Security & Privacy Disclosure, Final Report

JYouPro - Fitness Tracker for Android (com.jaga.ibraceletplus.aigoband)

A location upload path coded in plain HTTP behind a promise that location stays on the phone, and a consent screen and policy that only Chinese readers can read, with no reply since the notice.

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

Target	Liao Huaxing (Keeprapid Dev), JYouPro - Fitness Tracker
Versions Audited	3.39.18 / versionCode 638 (Play update 2026-03-07, APKPure build 2026-03-12, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	8: 2 High, 5 Medium, 1 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`86ae4415353a36c6476305fe0dccdf4b5b729d2c58178c9484cfb6ab05558734`

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: Login, device pairing and GPS upload are coded as plain HTTP endpoints while the permission text promises that location data is only saved on the phone 7

6.2 C2: The only consent screen and the file filed as the English privacy policy are written in Chinese and no consent management platform exists 8

6.3 H1: Menstrual cycle, pregnancy due date and ECG features are built into the app and absent from the Play description and the Data Safety card 9

6.4 H2: Caller names of people who never installed the app are pushed to the watch and a notification listener reads every app, described only in the untranslated policy 10

6.5 H3: The IMEI is named as the input for the guest account, and the app runs as a persistent process with backup allowed 11

6.6 M1: Facebook SDK with default automatic initialisation and no consent management platform 12

6.7 M2: A Google Maps API key and an application ID with secret for an unidentified SDK are shipped in plain text in the package 13

6.8 M3: PEGI 3 rating on an app that ships pregnancy tracking, cycle tracking and an ECG flow 14

7 Impact Analysis 14

8 The Complete Chain 15

9 Single-Operator Cluster and Fingerprint Keys 15

10 Data Protection: Article by Article 16

11 Platform Accountability & DSA 16

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 19

Executive Summary

JYouPro - Fitness Tracker is a companion app for Bluetooth bands and watches with more than 1 million installs on Google Play. The developer account is Keeprapid Dev, and the Play listing names an individual, Liao Huaxing, with two personal QQ mailboxes as the only contacts. On 23 August 2026 RFI-IRFOS sent a notice with REF JYOUPRO-2026-R1 to 838333180@qq.com and thinksth@qq.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 3.39.18 shows that the permission text promises that location data is only saved on the phone, while the code holds a labelled endpoint, gpsUpload, on plain HTTP at api.keeprapid.com port 8081, next to plain HTTP login, logout and device pairing calls and an app-wide cleartext flag (C1). The only consent screen and the file filed as the English privacy policy are written in Chinese and no consent management platform exists (C2). Menstrual cycle, pregnancy due date and ECG features are built into the app and are absent from the Play description and the Data Safety card (H1). The app pushes caller names and notification content to the watch (H2), names the IMEI as the input of the guest account (H3), initialises the Facebook SDK by default (M1), ships a Google Maps key and an SDK secret in plain text (M2) and carries PEGI 3 (M3).

A reassessment by CVSS v4.0 band puts two findings at High, five at Medium and one at Low. The Critical labels of C1 and C2 of 23 August 2026 move to High because the package shows capability and file content and not runtime behaviour, and C2 stays High only through a stated blast-radius escalation. The Play Data Safety card is accurate on one point, it says that data is not encrypted and not sent over a secure connection.

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 3.39.18 (versionCode 638), obtained as an APK from the APKPure mirror and checked against the package name, title, developer name and version on the live Google Play listing. The file size of 15,588,161 bytes matches the size declared by the mirror. Work done: manifest and resource decode (apktool, no source decode), string-pool extraction across the three classes*.dex files and the three native libraries of the arm64-v8a folder (libhello.so, libnative-lib.so, libimage_processing_util_jni.so). The Google Play listing and Data Safety card 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	HIGH	Login, device pairing and GPS upload are coded as plain HTTP endpoints while the permission text promises that location data is only saved on the phone
C2	HIGH	The only consent screen and the file filed as the English privacy policy are written in Chinese and no consent management platform exists
H1	MEDIUM	Menstrual cycle, pregnancy due date and ECG features are built into the app and absent from the Play description and the Data Safety card
H2	MEDIUM	Caller names of people who never installed the app are pushed to the watch and a notification listener reads every app, described only in the untranslated policy
H3	MEDIUM	The IMEI is named as the input for the guest account, and the app runs as a persistent process with backup allowed
M1	MEDIUM	Facebook SDK with default automatic initialisation and no consent management platform
M2	MEDIUM	A Google Maps API key and an application ID with secret for an unidentified SDK are shipped in plain text in the package
M3	LOW	PEGI 3 rating on an app that ships pregnancy tracking, cycle tracking and an ECG flow

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Live use of the gpsUpload endpoint not shown by the package.
C2	CRITICAL	HIGH	No reply. Evidence is file content and does not depend on runtime.
H1	HIGH	MEDIUM	No reply. Features are in the manifest, transmission not shown.
H2	HIGH	MEDIUM	No reply. Onward transmission not shown.
H3	HIGH	MEDIUM	No reply. Identifier received on current Android not shown.
M1	MEDIUM	MEDIUM	No reply. Not changed by any reply.
M2	MEDIUM	MEDIUM	No reply. Key restrictions not visible from the package.
M3	MEDIUM	LOW	No reply. Age gate not found in resources.

The findings file of 23 August 2026 labels C1 and C2 as Critical and H1 to H3 as High. The report uses the CVSS v4.0 band of each finding. C2 stays High through a blast-radius escalation that the finding states.

Subject & Operator Analysis

The Google Play developer field shows 廖华星 (Liao Huaxing), an individual in China, under the storefront name Keeprapid Dev. No street address and no company name are shown. The contacts are 838333180@qq.com for the developer and thinksth@qq.com for support, both personal QQ mailboxes. The signing certificate reads CN=keeprapid, OU=keeprapid, O=keeprapid, L=shenzhen, ST=guangdong, C=CN. The Play listing shows 1M+ downloads, 3.6 stars from 7.47K reviews, the category Health & Fitness, PEGI 3 and nine compatible watch models.

No Data Protection Officer and no Article 27 representative appear in the package or on the listing. No external privacy policy link exists on the listing. The only policy ships inside the APK.

Google Play lists three apps from the same account that share the package prefix com.jaga.ibraceletplus: JYouPro (com.jaga.ibraceletplus.keepfit), JYouPro - Fitness Tracker (com.jaga.ibraceletplus.aigoband, the subject of this report) and JYouPro Sport (com.jaga.ibraceletplus.bizzarosport). The audited build uses the content path .../apps/smartband/keepfit/... for firmware and watch face downloads, which ties it to the keepfit line. 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

JYouPro is a native Android app with three classes*.dex files and a small native footprint. It talks to the band over Bluetooth Low Energy. The custom UUIDs found are 000033f3 to 000033f6 and 000056ff and 000057ff, next to the generic 0000ffe5 and 0000ffe9 range, and a scan record field is named getWorldManufacturerID. Phone events reach the band through READ_CALL_LOG, READ_CONTACTS and the NLService notification listener (H2).

The network side runs against one backend family at keeprapid.com. The plain HTTP endpoints on api.keeprapid.com port 8081 are labelled login, logout, gear_auth and gpsUpload (C1). The path names ronaldo-member, ronaldo-gearcenter and ronaldo-dc carry no brand. The host download.keeprapid.com port 8181 serves firmware and watch face content and openapi.keeprapid.com is used over HTTPS for SDK validation. Third-party components found are the Facebook SDK (M1), the X SDK, Google Sign-In, Google Maps and Google Fit. No Firebase Analytics, Crashlytics, AdMob ad serving, Amplitude, Segment or Sentry integration was found, and no ByteDance, Tencent, Alibaba, Baidu, Xiaomi, Huawei HMS, JPush or Getui SDK class was found. The strings com.tencent.mm, com.tencent.mobileqq and ssdk_tencentweibo are package name checks for sharing and not a bundled Tencent SDK. The data model behind the calls was not observed.

Engagement Summary

The notice REF JYOUPRO-2026-R1 was sent on 23 August 2026 at 00:28 UTC from rfi.irfos@gmail.com to 838333180@qq.com and thinksth@qq.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried eight findings, a statement of what the app does well and three questions, and set the embargo date of 21 November 2026. 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: JYouPro. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: Login, device pairing and GPS upload are coded as plain HTTP endpoints while the permission text promises that location data is only saved on the phone

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

AndroidManifest.xml of version 3.39.18 sets android:usesCleartextTraffic="true" on the application element and no android:networkSecurityConfig attribute exists. The res/xml directory holds ad_services_config.xml, provider_paths.xml, ps_file_paths.xml and update_cache_path.xml and no network security configuration, so nothing restricts cleartext and nothing pins a certificate. The dex strings hold five labelled endpoints, four of them on plain HTTP at api.keeprapid.com port 8081: login, logout, gear_auth and gpsUpload. Only the validate_sdk call uses HTTPS. The permission rationale that the app shows when it asks for location access says that location data is only saved on the phone and not shared in any way. Whether the live build still calls the gpsUpload endpoint was not tested and is UNVERIFIED.

```
<application ... android:usesCleartextTraffic="true" ...>

login url http://api.keeprapid.com:8081/ronaldo-member
logout url:http://api.keeprapid.com:8081/ronaldo-member
gear_auth url http://api.keeprapid.com:8081/ronaldo-gearcenter
gpsUpload url http://api.keeprapid.com:8081/ronaldo-dc
http://download.keeprapid.com:8181/docs/keepfit/an_%s_%s
validate_sdk url https://openapi.keeprapid.com/developer
```

```
permission_location (res/values/strings.xml):
"JYouPro collects location data to enable fitness tracking even when the app is in
    background.
We will only save the location information on your phone and will not share it in any
    way.
If you have any questions, you can always refer to our privacy policy and terms of
    service."
```

Each endpoint string carries its own functional label in the binary. The labels login, logout, gear_auth and gpsUpload are the names the app uses for these calls. The app targets API level 35, where cleartext HTTP is refused by default, so the manifest flag switches that protection off for every host.

Impact: A person who wears the band all day and allows background location is told that the position stays on the phone. The package contains a labelled path for position upload and sends the account login over a channel that anyone on the same Wi-Fi network or a hostile access point can read. If the path is live, the person's movements and credentials are exposed on every public network they use. The Data Safety card is accurate on this one point and says that data is not transferred over a secure connection.

Fix: Move every endpoint to HTTPS with a pinned certificate, remove the cleartext flag, add

a network security configuration, and either remove the gpsUpload path or correct the permission text to say that location is uploaded.

C2: The only consent screen and the file filed as the English privacy policy are written in Chinese and no consent management platform exists

---

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, rated HIGH by blast-radius escalation

The consent dialog strings sit in the base resource set res/values/strings.xml and no values-en override exists for them in any English locale folder (en-rUS, en-rGB, en-rAU, en-rCA, en-rIE, en-rIN, en-rNZ, en-rSG, en-rSS, en-rXC, en-rZA), so every locale renders the Chinese text. The file assets/web/en/privacy.html, the path the app uses for its English policy, holds Chinese legal text and its content matches assets/web/zh/privacy.html. The dex files contain the functions showAgreement, showPrivacy and showPrivacyDialog, so the gate is wired in. A string search across all three classes*.dex files for OneTrust, Didomi, Usercentrics, IABTCF and consentmanager returned no match. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the consent screen and the policy are the only legal text a user of a health tracker with more than 1 million installs ever sees, they are unreadable to every non-Chinese reader, and every other processing basis in the app depends on them.

```
user_agreement_privacy_info_need_confirm:  □□□□□□□□□□□□□□□□□□□□,.
  (Please check the box below to agree to the service agreement to enter the app.)
user_agreement_privacy_info_need_confirm2: □□□□□□□□□□□□□□□□□□□□□□□□□□□□,
  (Thank you for using this app. Please carefully read and agree to the following
    before use:)
user_agreement_privacy_info_need_confirm3: □□□□□.
user_agreement_privacy_agree: □□  (Agree)
user_agreement_privacy_reject: □□  (Reject)
```

```
assets/web/en/privacy.html   opens with the Chinese legal text beginning □□□□ □□□□□
    ...
assets/web/zh/privacy.html   same content
assets/web/□□□□JYouPro.zip   downloadable copy
```

The Play listing carries no external privacy policy link other than Google's own generic policy page, so the file inside the APK is the only policy the app offers.

Impact: A person who installs a tracker from an English listing meets a consent box and a privacy policy that they cannot read. They agree to processing of heart rate, sleep, location, call log and contacts data without knowing what they agreed to. The 1M+ installs include users in markets where Chinese is not the first language.

Fix: Provide the consent text and the policy in the languages of the markets served, link the policy from the Play listing, and add a consent management platform for the optional SDKs.

H1: Menstrual cycle, pregnancy due date and ECG features are built into the app and absent from the Play description and the Data Safety card

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

The Play description lists eight features: call notifications, SMS notifications, heart rate, sleep and workout history, sedentary reminders, weather, alarm and water reminders, and watch faces. The Data Safety card says the app may collect Personal info, Photos and videos, and Device or other IDs. Health and fitness, location, contacts and call logs are not listed. The manifest declares a complete set of activities for menstruation and pregnancy settings and for an ECG flow with test, report, history and share screens, plus blood pressure, blood oxygen and body temperature screens. The string resources confirm that the features are not stubs. What the app does with the values (local storage, upload) was not tested and is UNVERIFIED.

```
com.jaga.ibraceletplus.aigoband.Female.FemaleReminderActivity
com.jaga.ibraceletplus.aigoband.Female.FemaleReminderCalendarActivity
com.jaga.ibraceletplus.aigoband.Female.MenstruationSetActivity
com.jaga.ibraceletplus.aigoband.Female.PregnancySetActivity
com.jaga.ibraceletplus.aigoband.ecg.EcgHealthActivity, EcgTestActivity,
    EcgReportActivity,
  EcgHistoryActivity, EcgShareActivity, EcgXtTestActivity, EcgGuideActivity
com.jaga.ibraceletplus.aigoband.theme.dup.BpAdjustActivity
com.jaga.ibraceletplus.aigoband.detail.DetailOxygenActivity
com.jaga.ibraceletplus.aigoband.detail.DetailBodyTemperatureActivity

female_reminder_pregnancy_date, female_reminder_menstruation_recent,
female_reminder_mummy_child_message ("Fill in child birth information"),
female_reminder_pregnant ("Prepare pregnant")
```

Impact: Women who use the app to log their cycle or a pregnancy due date, and people who run an ECG from the band, enter some of the most private data a person has, and the listing and the Data Safety card tell them nothing of it. Under Art. 9 this is health data and, for cycle and pregnancy, data about reproductive life that needs explicit consent given with knowledge, which the unreadable consent screen of C2 cannot supply.

Fix: List the health features in the Play description and the Data Safety declaration, state the Art. 9(2) basis and the storage location in a readable policy, and complete a data protection impact assessment.

H2: Caller names of people who never installed the app are pushed to the watch and a notification listener reads every app, described only in the untranslated policy

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_CALL_LOG and READ_CONTACTS and registers com.jaga.ibraceletplus.aigoband.service.NLService bound with BIND_NOTIFICATION_LISTENER_SERVICE. No READ_SMS, RECEIVE_SMS or SEND_SMS permission is declared, so message content reaches the watch through the listener. A listener is not scoped to one app and sees sender, preview and timing of notifications of every app while the user keeps the access enabled. The Chinese policy, translated by RFI-IRFOS, says the contacts permission is used to send the name that matches an incoming number to the device and the notification permission to send new messages of other apps to the device, and that content read from other apps is used for no other purpose. Whether any of this leaves the phone beyond the Bluetooth hop is UNVERIFIED.

```
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<service android:name="com.jaga.ibraceletplus.aigoband.service.NLService"
         android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
    NotificationListenerService"/></intent-filter>
</service>
```

The strings permission_receive_sms and permission_send_sms exist in strings.xml although the manifest declares no SMS permission. This reads as a leftover from an earlier permission model and is recorded as an observation and not scored.

Impact: The person who calls a wearer, and every contact who messages them, is processed without notice and without any choice. These people never installed the app and never saw a consent screen in any language. The sender of a message and the frequency of contact reveal relationships and routines.

Fix: Name the caller and notification processing in a readable policy, limit the listener to the apps the feature needs, and state whether any content leaves the phone.

H3: The IMEI is named as the input for the guest account, and the app runs as a persistent process with backup allowed

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_PHONE_STATE and sets android:persistent="true" and android:allowBackup="true" on the application element. The translated Chinese policy says that the app reads IMEI, DeviceId, brand and model to generate a guest account when the user taps skip login. An IMEI cannot be reset by the user. The package does not show which identifier the app receives on current Android versions, since the platform withholds the IMEI from ordinary apps from Android 10, and that is UNVERIFIED. allowBackup permits extraction of the private data directory through adb backup on a device with USB debugging enabled. The persistent flag asks the system to keep the process alive.

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<application android:allowBackup="true" ... android:persistent="true" ...>
```

Policy sentence, translated by RFI-IRFOS: the app reads IMEI, DeviceId, Brand and Model to obtain device characteristic information to generate a guest account, and when the user selects the skip login button the system logs in using the guest account.

Impact: A person who chose not to register is tied to a hardware identifier that survives a reset and an app reinstall, so the guest session is a pseudonym only in name. A random identifier created on the phone would give the same session continuity.

Fix: Replace the hardware identifier with a locally generated random identifier, remove READ_PHONE_STATE if nothing else needs it, set allowBackup to false and drop the persistent flag.

M1: Facebook SDK with default automatic initialisation and no consent management platform

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 carries the Facebook application ID and client token and the provider FacebookContentProvider653353401518097. No com.facebook.sdk.AutoInitEnabled or AutoLogAppEventsEnabled override is present. The dex files hold the standard flag reading logic (autoInitEnabled, autoLogAppEventsEnabledLocally, loadAutoLogAppEventsSettingFromManifest) and no evidence that the app switches either flag off. The app declares its own Application subclass, AppMng, whose onCreate runs before any activity, including the one that shows the consent dialog. The instruction level call order was not disassembled and is UNVERIFIED. The Data Safety card says no data is shared with third parties.

```
<meta-data android:name="com.facebook.sdk.ApplicationId" android:value="@string/
    facebook_app_id"/>
<meta-data android:name="com.facebook.sdk.ClientToken" android:value="@string/
    facebook_client_token"/>
<provider android:authorities="com.facebook.app.FacebookContentProvider653353401518097
    " android:exported="true" .../>

facebook_app_id           653353401518097
facebook_client_token     4243f419b385008eb84549d44719d75a
```

Impact: Meta's SDK can start logging app events before the person has made any choice, in an app that holds health data and offers no readable choice at all (C2).

Fix: Disable automatic initialisation and event logging until a recorded consent decision and correct the Data Safety card.

M2: A Google Maps API key and an application ID with secret for an unidentified SDK are shipped in plain text in the package

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 Google Maps key in com.google.android.geo.API_KEY. The asset file assets/JySDK.xml holds an appid and secret pair under the tag czjksdk. The vendor behind it was not identified, since no class with that name was found in the dex files and the file is probably read through generic XML parsing. Anyone who downloads the public package can read both values. The restrictions set on the key in the Google console and the scope of the secret were not tested, and the keys were not used.

```
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyD079ZSbcrWLavaCDsOK0S90SE0gDqI4sk"/>

<czjksdk>
    <vid>000001001003</vid>
    <appid>HUNEPX60P3KIDYH</appid>
    <secret>b8FXJMzfELLOTM6BgGsFXmieePgqx1Ya50gPEUur</secret>
</czjksdk>
```

Impact: A secret inside a public package is not confidential. Abuse of the key could run up quota or billing for the operator, and the secret could allow calls to an unidentified service in the operator’s name.

Fix: Restrict the Google key by package name and signature, rotate the SDK secret and move it to a server side call.

M3: PEGI 3 rating on an app that ships pregnancy tracking, cycle tracking and an ECG flow

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The Play listing carries PEGI 3. The same package ships pregnancy due date tracking, menstrual cycle tracking and an ECG test, report, history and share flow (H1), and requests call log, contacts and background location permissions. The listing and the policy offer no age gate. No date of birth field or parental consent string was located in the resources, which cover the resources and not the bytecode, so an age gate implemented in code would not appear. The absence is therefore not asserted.

```
Google Play content rating: PEGI 3 ("Users Interact")
Compatible devices listed on Google Play: ZW01, T18, ZW27T, T100, T100A, L21, S050,
    T95, G12Pro
```

Impact: Parents who choose by rating see a product for everyone, and a child can install an app that carries reproductive health tracking and reads the call log.

Fix: Align the rating with the feature set, add an age gate or state that the app is for adults.

Impact Analysis

The people affected are the users of a health and fitness companion with more than 1 million installs. They put a band on the wrist, grant Bluetooth, location, phone, contacts and notification access, and may record a menstrual cycle, a pregnancy due date or an ECG. Some are children, since the Play rating is PEGI 3. Callers and contacts of those users are affected too.

The weight of the case sits on two points. The permission text tells users that location stays on the phone while the code holds a labelled plain HTTP upload path (C1). The consent screen and the policy cannot be read by anyone outside the Chinese reading public (C2), which removes the basis for informed consent to everything else, including the reproductive and ECG features of H1.

What the package shows is configuration, labelled capability and file content. No location value, 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 finds the app in an English listing that offers eight features and a Data Safety card that omits health data. The Facebook SDK can start at process creation (M1).

Step 2, consent: the first screen is a Chinese consent box and a Chinese policy. The user taps Agree to enter (C2).

Step 3, pairing and use: the user grants Bluetooth, location, phone, contacts and notification access. Caller names and notifications of all apps go to the watch (H2). Cycle, pregnancy and ECG entries are possible (H1).

Step 4, backend: login, device pairing and the labelled gpsUpload call are coded for plain HTTP on api.keeprapid.com port 8081 under an app-wide cleartext flag (C1). A user who skips login receives a guest account built from device characteristics that include the IMEI (H3).

Step 5, rights: a person who wants access or deletion finds an individual developer, two personal QQ mailboxes and no policy link on the listing.

Single-Operator Cluster and Fingerprint Keys

A cross-check against the archived HryFine, WearFit2.0 and Wearfit Pro packages of this programme found no shared signing certificate, native library, BLE chipset SDK or backend domain. The HryFine certificate begins 923b7186 and the WearFit2.0 certificate 903aedb9, so no cross-vendor link is asserted. What is confirmed is a single-operator cluster of three Google Play listings with the package prefix com.jaga.ibraceletplus, one backend family at keeprapid.com and shared internal service names. The audited aigoband build references the keepfit content path, so the three listings are re-skins of one codebase.

```
Signing cert SHA-256
    c7486419f1c312ef1874df208ce8187d45b7bc6d8e6135396e0ea696df08d08c
Signing DN            CN=keeprapid, OU=keeprapid, O=keeprapid, L=shenzhen, ST=
    guangdong, C=CN
Native libraries      libhello.so, libnative-lib.so, libimage_processing_util_jni.so
BLE UUIDs (custom)    000033f3 to 000033f6, 000056ff, 000057ff
Scan record field     getWorldManufacturerID / worldManufacturerID
Sibling packages      com.jaga.ibraceletplus.keepfit, com.jaga.ibraceletplus.
    bizzarosport
Backend family        api.keeprapid.com:8081, download.keeprapid.com:8181, openapi.
    keeprapid.com
```

Data Protection: Article by Article

Article 4(11) and Article 7(2), conditions for consent: engaged by C2. A consent in a language the person cannot read is not informed.

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

Article 5(1)(c), data minimisation: engaged by H2 and H3.

Article 6(1): engaged by C2, H2 and M1.

Article 7(1): engaged by M1.

Article 8, children: engaged by M3.

Article 9(1) and (2)(a): engaged by H1 for cycle, pregnancy and ECG data. No processing of these values by the operator is asserted, the engagement is the unreadable consent and the omission from the listing.

Article 12(1) and Article 13(1)(c): engaged by C2 and H1. Article 14 is engaged by H2 for callers and contacts.

Article 25(1): engaged by C1, H3, M1 and M3.

Article 27: no representative is named for an individual controller in China that offers the app in the Union.

Article 32(1)(a) and (b): engaged by C1 and M2. Article 32(1)(b) is also engaged by H3 for the backup flag.

Article 35(3)(b): engaged by H1 as an open question.

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 Data Safety card of the listing, read on 23 August 2026, says the app may collect Personal info, Photos and videos, and Device or other IDs, shares no data with third parties, does not encrypt data, does not transfer it over a secure connection and allows a deletion request. The cleartext statements match the package. The omission of health, location, contacts and call data and the statement that no data is shared with third parties do not match the package (H1, M1).

Regulatory & Legal Landscape

The individual developer Liao Huaxing 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.jaga.ibraceletplus.aigoband
Version            3.39.18 (versionCode 638), minSdk 21, targetSdk 35, compileSdk 35
APK size           15,588,161 bytes
APK SHA-256        86ae4415353a36c6476305fe0dccdf4b5b729d2c58178c9484cfb6ab05558734
Signing cert SHA-256 c7486419f1c312ef1874df208ce8187d45b7bc6d8e6135396e0ea696df08d08c
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
Google Maps API key      AIzaSyD079ZSbcrWLavaCDsOK0S90SE0gDqI4sk
Facebook App ID          653353401518097
Facebook client token    4243f419b385008eb84549d44719d75a
JySDK vid                000001001003
JySDK appid              HUNEPX60P3KIDYH
JySDK secret             b8FXJMzfELLOTM6BgGsFXmieePgqx1Ya50gPEUur
http://api.keeprapid.com:8081/ronaldo-member   (login, logout)
http://api.keeprapid.com:8081/ronaldo-gearcenter   (gear_auth)
http://api.keeprapid.com:8081/ronaldo-dc   (gpsUpload)
http://download.keeprapid.com:8181/docs/keepfit/an_%s_%s
https://openapi.keeprapid.com/developer   (validate_sdk)
Contacts               838333180@qq.com, thinksth@qq.com
```

```
C1  AndroidManifest.xml (usesCleartextTraffic), res/xml listing, classes*.dex (
    labelled endpoints), res/values/strings.xml (permission_location)
C2  res/values/strings.xml (user_agreement_privacy_*), res/values-en-* folders, assets
    /web/en/privacy.html, assets/web/zh/privacy.html, classes*.dex (showAgreement,
    showPrivacy)
H1  AndroidManifest.xml (Female and ecg activities), res/values/strings.xml, Google
    Play listing
H2  AndroidManifest.xml (READ_CALL_LOG, READ_CONTACTS, NLService), assets/web/en/
    privacy.html
H3  AndroidManifest.xml (READ_PHONE_STATE, persistent, allowBackup), assets/web/en/
    privacy.html
M1  AndroidManifest.xml (com.facebook.sdk.*), res/values/strings.xml, classes*.dex
M2  AndroidManifest.xml (geo.API_KEY), assets/JySDK.xml
M3  Google Play listing
```

Reproduction: obtain com.jaga.ibraceletplus.aigoband 3.39.18 (638), 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. The Chinese policy text is read with the glosses given in this report.

Disclosure Timeline & Outcome

2026-08-23 Notice REF JYOUPRO-2026-R1 at 00:28 UTC to 838333180@qq.com and thinksth@qq.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Eight findings, three questions, embargo date 21 November 2026.

2026-09-12 Follow-up to both addresses at 17:03 UTC. It restated the findings and asked the three questions on the basis of the location promise, the validity of a consent in Chinese and the legal basis and impact assessment for cycle, pregnancy and ECG data, with answers due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:05 UTC, under the subject 35 days to publication: JYouPro.

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 Data Safety card is honest on transport security. It says that data is not encrypted and not transferred over a secure connection, which matches the package and is more candid than many comparable listings. A deletion request path is stated on the card. The permission rationale strings for call log, call notifications, location and Bluetooth scanning explain in readable English why each permission is requested. The third-party footprint is small. No Chinese advertising or analytics SDK, no Firebase Analytics, no AdMob ad serving and no Crashlytics integration was found at class level.

Residual Risk & Recommendations

Open at the date of publication: all eight findings. The operator has not replied and the build analysed is version 3.39.18 of March 2026. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, move all endpoints to HTTPS with pinning, remove the cleartext flag and either remove gpsUpload or correct the permission text (C1). Second, provide the consent screen and the policy in the languages of the markets served and link the policy from the listing (C2). Third, describe the cycle, pregnancy and ECG features in the listing and the Data Safety card with the Art. 9(2) basis (H1). Fourth, scope the notification listener and name caller and notification processing in the policy (H2). Fifth, replace the IMEI based guest identifier and set allowBackup to false (H3). Sixth, gate the Facebook SDK on consent, restrict or rotate the keys and align the rating with the feature set (M1 to M3).

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 JYOUPRO-2026-R1.