisher Services	Lcom/amazon/aps/
Maio	Ljp/maio/sdk/
FiveAd	Lcom/five_corp/ad/
Presage / Adjoe	Lio/presage/
Google AdMob	Lcom/google/android/gms/ads/
Tencent Beacon (analytics)	Lcom/tencent/beacon/
ByteDance APM Insight (analytics)	Lcom/apm/insight/

The Complete Chain

Step 1, install: a user finds an app with 50 million downloads, PEGI 3 and a Data safety label that says data is encrypted in transit (C2, M5).

Step 2, first launch: ContentProviders of Firebase, AppLovin, Vungle, Meta, ironSource and Mintegral construct their SDKs inside Application.onCreate, before any consent form can render (C1).

Step 3, permissions and features: the user grants contacts, call log, SMS, location, camera and notification access and starts logging glucose, blood pressure and sleep (H2, H3, H4).

Step 4, transmission: the network security configuration permits plaintext for every host, and the dex holds literal Tencent and Pangle endpoints (C2, H1).

Step 5, the user tries to understand: the in-app text names Pangle, Tencent GDT, Amap and Umeng in Chinese brand names, two of which do not appear in the build, and names no controller contact except a Gmail address (H1).

Shared Chipset SDK Fingerprint

HryFine ships the Bluetrum abpartool SDK for Bluetooth chipsets. A class-level comparison on 22 August 2026 found the same namespace (Lcom/bluetrum/abpartool/ParTool, R and utils/ImageUtils) in Wearfit Pro, an app of another operator with its own report of the same date. Wearfit Pro adds a Bluetrum fota over-the-air update stack. The signing certificates differ, which is expected, since each operator signs its own build. The shared element is the chipset vendor component. A WearFit2.0 comparison was not possible at that time and is not claimed. FitCloudPro later showed the same namespace.

```
Signing cert SHA-256
   923b7186b8811b3b71ae22c2bb506b4e2ab80dd53fb5460c412d6f97a7ae3375
Signing DN             CN=hy, OU=hy, O=huayan, L=sz, ST=gd, C=cn
BLE vendor SDK         com.bluetrum.abpartool (Java), libabpartool.so SHA-256
   a2cbdf4c7366f5a84b23d8ee4043013c7a88ad9e2e4201ab99366c4321efffbb
BLE GATT layer         com.welie.blessed (open-source Blessed library)
Field names            device_model, product_id, firmware_version, PER_VENDOR_ID
   (dex string pool)
```

BLE manufacturer IDs and GATT UUID constants were not extracted at this depth.

Data Protection: Article by Article

Article 5(1)(a) and (c) and Article 5(2), transparency, minimisation and accountability: engaged by C1, H1, H3 and M5.

Article 5(1)(f), integrity and confidentiality: engaged by C2 and H4.

Articles 6(1) and 7(1), lawfulness and conditions for consent: engaged by C1. Processing by SDKs that construct at process start precedes any consent decision, and ePrivacy Art. 5(3) applies to access to the terminal equipment.

Article 8, a child's consent: engaged by M5.

Article 9, special categories: engaged by H4. Blood glucose, blood pressure, blood oxygen, temperature, heart rate and sleep data are health data.

Articles 12(1), 13(1) and 14, information duties: engaged by H1 and H2. The SDK disclosure is in untranslated Chinese brand names and the contacts of H2 receive no notice.

Article 25, data protection by design and by default: engaged by C1, C2, M3 and M4.

Article 27, EU representative: engaged. None found.

Article 32(1)(a) and (b), security of processing: engaged by C2, M2, M3 and M4.

Article 35, impact assessment: engaged by H1 and H4. None is published.

Articles 44 and 46, transfers: engaged by H1. Tencent and ByteDance infrastructure appears in the evidence and no safeguard is named.

Platform Accountability & DSA

The Google Play Data safety panel of HryFine says that the app may share device or other identifiers with third parties, may collect location, personal information and two other categories, that data is encrypted in transit and that users can request deletion. The manifest permits cleartext traffic for the whole app (C2), so the statement on encryption in transit conflicts with the shipped configuration. The Contains ads badge and the sharing statement agree with the advertising stack of C1.

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

Regulatory & Legal Landscape

Shenzhen United Power Technology Co., Ltd. offers the app to users in the Union, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the notice in copy.

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27, 32 and 35 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers storage of and access to information on the user's device.

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

Indicators of Compromise & Reproducible Evidence

Every point is reproducible from the public Google Play build of 10 August 2026 and public web pages read by plain HTTP GET.

```
Package            com.lianhezhuli.hyfit
Version            3.8.12 (versionCode 216), Play update 10 Aug 2026
APK size           102,631,090 bytes
APK SHA-256        a462666229d46dd20911159abd4b75f32912492e31caf85b6b017df7c0768e6f
Signing cert       923b7186b8811b3b71ae22c2bb506b4e2ab80dd53fb5460c412d6f97a7ae3375
minSdk / target    24 / 35
Obtained from      APKPure mirror, matched to APKMirror and the live Play listing
   (developer name identical on all three)
```

```
google_api_key / google_crash_reporting_api_key
   AIzaSyBSIswUuEEh8NqHAOUKTCCA2TC_hkZc6-w
google_app_id   1:769389742827:android:c717b6939ce16cbeed0cae
project_id      hryfine-85cf2     storage bucket  hryfine-85cf2.appspot.com
   gcm_defaultSenderId  769389742827
default_web_client_id
   769389742827-aftqmvfg93n028q62e1d2thkua50p366.apps.googleusercontent.com
com.google.android.geo.API_KEY   AIzaSyBckbG6Lmnc88g3MsGub4Nu7udMHdfwM5U
```

```
otheve.beacon.qq.com  mqqeve.beacon.qq.com  othstr.beacon.qq.com  h.trace.qq.com
   api16-access-sg.pangle.io  redirector.gvt1-cn.com
hdtapp2016@gmail.com  www.lhzl666.com  privacy.lhzl666.com
```

```
https://privacy.lhzl666.com/static/hryfine/privacypolicy_gp.html  (in-app strings
   user_privacy_content29, 40 to 49)
```

Disclosure Timeline & Outcome

2026-08-22 First notice, REF HRYFINE-2026-R1, sent at 14:19 UTC to hdtapp2016@gmail.com with the Austrian DSB and the EDPS in copy. A second message with the same reference and findings went to the same address at 17:05 UTC. The notice states a 90-day embargo counted from delivery.

2026-09-12 Follow-up to hdtapp2016@gmail.com restating the findings and asking three questions with a response date of 19 September 2026. They asked which code path stops the seven ContentProviders from producing network traffic before a documented consent, on what basis the Data safety statement on encryption in transit was made, and whether address book, call or SMS content ever leaves the device toward a backend.

2026-10-17 Second follow-up from security@rfi-irfos.com, 34 days before publication, with the three questions unchanged and the embargo stated as 20 November 2026.

2026-11-14 No reply of any kind, no automated acknowledgment and no bounce. A search of the mailbox for inbound mail from the operator’s address returned nothing.

2026-11-20 Publication date as stated in the second follow-up and equal to 90 days from the notice of 22 August 2026.

What Was Done Well

Google’s User Messaging Platform SDK and IAB TCF constants are bundled, so the app has real consent tooling and the problem of C1 is one of timing and not of absence. The sensitive permissions come with specific plain-language purpose strings (user_privacy_content40 to 43). The share_pic FileProvider path is correctly scoped to one subfolder. According to the web policy, iOS HealthKit data is not shared, sold or used for advertising, which is a specific commitment. A working account-deletion path exists (CancelAccountActivity) and the Data safety label confirms that users can request deletion.

Residual Risk & Recommendations

Open at the date of publication: all eleven findings. The operator has not replied, and the build analysed is version 3.8.12 of 10 August 2026. A final APK diff before 20 November 2026 determines the state that the published report records. Silent fixes are recorded as such.

Recommendations in order of effect. First, hold every advertising and analytics SDK behind the consent decision (C1). Second, remove the global cleartext permission, pin the first-party hosts and correct the Data safety declaration (C2). Third, state the data recipients in plain English with countries and safeguards, remove references to SDKs that are not in the build and publish a data protection impact assessment for the health features (H1, H4). Fourth, confirm that contacts, call, SMS and notification content stay on the Bluetooth link (H2, H3). Fifth, appoint an Art. 27 representative, set up a corporate contact channel, restrict the keys, review backup rules and the exported service, narrow the FileProvider and add an age gate (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) from the FIRST lookup tables 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 HRYFINE-2026-R1.