Security & Privacy Disclosure, Final Report

MActivePro for Android (com.njj.mactivepro)

A Data Safety card that says nothing is shared and lists device identifiers only, against a policy that names a dozen SDK vendors, with no reply since the notice.

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

Target	Shenzhen Horn Big Data Software Co.,Ltd (MActivePro)
Versions Audited	2.0.0 / versionCode 20000 (Play update 2026-08-06, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	10: 2 High, 4 Medium, 2 Low, 2 Info (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`078c8dbd38555f4ecd36ae615ba55cde8ec599733527eba7270a7b6550d34ead`

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: The Data Safety card says no data is shared with third parties and lists only device identifiers, while the operator's own policy names more than a dozen SDK vendors and a long list of collected categories . . . 7

6.2 C2: Cleartext traffic is permitted for the whole app and the policy states that the data is stored in the People's Republic of China, for an app with health, menstrual, pregnancy and Qibla features . . . 8

6.3 C3: Google ML Kit and Google Mobile Ads construct at process start, no consent management platform was found, and a notification listener sits next to call log, contacts and SMS access . . . 9

6.4 H1: A commercial packer (Qihoo 360 Jiagu) hides the application's own strings from independent verification . . . 10

6.5 H2: Jieli chipset SDK libraries, two Shenzhen company names behind one product and a hosting domain of a white label platform . . . 11

6.6 H3: An AI smart glasses assistant with meeting transcription, simultaneous interpretation and face translation ships inside a bracelet app, and the Play description mentions none of it . . . 12

6.7 M1: Only two personal mailboxes are published as contacts and no Article 27 representative or Data Protection Officer is named . . . 13

6.8 M2: PEGI 3 rating, a policy that sets the minor threshold at 14 and no client side age gate in the resources . . . 13

6.9 M3: Google Maps, AutoNavi, AdMob and HIFIVE identifiers and a server code are hardcoded in the manifest . . . 14

6.10 M4: The Jieli authentication and OTA libraries give the backend a firmware channel to the worn device . . . 15

7 Impact Analysis 15

8 The Complete Chain 16

9 Chipset SDK Cluster and Fingerprint Keys 16

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 18

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 20

Executive Summary

MActivePro is a companion app for a smart bracelet with more than 10 million downloads on Google Play. The publisher is Shenzhen Horn Big Data Software Co.,Ltd. The listing describes steps, activity, sleep and menstrual cycle tracking and shows the Contains ads badge, PEGI 3 and a Data Safety card. On 23 August 2026 RFI-IRFOS sent a notice with REF MACTIVEPRO-2026-R1 to fhjjbffhu@gmail.com and HuangXiaoLong2023@163.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 2.0.0 shows that the Data Safety card says no data is shared with third parties and that only device identifiers are collected, while the operator's own policy lists health data including the female menstrual cycle among the collected data and names more than a dozen SDK vendors that receive device identifiers, location, steps and advertising data (C1). The app permits cleartext traffic for every host and the policy states that data is stored in the People's Republic of China (C2). Google ML Kit and Google Mobile Ads construct at process start and no consent management platform was found (C3). The package also holds an AI smart glasses assistant with meeting transcription and face translation that the listing never mentions (H3), personal mailboxes as the only contacts (M1) and hardcoded keys (M3).

The application code is packed with the Qihoo 360 Jiagu packer, so endpoints and BLE identifiers could not be read and most runtime questions stay open (H1). A reassessment by CVSS v4.0 band puts two findings at High, four at Medium and two at Low, with two informational entries. All three Critical labels of 23 August 2026 move down because the package shows configuration and file content and not runtime behaviour. C1 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 2.0.0 (versionCode 20000). The package was obtained as an XAPK bundle (armeabi-v7a variant, 250.8 MB) from the APKPure mirror and checked against the package name, developer name, version and update date on the live Google Play listing. The Google Play update date is 6 August 2026 and the mirror date is 7 August 2026. Work done: manifest and resource decode (apktool, no source decode), the native library inventory with SHA-256 values, the bundled asset and JSON files, and a string pass across the single classes.dex. That dex is packed by the Jiagu stub, so its string pool does not contain the application's own literals. The live Google Play listing and the operator's English policy were read on 23 August 2026. The app was not installed, no account was created, no operator server was called and no traffic was captured. No bytecode pass and no dynamic unpacking were done. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	HIGH	The Data Safety card says no data is shared with third parties and lists only device identifiers, while the operator’s own policy names more than a dozen SDK vendors and a long list of collected categories
C2	HIGH	Cleartext traffic is permitted for the whole app and the policy states that the data is stored in the People’s Republic of China, for an app with health, menstrual, pregnancy and Qibla features
C3	MEDIUM	Google ML Kit and Google Mobile Ads construct at process start, no consent management platform was found, and a notification listener sits next to call log, contacts and SMS access
H1	INFO	A commercial packer (Qihoo 360 Jiagu) hides the application’s own strings from independent verification
H2	INFO	Jieli chipset SDK libraries, two Shenzhen company names behind one product and a hosting domain of a white label platform
H3	MEDIUM	An AI smart glasses assistant with meeting transcription, simultaneous interpretation and face translation ships inside a bracelet app, and the Play description mentions none of it
M1	MEDIUM	Only two personal mailboxes are published as contacts and no Article 27 representative or Data Protection Officer is named
M2	LOW	PEGI 3 rating, a policy that sets the minor threshold at 14 and no client side age gate in the resources
M3	MEDIUM	Google Maps, AutoNavi, AdMob and HIFIVE identifiers and a server code are hardcoded in the manifest
M4	LOW	The Jieli authentication and OTA libraries give the backend a firmware channel to the worn device

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. The contradiction is shown by two public documents.
C2	CRITICAL	HIGH	No reply. Plain HTTP use not readable because of the packer.
C3	CRITICAL	MEDIUM	No reply. Network activity before consent not shown.
H1	HIGH	INFO	No reply. Packer present, no score.
H2	HIGH	INFO	No reply. Structural observation, no score.
H3	HIGH	MEDIUM	No reply. Use and recipients of the modules not shown.
M1	MEDIUM	MEDIUM	No reply. Only the two personal mailboxes exist.
M2	MEDIUM	LOW	No reply. Age gate not found in resources.
M3	MEDIUM	MEDIUM	No reply. Key restrictions not visible from the package.
M4	MEDIUM	LOW	No reply. Command structure not shown.

The findings file of 23 August 2026 labels C1 to C3 as Critical, H1 to H3 as High and M1 to M4 as Medium. The report uses the CVSS v4.0 band of each finding. C1 stays High through a blast-radius escalation that the finding states. H1 and H2 are structural observations without a score.

Subject & Operator Analysis

The publisher on Google Play is Shenzhen Horn Big Data Software Co.,Ltd, Room 301, Block B, Jiada R&D Building, No. 5 Songpingshan Road, Songpingshan Community, Xili Street, Nanshan District, Shenzhen. The policy names the same company as holder of the MActive Pro trademark and names a second company, Shenzhen Nano-Jing Cloud Technology Co., Ltd., as operator of the server that receives device update and activation data. The policy is hosted at download.microwear.com, a white label wearable platform domain. Whether the two companies belong to one group is UNVERIFIED without a registry check.

The contacts are the personal mailboxes fhjjbffhu@gmail.com (Google Play) and HuangXiao-Long2023@163.com (policy section 12). No phone number, Data Protection Officer or Article 27 representative is named. The Play listing shows more than 10 million downloads, 3.0 stars from 28.3K reviews, the category Health & Fitness and the Contains ads badge.

The signing certificate is the Google Play App Signing certificate with the generic DN CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US, and does not identify the developer. 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

MActivePro is a native Android app with a single 27.8 MB classes.dex, packed by the Qihoo 360 Jiagu stub (com.stub.StubApp, libjiagu.so), and a native library split of 148.9 MB. The split holds nine Jieli chipset libraries, sherpa-ncnn speech libraries, TensorFlow Lite, Microsoft Cognitive Services Speech libraries and the Alibaba NUI voice stack. The bundled configuration assets/ali_nui.json sets the service mode to full cloud.

The app talks to the band and to smart glasses over Bluetooth Low Energy and receives phone events through the notification listener NJJNoticeService and the call log, contacts and SMS permissions (C3). The policy names the SDKs that receive data (C1). Two video calling engines (Zego and Alibaba Cloud RTC), Alipay, WeChat Pay and PayPal integrations and a stock ticker, a prayer direction compass and e-book and music functions are listed in the R1 findings from the manifest and assets. Because of the packer, no backend endpoint, BLE UUID or device identity constant could be read. The data model behind the calls was not observed.

Engagement Summary

The notice REF MACTIVEPRO-2026-R1 was sent on 23 August 2026 at 07:17 UTC from rfi.irfos@gmail.com to fhjjbffhu@gmail.com and HuangXiaoLong2023@163.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried three critical findings, the packer and cluster findings, 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: MActivePro. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: The Data Safety card says no data is shared with third parties and lists only device identifiers, while the operator's own policy names more than a dozen SDK vendors and a long list of collected categories

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 CRITICAL on 23 August 2026, rated HIGH by blast-radius escalation

The live Data Safety card of 23 August 2026 says: No data shared with third parties, This app may collect these data types: Device or other IDs, Data isn't encrypted, You can request that data be deleted. The operator's policy at download.microwear.com lists in section 1 the data that the app collects: age, gender, height and weight, account information, sports and health data (sleep, heart rate, electrocardiogram, blood oxygen, blood pressure, calories, body age and female menstrual cycle), location including precise location and trajectory, device identifiers (IMEI, MAC, IMSI, Android ID, OAID, advertising ID, hardware serial number, SIM ID), Bluetooth information, and contact and call log data for wearable call features. Section 6 names the SDK vendors and the data each receives. The table shows device identifiers, location, steps, payment data and advertising data, and it does not show menstrual, pregnancy or ECG values going to these vendors. The manifest declares 53 dangerous or special permissions, among them RECORD_AUDIO, CAMERA, READ_SMS, READ_CALL_LOG, READ_CONTACTS, CALL_PHONE, ANSWER_PHONE_CALLS, ACCESS_BACKGROUND_LOCATION, QUERY_ALL_PACKAGES and READ_LOGS. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the card is the first and often only disclosure for a health app with more than 10 million installs, it contradicts the operator's own policy point for point, and the collected categories include a menstrual cycle, a pregnancy and ECG readings.

```
Gaode (AutoNavi, Amap)        location
WeChat, QQ                    steps and device ID
WeChat Pay, Alipay            payment and device data
Tencent Bugly                 device identifiers
Amap SDK, Google Maps SDK     location
Baidu Smart Cloud Speech, Alibaba Cloud Voice Dictation   device identifiers for
    online speech to text
Mgmobi SDK                    location, device IDs, ad data
Baidu SDK (Baiqingteng)       device information, app signature, location, ad
    interaction data
Tencent Youlianghui (Guangdiantong) SDK   base stations, WiFi, IMEI, OAID, Android_ID,
     IDFV, app list
Kuaishou SDK                  IMEI, MEID, OAID, AndroidId, IMSI, ICCID, GPS, app
    install list
Mediatom SDK                  device IDs, IP, sensor, ad data
Pangolin SDK (ByteDance)      Android ID, IMEI, OAID, IMSI, ICCID, GAID, MEID, device
    serial, MAC, app package and process information, sensor data
```

The Play listing and the Data Safety card were captured as read on 23 August 2026. The policy runs to about 9,000 words in 12 numbered sections.

Impact: More than 10 million installs rely on a card that tells them that nothing is shared and that only device identifiers are collected. Users who track a menstrual cycle, a pregnancy or an ECG with the band cannot learn from the card what is collected, and they cannot learn from it that advertising SDKs of four Chinese companies receive device identifiers and location.

Fix: Correct the Data Safety declaration to match the policy and the manifest, list the health, location, contacts and call data categories and state which vendors receive which fields.

C2: Cleartext traffic is permitted for the whole app and the policy states that the data is stored in the People's Republic of China, for an app with health, menstrual, pregnancy and Qibla features

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 holds a base-config with cleartextTrafficPermitted set to true and a domain-config for android.bugly.qq.com that also permits cleartext. The application element sets android:usesCleartextTraffic="true". The file holds no pin-set and no restricted trust anchors. Section 2.1 of the operator's policy says that the personal information is stored within the People's Republic of China and that the data will be uploaded to the server only after explicit agreement in the application. The policy names no standard contractual clause or other transfer mechanism beyond a generic promise of adequate protection. The manifest holds WomanHealthDataActivity, MensesActivity, PregnantActivity and FemaleHealthTypeActivity next to ECG, blood pressure, blood oxygen and sleep activities. strings.xml holds a Qibla function (str_worship, str_download_worship_tip). A Qibla compass reveals a religious practice only if its use is recorded, and whether it is recorded is UNVERIFIED. Which endpoints are called over plain HTTP cannot be read because the dex string pool is packed (H1).

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

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

```
Policy section 2.1: "...we will store your personal information collected and
    generated during operations within the People's Republic of China within China...
    Your [MActive Pro] information contains sensitive personal information. We will
    upload it to the server only after you have explicitly agreed in the application.
    Your above data will be stored in the territory of the People's Republic of China
    ."
```

Health activities in the manifest: WomanHealthDataActivity, MensesActivity, PregnantActivity, FemaleHealthTypeActivity. String resources: str_baby_birth, str_begin_prepare_pregnancy, str_duration_last_menstruation, str_duration_menstruation, str_worship ("worship"), str_download_worship_tip ("Please go to the app store to download the Qibla function").

Impact: Women who track a menstrual cycle or prepare for a pregnancy, and people who read an ECG or blood pressure from the band, use an app whose transport settings permit plain HTTP and whose operator states that their data is stored in the People's Republic of China without naming a safeguard for transfers from the Union.

Fix: Remove the cleartext allowance, pin first-party hosts, name the Chapter V transfer mechanism in the policy and state the Article 9(2) basis for health data.

C3: Google ML Kit and Google Mobile Ads construct at process start, no consent management platform was found, and a notification listener sits next to call log, contacts and SMS access

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 registers MlKitInitProvider with initOrder 99 and MobileAdsInitProvider with initOrder 100. Android constructs them at process start, before any activity and so before any consent dialog. The AdMob application ID is in the manifest. A search of the resource files and the manifest for onetrust, didomi, usercentrics, iabtcf and consentmanager returned no match. The manifest registers com.njj.mactivepro.ble.notification.NJJNoticeService as a notification listener (BIND_NOTIFICATION_LISTENER_SERVICE) next to READ_CALL_LOG, READ_CONTACTS, READ_SMS, CALL_PHONE and ANSWER_PHONE_CALLS. The listener is the mechanism that the advertised notification mirroring needs. The combination can reconstruct who messages and calls the user and through which app. Whether notification content is kept or sent is UNVERIFIED because the dex is packed.

```
<provider android:authorities="com.njj.mactivepro.mlkitinitprovider" android:exported
    ="false" android:initOrder="99" android:name="com.google.mlkit.common.internal.
    MlKitInitProvider"/>
<provider android:authorities="com.njj.mactivepro.mobileadsinitprovider" android:
    exported="false" android:initOrder="100" android:name="com.google.android.gms.ads.
    MobileAdsInitProvider"/>

<service android:exported="true" android:name="com.njj.mactivepro.ble.notification.
    NJJNoticeService" android:permission="android.permission.
    BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter android:priority="1000">
        <action android:name="android.service.notification.NotificationListenerService
    "/>
        <action android:name="android.deletion.notification"/>
    </intent-filter>
</service>
```

Impact: The Play listing carries the Contains ads badge and the person who opens the app first meets no consent platform. People who write to the wearer, and whose notifications and call data the app can read, never see any notice.

Fix: Delay SDK initialisation until a recorded consent decision, add a consent management platform and limit the listener to the apps that the watch feature needs.

H1: A commercial packer (Qihoo 360 Jiagu) hides the application’s own strings from independent verification

INFO, no CVSS v4.0 score assigned, disclosed as HIGH on 23 August 2026

The Application class is com.stub.StubApp and the native split ships libjiagu.so, the runtime of the Qihoo 360 Jiagu packer. A string extraction across the 27.8 MB classes.dex (273,747 strings) found no match for http or https, and the pool consists mostly of short binary blobs. The application code and its literal strings, including backend endpoints, BLE UUIDs and device identity constants, are therefore not readable from the package. This is not a data protection violation. It is the reason that most of the runtime questions of this report stay UNVERIFIED and that the BLE manufacturer data and UUIDs could not be extracted.

```
AndroidManifest.xml     android:name="com.stub.StubApp"
lib/armeabi-v7a/libjiagu.so   SHA-256 4
    dd617b06fc16023e0c2166db1bea669b6876252088b535ce91e6f9e49749e1b
```

Impact: Nothing for users directly. A reviewer, a regulator or an auditor cannot verify from the package what the app sends and where.

Fix: Provide an unpacked build or a data flow description to supervisory authorities on request.

H2: Jieli chipset SDK libraries, two Shenzhen company names behind one product and a hosting domain of a white label platform

INFO, no CVSS v4.0 score assigned, disclosed as HIGH on 23 August 2026

The native split holds nine libraries of the Zhuhai Jieli Technology chipset SDK and the manifest holds GlassesJieLiOTAActivity, JieLiOtaFromFileActivity and com.jieli.component.permission.PermissionActivity. The same libjl family is recorded in the R1 findings of Fere Fit, FitPro, HumeHealth, Lefun Health and OnWear Pro, so the vendor SDK circulates across differently branded apps. The file level hashes of this report were not diffed byte for byte against those apps, and the correlation holds at library name level. The policy names Shenzhen Horn Big Data Software Co.,Ltd as trademark holder and publisher and, in section 1.2, Shenzhen Nano-Jing Cloud Technology Co., Ltd. as the operator of the server that receives device update and activation data. The policy is hosted on download.microwear.com, which is the domain of a white label wearable platform. The hosting domain is a circumstantial signal and not a proven code artefact.

```
e695e324484ba9690c38293541b385f660b24769b3df64caff44402625b597aa  libjl_auth.so
8cd3b9dc44f86b37ae6aa7ae226d0ae3f87404297715f1ebe4370dddbe0d4236  libjl_bmp_convert.so
8a6b1c791fce5a9f8e0e8cca262f52e2854e9fad92a5ad943f2af0133e4a5020  libjl_crc.so
b4aba62bcb4ccfd3f86d86fa48360d32eb7a11f09d989b24638658f41db07277  libjl_enc.so
0794b2f63b9388f4233b2101f41796f8b7604cbeb66d0ed8f94e57a8ef13e1cb  libjl_fatfs.so
26d9a6561cb523dee7a95146530fd8edb6bc5ccdb158ad2979f04c370496e837  libjl_opus.so
503b187a690d153e42fda622cbebff7ca46a337e6b63c6196b931beabbad8074  libjl_ota_auth.so
3d1618dd2c07d0132ebce7c96f033de8218413cf37818ba2ccb83260464e6dac  libjl_pack_format.so
539e04d7a4308cd6995e57be5ac25676b2166fa7ddf01ae7c412409b53d80605  libjl_speex.so
```

```
Policy section 1.2: "connecting to Shenzhen Nano-Jing Cloud Technology Co., Ltd.'s '
    MActive Pro' smart wearable device... your device name, device identification
    information... will also be uploaded to the Shenzhen Nano-Jing Cloud Technology Co
    ., Ltd. server"
```

Impact: A user cannot tell from the listing which company decides about the data that the band and the update server collect.

Fix: State in the policy which company is the controller for the app and which for the update backend, and the roles under Art. 26 or Art. 28.

H3: An AI smart glasses assistant with meeting transcription, simultaneous interpretation and face translation ships inside a bracelet app, and the Play description mentions none of it

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 Play description says only that the smart bracelet application manages steps, records activities and fitness, tracks sleep and the menstrual cycle. The manifest holds activities under com.njj.mactivepro.ui.activity.smartGlasses for an AI glasses assistant (three variants), an AI voice assistant, meeting minutes (record, details), simultaneous interpretation (two variants, record, details), face translation (two variants), a recording list, AI translation and a glasses AI history. The assets hold the sherpa-ncnn bilingual Chinese and English streaming speech model, the Qwen tokenizer file qwen.tiktoken (2.4 MB) and ESRGAN.tflite. The native libraries include libsherpa-ncnn-core.so, libsherpa-ncnn-jni.so, libkaldi-native-fbank-core.so, libnative-multimodal-tongyimetathings.so, the TensorFlow Lite libraries, seven Microsoft Cognitive Services Speech libraries and the Alibaba NUI libraries libneonui_shared.so and libneonuijni_public.so. The bundled file assets/ali_nui.json sets service_mode to kModeFullCloud. Whether these modules are used in the product and what they send is UNVERIFIED.

```
AIGlassesAssistantActivity (3 variants), AiVoiceAssistantActivity,
MeetingMinutesActivity, MeetingMinutesRecordingActivity, MeetingDetailsActivity,
SimultaneousInterpretationActivity (2), SimultaneousRecordActivity,
    SimultaneousDetailsActivity,
FaceTranslationActivity (2), RecordingListActivity, AiTranslationActivity,
    GlassesAiHistoryActivity

assets/sherpa-ncnn-streaming-zipformer-bilingual-zh-en-2023-02-13/
assets/qwen.tiktoken
assets/ESRGAN.tflite
assets/ali_nui.json  "service_mode":"kModeFullCloud"
```

Impact: Meeting minutes and live interpretation record the voices of other people in a room, who never installed the app. A user who installs a bracelet app does not learn from the listing that voice and camera based translation tools are inside the same package.

Fix: Describe the AI and glasses features, their recipients and their recording behaviour in the listing and the policy, or ship them as a separate app.

M1: Only two personal mailboxes are published as contacts and no Article 27 representative or Data Protection Officer is named

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The Play support contact is fhjjbffhu@gmail.com. The contact in section 12 of the policy is HuangXiaoLong2023@163.com. Neither is a corporate domain. No phone number, Data Protection Officer or Union representative appears in the listing, the policy or the manifest. The listing shows more than 10 million downloads. The publisher is Shenzhen Horn Big Data Software Co.,Ltd, Room 301, Block B, Jiada R&D Building, No. 5 Songpingshan Road, Songpingshan Community, Xili Street, Nanshan District, Shenzhen. The signing certificate is the Google Play App Signing certificate (CN=Android, OU=Android, O=Google Inc.) and identifies nothing about the developer.

```
Support (Google Play)     fhjjbffhu@gmail.com
Privacy policy section 12  HuangXiaoLong2023@163.com
Publisher                 Shenzhen Horn Big Data Software Co.,Ltd
Server operator (policy 1.2)  Shenzhen Nano-Jing Cloud Technology Co., Ltd.
```

Impact: A person who wants access to health data or deletion has two private mailboxes to write to and no representative in the Union.

Fix: Name one controller, a corporate contact and an Article 27 representative in the Union.

M2: PEGI 3 rating, a policy that sets the minor threshold at 14 and no client side age gate in the resources

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

The Play listing carries PEGI 3. Section 7 of the policy says: although local laws and customs may define a minor differently, we consider anyone under the age of 14 to be a minor, and minors are prohibited from creating their own accounts without parental or guardian consent. A resource search for birthday, date_of_birth, parental, coppa, age_gate and under 14 returned no age check, blocking or parental consent string. The dex is packed, so a server side or code side age check cannot be seen. The absence is therefore not asserted. The app offers menstrual cycle and pregnancy tracking.

```
Google Play content rating: PEGI 3
Policy section 7: "we consider anyone under the age of 14 to be a minor ... Minors are
     prohibited from creating their own user accounts without parental or guardian
    consent."
```

Impact: A child can install an app that is rated for everyone and that offers menstrual cycle and pregnancy tracking.

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

M3: Google Maps, AutoNavi, AdMob and HIFIVE identifiers and a server code are hard-coded in the manifest

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

AndroidManifest.xml holds the meta-data entries below. They are client side keys by SDK design, and each is a quota or billing abuse surface if scraped. HIFIVE is a Chinese H5 mini game platform that the privacy policy SDK section does not name, so it points to an integration that the policy omits. The Tencent QQ AppID 1112047156 appears in the tencent1112047156 intent filter scheme. Restrictions on the keys could not be seen and were not tested.

```
<meta-data android:name="com.amap.api.v2.apikey" android:value="208
    a5aa9117f8a6f6d3b142fbc34164f"/>
<meta-data android:name="com.google.android.maps.v2.API_KEY" android:value="
    AIzaSyBQgrGkqQ4gjfXwMIoH5xKQUUVYLinZCJY"/>
<meta-data android:name="HIFIVE_APPID" android:value="5a89bd7617f94ca4b861995ed9100b5c
    "/>
<meta-data android:name="HIFIVE_SERVERCODE" android:value="c703601c48de4086b5"/>
<meta-data android:name="com.google.android.gms.ads.APPLICATION_ID" android:value="ca-
    app-pub-6152885277333401~3369557885"/>
```

Impact: Keys in a public package can be reused by others at the operator’s cost, and an integration that the policy omits cannot be assessed by the user.

Fix: Restrict the keys by package name and signature, rotate the HIFIVE server code and list the HIFIVE integration in the policy.

M4: The Jieli authentication and OTA libraries give the backend a firmware channel to the worn device

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

The Jieli libraries libjl_auth.so and libjl_ota_auth.so together with FirmwareOTAActivity, FirmwareUpdateActivity, JieLiOtaFromFileActivity and GlassesJieLiOTAActivity confirm a firmware update path from the app to the paired band or glasses. A firmware channel can change the behaviour of a worn device after install. Whether any channel beyond ordinary user initiated updates exists, and how commands are authorised, is UNVERIFIED because the dex is packed.

```
libjl_auth.so      SHA-256
    e695e324484ba9690c38293541b385f660b24769b3df64caff44402625b597aa
libjl_ota_auth.so  SHA-256 503
    b187a690d153e42fda622cbebff7ca46a337e6b63c6196b931beabbad8074
FirmwareOTAActivity, FirmwareUpdateActivity, JieLiOtaFromFileActivity,
    GlassesJieLiOTAActivity
```

Impact: The wearer trusts the update channel with the firmware of a device on the wrist or face.

Fix: Document who can push firmware, how images are signed and verified and that updates need user action.

Impact Analysis

The people affected are the users of a health and fitness companion with more than 10 million downloads. They wear a band, grant Bluetooth, location, phone, contacts, SMS, camera, microphone and notification access, and some record a menstrual cycle, a pregnancy, an ECG or blood pressure readings. Some are children, since the Play rating is PEGI 3. Contacts, callers and the people in a room where smart glasses record a meeting are affected as well.

The weight of the case sits on three points. The Data Safety card tells the users of 10 million installs that nothing is shared and that only device identifiers are collected, while the operator's policy lists far more (C1). The app permits plain HTTP and the policy says that data is stored in the People's Republic of China (C2). A set of AI and glasses features that the listing never mentions ships in the same package (H3).

What the package shows is configuration, file content and the operator's own text. No health reading, voice recording or personal field was observed leaving a device and the report asserts no such flow. The policy table names device identifiers, location, steps and advertising data as the data that the SDK vendors receive.

The Complete Chain

Step 1, listing: the user reads a description of steps, sleep and menstrual cycle tracking and a Data Safety card that says no data is shared and that only device identifiers are collected (C1).

Step 2, first start: Google ML Kit and Google Mobile Ads construct at process creation. No consent platform exists (C3).

Step 3, pairing and use: the user grants Bluetooth, location, phone, contacts, SMS and notification access. The listener and the call data can reconstruct who contacts the user (C3). Health activities record menstrual cycle, pregnancy, ECG and blood pressure data (C2). Smart glasses features can record meetings (H3).

Step 4, backend: the policy says that data is stored in the People's Republic of China and the app permits cleartext (C2). The advertising SDKs listed in the policy receive device identifiers and location (C1). The firmware channel can update the worn device (M4).

Step 5, rights: a person who wants access or deletion finds two personal mailboxes and no representative in the Union (M1).

Chipset SDK Cluster and Fingerprint Keys

The nine Jieli libraries below match by name the Jieli family recorded in the R1 findings of Fere Fit, FitPro, HumeHealth, Lefun Health and OnWear Pro in this programme, which are published by different companies under different signing identities. The hashes of this report were not diffed against those apps, so the correlation holds at library name level and a byte level comparison is the natural next step. The BLE service UUIDs and device identity constants could not be extracted because of the packer.

```
e695e324484ba9690c38293541b385f660b24769b3df64caff44402625b597aa  libjl_auth.so
8cd3b9dc44f86b37ae6aa7ae226d0ae3f87404297715f1ebe4370dddbe0d4236  libjl_bmp_convert.so
8a6b1c791fce5a9f8e0e8cca262f52e2854e9fad92a5ad943f2af0133e4a5020  libjl_crc.so
b4aba62bcb4ccfd3f86d86fa48360d32eb7a11f09d989b24638658f41db07277  libjl_enc.so
0794b2f63b9388f4233b2101f41796f8b7604cbeb66d0ed8f94e57a8ef13e1cb  libjl_fatfs.so
26d9a6561cb523dee7a95146530fd8edb6bc5ccdb158ad2979f04c370496e837  libjl_opus.so
503b187a690d153e42fda622cbebff7ca46a337e6b63c6196b931beabbad8074  libjl_ota_auth.so
3d1618dd2c07d0132ebce7c96f033de8218413cf37818ba2ccb83260464e6dac  libjl_pack_format.so
539e04d7a4308cd6995e57be5ac25676b2166fa7ddf01ae7c412409b53d80605  libjl_speex.so

libjiagu.so          4dd617b06fc16023e0c2166db1bea669b6876252088b535ce91e6f9e49749e1b
Signing cert SHA-256 275d00b47de3f86651433fbd71b98afcfa601f43fe9d65cda55d9746d6f38bdc
Signing cert SHA-1   54fdf1b44c06ebf855ae2b811af885d4ce11f9dd
Signing DN           CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=
    California, C=US (Google Play App Signing)
```

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C3, H3 and M1.

Article 5(1)(b), purpose limitation: engaged by H3 as an open question.

Article 5(1)(c), data minimisation: engaged by C3 and M4.

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

Article 5(2), accountability: engaged by C1 and, as a verifiability point, by H1 and H2.

Article 6(1) and Article 7(1): engaged by C3.

Article 8: engaged by M2.

Article 9: engaged by C2 for menstrual cycle, pregnancy, ECG and blood pressure data. A religious practice is engaged only if Qibla use is recorded, which is UNVERIFIED. Article 9 is an open question for H3 and, as indirect inference, for C3.

Articles 12(1), 13 and 14: engaged by C1 and H3. Article 13(1)(a) is engaged by M1 and H2.

Article 25: engaged by M4.

Article 27: engaged by M1. No representative is named.

Article 28: engaged by H2 as an open question on the roles of the two companies.

Articles 44 and 46: engaged by C2. The policy states storage in the People's Republic of China and names no transfer mechanism.

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 was read on 23 August 2026. It says: No data shared with third parties, This app may collect these data types: Device or other IDs, Data isn't encrypted and You can request that data be deleted. The statement that data is not encrypted matches the cleartext configuration of C2. The statement that no data is shared and the list of one data category do not match the operator's own policy (C1).

Regulatory & Legal Landscape

Shenzhen Horn Big Data Software 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.njj.mactivepro
Version            2.0.0 (versionCode 20000), minSdk 27, targetSdk 36, compileSdk 36
XAPK SHA-256       ade4e3a00f2e537966bc2ad48494b11f202ab6edb9c8742e22d71bf64b83a323
base APK SHA-256   078c8dbd38555f4ecd36ae615ba55cde8ec599733527eba7270a7b6550d34ead
    (100,190,475 bytes)
native split SHA-256 78e2b4ecf081090cafaa35764cbb4a29de463ec307419780f2d747800686b995
      (config.armeabi_v7a.apk, 156,153,054 bytes)
Signing cert SHA-256 275d00b47de3f86651433fbd71b98afcfa601f43fe9d65cda55d9746d6f38bdc
Signing cert SHA-1   54fdf1b44c06ebf855ae2b811af885d4ce11f9dd
Audit device       none, the app was not installed
Acquisition        APKPure mirror (d.apkpure.com), checked against the Google Play
    listing, 2026-08-23
```

```
Amap API key          208a5aa9117f8a6f6d3b142fbc34164f
Google Maps API key   AIzaSyBQgrGkqQ4gjfXwMIoH5xKQUUVYLinZCJY
HIFIVE_APPID          5a89bd7617f94ca4b861995ed9100b5c
HIFIVE_SERVERCODE     c703601c48de4086b5
AdMob application ID  ca-app-pub-6152885277333401~3369557885
Tencent QQ AppID      1112047156
Policy                https://download.microwear.com/mactiveproen.html
Contacts              fhjjbffhu@gmail.com, HuangXiaoLong2023@163.com
Server operator       Shenzhen Nano-Jing Cloud Technology Co., Ltd. (policy section
    1.2)
```

```
C1  Google Play Data Safety card, operator privacy policy sections 1 and 6,
    AndroidManifest.xml (permissions)
C2  res/xml/network_security_config.xml, AndroidManifest.xml, policy section 2.1, res/
    values/strings.xml
C3  AndroidManifest.xml (providers, NJJNoticeService)
H1  AndroidManifest.xml (com.stub.StubApp), lib/armeabi-v7a/libjiagu.so, classes.dex
    string pool
H2  lib/armeabi-v7a/libjl_*.so, policy section 1.2, policy host
H3  AndroidManifest.xml (smartGlasses activities), assets, lib/armeabi-v7a
M1  Google Play listing, policy section 12
M2  Google Play listing, policy section 7, res/values/strings.xml
M3  AndroidManifest.xml (meta-data)
M4  AndroidManifest.xml, libjl_auth.so, libjl_ota_auth.so
```

Reproduction: obtain com.njj.mactivepro 2.0.0 (20000), check the SHA-256 values above, decode the manifest and resources with apktool and list the native libraries of the architecture split. No device, account or network access is needed. Reading the application code needs dynamic unpacking, which was not done.

Disclosure Timeline & Outcome

2026-08-23 Notice REF MACTIVEPRO-2026-R1 at 07:17 UTC to fhjjbffhu@gmail.com and HuangXiaoLong2023@163.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Three critical findings, the packer and cluster findings, three questions, embargo date 21 November 2026.

2026-09-12 Follow-up to both addresses at 17:02 UTC. It restated the three critical findings and the three questions with answers due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:06 UTC, under the subject 35 days to publication: MActivePro.

2026-11-14 No reply of any kind and no delivery failure. The mailbox holds no inbound message from the operator.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

What Was Done Well

A privacy policy exists and is unusually detailed. It runs to about 9,000 words in 12 numbered sections with a table of collected personal information and a named SDK table, and it is what makes the Data Safety mismatch visible. A deletion request path is stated on the Data Safety card and in the policy section on user rights. The policy sets a minor threshold at 14 and states a commitment to delete data of unverified minors. The app targets API level 36 and the Play update of 6 August 2026 is recent.

Residual Risk & Recommendations

Open at the date of publication: all ten entries. The operator has not replied and the build analysed is version 2.0.0 of August 2026. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, correct the Data Safety declaration to match the policy and the manifest (C1). Second, remove the cleartext allowance and name the Chapter V mechanism and the Article 9(2) basis for health data (C2). Third, gate the SDKs on a recorded consent decision and add a consent platform (C3). Fourth, describe the AI and glasses features and their recipients (H3). Fifth, name one controller, a corporate contact and an Article 27 representative (M1, H2). Sixth, restrict the keys, align the rating with the feature set and document the firmware channel (M2 to M4).

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 MACTIVEPRO-2026-R1.