Security & Privacy Disclosure, Final Report

Haylou Watch for Android (com.smart.haylou)

A Play label that says no data is shared, six third-party platforms in the package and exclusive storage in mainland China, with no reply since the notice.

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

Target	Dongguan Liesheng Electronic Technology Co., Ltd. (Haylou Watch)
Versions Audited	2.0.5.3 / versionCode 7308 (updated 2025-11-26, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	12: 1 High, 6 Medium, 3 Low, 2 observations (R1 labels re-assessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`f440df40de1236634a400b44855b267a0111dff50be3abb73bf6b4e4efa31128`

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 Play Data Safety panel says no data is shared with third parties and the package links six third-party platforms . . . 7

6.2 C2: Cleartext traffic permitted for the whole app, no certificate pinning, on an app with SMS, call log, contacts, location, camera and microphone permissions 8

6.3 C3: The bundled privacy text states that all user data is stored only on Alibaba Cloud servers in mainland China, and no Article 27 representative is named . . 9

6.4 H1: Shared SmartV3 platform with a hard-coded route to a second brand, third Bluetrum cluster member . . . 10

6.5 H2: Contacts, call log and SMS content are pushed to the watch, which is third-party data . . . 11

6.6 H3: Notification listener with system-wide notification access . . . 12

6.7 H4: Exported microphone service and exported MQTT service, both without a protecting permission . . . 13

6.8 H5: Live voice pipeline to a fixed United States Azure region . . . 14

6.9 M1: The bundled text names two minimum ages, 18 and 16, in a PEGI 3 app with no age gate . . . 14

6.10 M2: Google Maps key in the resource table . . . 15

6.11 M3: Development, test and staging artifacts compiled into the production build 15

6.12 M4: Signature-level permissions declared that a Play-distributed app cannot be granted . . . 16

7 Impact Analysis 16

8 The Complete Chain 17

9 Shared Chipset or Platform Fingerprint 17

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 18

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

Haylou Watch (package com.smart.haylou) is the companion app of Haylou smartwatches. It is published on Google Play by Dongguan Liesheng Electronic Technology Co., Ltd., has more than 100 thousand installs and carries PEGI 3. On 23 August 2026 RFI-IRFOS sent a notice with REF HAYLOUWATCH-2026-R1 to haylouls123@gmail.com, service@haylou.com and asmsservice@outlook.com, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

The Google Play Data Safety panel states No data shared with third parties. The root level code analysis of version 2.0.5.3 finds linked integrations with Microsoft Azure Speech, OpenAI, Alibaba Cloud, Baidu, Tencent and Sina Weibo (C1). The privacy text bundled in the app says that all user data is stored only on Alibaba Cloud servers in mainland China and names no Article 27 representative (C3). Cleartext traffic is permitted for the whole app on a product with SMS, call log, contacts, location, camera and microphone permissions, which makes it the one finding that stays at High (C2). The package contains an exported microphone service and an exported MQTT service without a permission (H4), a voice pipeline to a fixed United States Azure region (H5) and a notification listener (H3). The internal package com.sma.smartv3 and a route to the backend of a second brand show a shared platform (H1).

A reassessment by CVSS v4.0 band puts six findings at Medium, three at Low and one at High, with two observations left unrated. The three findings disclosed as Critical move to Medium, High and Medium because the package shows the integrations, the permissive setting and the operator's own storage statement, and does not show a data flow. Haylou Watch is the third member of the Bluetrum cluster after HryFine and Wearfit Pro.

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 2.0.5.3 (versionCode 7308), obtained as an XAPK bundle (base APK and two config splits) from a download mirror and matched to the live Google Play listing on package ID, app name, developer name and description. Work done: manifest and resources decoded without a source decode (apktool) and a string pass across all twelve classes dex files. The Google Play listing and Data Safety page were read on 23 August 2026. No external privacy policy URL was found in the package or the listing, and the policy text bundled in the app was read instead. 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. Anything that depends on runtime behaviour is marked as such.

ID	Severity	Title
C1	MEDIUM	The Play Data Safety panel says no data is shared with third parties and the package links six third-party platforms
C2	HIGH	Cleartext traffic permitted for the whole app, no certificate pinning, on an app with SMS, call log, contacts, location, camera and microphone permissions
C3	MEDIUM	The bundled privacy text states that all user data is stored only on Alibaba Cloud servers in mainland China, and no Article 27 representative is named
H1	INFO	Shared SmartV3 platform with a hard-coded route to a second brand, third Bluetrum cluster member
H2	MEDIUM	Contacts, call log and SMS content are pushed to the watch, which is third-party data
H3	MEDIUM	Notification listener with system-wide notification access
H4	MEDIUM	Exported microphone service and exported MQTT service, both without a protecting permission
H5	MEDIUM	Live voice pipeline to a fixed United States Azure region
M1	LOW	The bundled text names two minimum ages, 18 and 16, in a PEGI 3 app with no age gate
M2	LOW	Google Maps key in the resource table
M3	LOW	Development, test and staging artifacts compiled into the production build
M4	INFO	Signature-level permissions declared that a Play-distributed app cannot be granted

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Data flow per vendor not traced.
C2	CRITICAL	HIGH	No reply. Kept at High by blast-radius escalation, computed band Medium.
C3	CRITICAL	MEDIUM	No reply. Operator text names exclusive PRC storage.
H1	HIGH	INFO	Not rated. Platform and chipset fingerprint.
H2	HIGH	MEDIUM	No reply. Destination of call and SMS content not shown.
H3	HIGH	MEDIUM	No reply. Destination of notification content not shown.
H4	HIGH	MEDIUM	No reply. Behaviour on start not shown.
H5	HIGH	MEDIUM	No reply. Reachability in the user interface not tested.
M1	MEDIUM	LOW	No reply. Server side age check not excluded.
M2	MEDIUM	LOW	No reply. Restriction state not visible.
M3	MEDIUM	LOW	No reply. Hosts not reachable externally.
M4	MEDIUM	INFO	Not rated. Dead manifest entries.

Subject & Operator Analysis

Haylou Watch is published by Dongguan Liesheng Electronic Technology Co., Ltd. of Dongguan, Guangdong. The support email on the Play listing is the private Gmail address haylouls123@gmail.com, the in-app feedback address is service@haylou.com and a third address, asmsservice@outlook.com, sits in the resources as a platform contact. No postal address, phone number, data protection officer or Article 27 representative was found, and no external privacy policy URL exists.

The internal package of the whole app is com.sma.smartv3 and the signing certificate names CN=sma, OU=smalife, O=sma in Shenzhen. A Croatian locale file calls the app SmartV3-Android. The platform is a white-label code base with several storefronts (H1). Hosts in the package point to further brand names that were not investigated here, among them codingiot.net/cofit, 10m, vtio and zewa.

A controller without an establishment in the Union is not covered by the one-stop-shop mechanism. The Austrian Datenschutzbehörde received the notice in copy.

Architecture & Data Flow

Haylou Watch is a native Android app with twelve classes dex files, targeting API level 35 with a minimum of API level 21. The code base lives under com.sma.smartv3 and the band side uses the Bluetrum OTA stack (abota and fota modules) and custom GATT UUIDs. The package also holds endpoints of MediaTek firmware delivery and u-blox GNSS assistance, which suggests more than one chipset vendor in the supply chain.

On the network side the package holds Alibaba Cloud OSS and IoT Hub, an instance-specific MQTT broker, Microsoft Azure Speech with a fixed United States region, OpenAI chat completions, Baidu map and location, Tencent login and Sina Weibo share (C1). The network configuration permits cleartext for all hosts (C2). The app bundles its own privacy text (C3). Two exported services expose the microphone and the MQTT client to other apps (H4). The manifest sets allowBackup to false.

Engagement Summary

The notice REF HAYLOUWATCH-2026-R1 was sent on 23 August 2026 at 00:28 UTC from rfi.irfos@gmail.com to haylouls123@gmail.com, service@haylou.com and asmsservice@outlook.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried three critical findings, the platform finding and further findings with evidence, and three questions. A follow-up of 12 September 2026 restated the open findings and set 19 September 2026 as the date for the three questions. A second follow-up of 17 October 2026 came from security@rfi-irfos.com. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: The Play Data Safety panel says no data is shared with third parties and the package links six third-party platforms

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 23 August 2026

The Google Play Data Safety panel of com.smart.haylou, read on 23 August 2026, states No data shared with third parties and lists as collected Contacts, Personal info (Name, Email address, User IDs, Other info), Photos, Audio (Music files), Health and fitness (Fitness info) and Messages (SMS or MMS). The dex files of version 2.0.5.3 contain linked classes and endpoint literals of Microsoft Azure Cognitive Services Speech (AudioConfig, AudioInputStream, MicrophoneArrayGeometry, PullAudioInputStream), the OpenAI endpoint api.openai.com/v1/chat/completions, the Alibaba Cloud OSS client and IoT Hub, the Baidu map, location and Yingyan suite, the Tencent WeChat OpenSDK and QQ Connect and the Sina Weibo share SDK. These integrations work by passing data to the vendor, for example audio to the speech service, queries to the map service and tokens to the login services. Which data reaches which vendor in a given session was not traced, and the declaration to Google may rest on a reading of the term share that the report does not know. The finding is the gap between the label and the package.

```
Lcom/microsoft/cognitiveservices/speech/*      (Azure Cognitive Services Speech, audio
     classes)
api.openai.com/v1/chat/completions                (OpenAI Chat Completions)
Lcom/alibaba/sdk/android/oss/OSSClient
  oss.aliyuncs.com, oss-cn-hangzhou.aliyuncs.com, oss-cn-shenzhen.aliyuncs.com, oss-
    accelerate.aliyuncs.com,
  sma-product.oss-accelerate.aliyuncs.com, 10mlove.oss-cn-shenzhen.aliyuncs.com
  iothub.aliyuncs.com, iot-auth.cn-shanghai.aliyuncs.com, iot-06z00c6kgq6t1w4.mqtt.
    iothub.aliyuncs.com
Lcom/baidu/mapapi/*, Lcom/baidu/location/*, Lcom/baidu/lbsapi/*
  api.map.baidu.com, loc.map.baidu.com, yingyan.baidu.com, openapi.baidu.com, app.navi
    .baidu.com
Lcom/tencent/mm/opensdk/*, Lcom/tencent/connect/avatar/*
  open.weixin.qq.com, cgi.connect.qq.com, openmobile.qq.com, appsupport.qq.com
Lcom/sina/weibo/sdk/api/*
  api.weibo.com, open.weibo.cn
```

Impact: The label is the place where a user decides whether to install a health and message app. A user who reads that no data is shared does not learn that voice audio, location queries and login tokens go to platforms of six companies.

Fix: Align the Data Safety declaration with the integrations, name each recipient and the data it receives in the policy and remove integrations the product does not use.

C2: Cleartext traffic permitted for the whole app, no certificate pinning, on an app with SMS, call log, contacts, location, camera and microphone permissions

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

The manifest points the application to res/xml/network_config.xml, which consists of a base-config with cleartextTrafficPermitted set to true and nothing else. No pin-set and no domain-scoped exception exists in res/xml. A second file, res/xml/network_security_config.xml, sits in the resource tree and is not the one the manifest references. The app targets API level 35, where cleartext HTTP is refused by default, so this file switches that protection off for every host. The app holds READ_SMS, READ_CALL_LOG, READ_CONTACTS, ACCESS_FINE_LOCATION, ACCESS_BACKGROUND_LOCATION, CAMERA and RECORD_AUDIO, and C1 lists the endpoints it talks to. Whether a given endpoint is called over plain HTTP was not tested and no traffic was captured. The score reflects an attacker on the same network path and the need for the app to use an http:// address. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the app is positioned to carry voice audio, location, message content, contacts and call log, the override covers every host including the speech, chat and cloud endpoints of C1, and no per-domain exception limits it.

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

Impact: The app is positioned to carry voice audio, location, text message content, contacts and call log. A global cleartext allowance means that a plain HTTP request to any host travels in the open on a shared Wi-Fi network or a hostile access point. For a person who wears the watch all day, the data at stake is the most personal kind a phone holds.

Fix: Remove the base-config override, allow cleartext only for named hosts that need it, pin the first-party hosts and verify that every endpoint in the dex strings uses https.

C3: The bundled privacy text states that all user data is stored only on Alibaba Cloud servers in mainland China, and no Article 27 representative is named

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 23 August 2026

The app bundles its privacy text as the string resource privacy_info_content and does not link to an external policy. Section 6.9 of that text says that the product service side is used by China Ali Cloud Company, that the information related to the user is only stored on Ali Cloud servers and that the operator does not store relevant materials locally. The dex endpoints agree with it: Alibaba Cloud OSS in Hangzhou and Shenzhen, IoT authorisation in Shanghai and an instance-specific IoT Hub MQTT broker. The text carries the unsubstituted placeholder %s (Or We) in place of the operator name, which shows an unedited template. It also states compliance with the GDPR and COPPA. No transfer mechanism, no transfer impact assessment and no Article 27 representative is named in the text, the Play listing or the package. The report does not assess PRC law. The finding is the absence of a named mechanism next to the operator's own statement of exclusive storage in the PRC.

```
6.9 We's Product Service Side Is Used By China Ali Cloud Company (Ali Cloud) Server,
    Its Official Website
Access Address Is: Https://Www.Aliyun.Com/. The Information And Materials Related To
    You In The We's App
Products Are Only Stored On Ali Cloud Servers, And We Does Not Store Relevant
    Materials Locally.

we Comply With The Requirements Of The Eu General Data Protection Regulation (Gdpr)
    And The Children's
Online Privacy Protection Act (Coppa). We Services Are Available For People At Least
    16 Years Of Age
Or Above.
```

Impact: A person in the Union who wears the watch is told in the operator's own words that their information lives only on servers in mainland China. The text names no safeguard and no one to ask in the Union.

Fix: Name the controller with a postal address and an Article 27 representative, state the transfer mechanism and publish the transfer impact assessment.

H1: Shared SmartV3 platform with a hard-coded route to a second brand, third Bluetrum cluster member

INFO, no CVSS v4.0 score assigned, observation, not rated, disclosed as HIGH on 23 August 2026

The internal Java package of the whole application is com.sma.smartv3, not the Play package com.smart.haylou, and the signing certificate names CN=sma, OU=smalife, O=sma. The Croatian locale file res/values-hr-rHR/strings.xml sets app_name to SmartV3-Android. The dex files hold the URL templates https://ali-cloud.beatxp.com/kotlinweb, https://api-c.iot-solution.net/kotlinweb and https://api-eg.iot-solution.net/kotlinweb in one code region, and the resources hold the string beatxp_new_app_tip. BeatXP is an independently marketed wearable brand, and a corporate link to the operator of Haylou Watch was not found. The shared route shows one code base behind more than one storefront. The package also ships the Bluetrum SDK (abota and fota modules), which makes Haylou Watch the third member of the Bluetrum cluster after HryFine and Wearfit Pro. The shared platform changes the unit of a data protection impact assessment from one app to the platform. No exposure follows from it, so the report records it as an observation and does not rate it.

```
com.sma.smartv3.ble.MyNotificationListenerService
com.sma.smartv3.biz.VoiceService
com.sma.smartv3.ui.launcher.LauncherActivity
Signing DN: CN=sma, OU=smalife, O=sma, L=shenzhen, ST=guandong, C=86
res/values-hr-rHR/strings.xml: <string name="app_name">SmartV3-Android</string>

https://ali-cloud.beatxp.com/kotlinweb
https://api-c.iot-solution.net/kotlinweb
https://api-eg.iot-solution.net/kotlinweb
beatxp_new_app_tip

Lcom/bluetrum/abota/bluetooth/BleManager, BluetoothSppService, SppManager
Lcom/bluetrum/fota/abota/ABOta, ABOtaManager
Lcom/bluetrum/fota/manager/OtaCommandGenerator, OtaConstants
```

Impact: A user or an authority who looks at the Haylou listing alone does not see that the same platform serves other brands, so the question of who answers for the processing stays open.

Fix: Name the controller of the platform, assess it as one processing operation and list the brands it serves.

H2: Contacts, call log and SMS content are pushed to the watch, which is third-party data

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 requests READ_CONTACTS, READ_CALL_LOG, READ_SMS and ANSWER_PHONE_CALLS. The Play description says: We will push the phone call and text message content to the watch to prevent you from missing key information (this feature requires your authorization). The caller or sender who appears in a pushed notification is not the account holder and saw no consent screen. Whether the content stays on the Bluetooth link to the paired watch or also reaches the operator's cloud is not shown. The Alibaba Cloud and account architecture in the package makes the second reading possible, and no bytecode control-flow pass was done.

```
Permissions: READ_CONTACTS, READ_CALL_LOG, READ_SMS, ANSWER_PHONE_CALLS
"We will push the phone call and text message content to the watch to prevent you from
     missing key information (this feature requires your authorization)."
```

Impact: People who call or text the user have their number, name and message text shown on another device without having agreed to anything.

Fix: State in the policy that call and message content stays on the Bluetooth link, or name the recipient and the legal basis if it leaves the phone.

H3: Notification listener with system-wide notification access

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 com.sma.smartv3.ble.MyNotificationListenerService with BIND_NOTIFICATION_LISTENER_SERVICE. The service is marked exported, which the system permission limits to the operating system as binder. A bound listener sees sender, source app and text of every notification, which is enough to derive who messages the user and how often. Whether the parsed content stays on the Bluetooth link or reaches the backend is not shown.

```
<service android:exported="true" android:label="@string/app_name"
         android:name="com.sma.smartv3.ble.MyNotificationListenerService"
         android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action android:name="android.service.notification.NotificationListenerService
    "/>
    </intent-filter>
</service>
```

Impact: Message previews of other people, including banking alerts and codes, pass through the app. Those people never agreed.

Fix: Restrict the listener to the apps the user selects and state that message content stays on the Bluetooth link.

H4: Exported microphone service and exported MQTT service, both without a protecting permission

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 23 August 2026

The manifest declares com.sma.smartv3.biz.VoiceService with foregroundServiceType microphone, exported true, no android:permission attribute and stopWithTask true. It also declares org.eclipse.paho.android.service.MqttService, exported true and without a permission, which is the client for the Alibaba Cloud IoT Hub broker of C3. Any other app on the phone can try to start or bind both components. What a start does is not shown, since no other app was used to invoke either component and no bytecode control-flow pass was done. The score assumes a local attacker app and a user action that installs it.

```
<service android:enabled="true" android:exported="true" android:foregroundServiceType
    ="microphone"
         android:name="com.sma.smartv3.biz.VoiceService" android:stopWithTask="true"/>
<service android:enabled="true" android:exported="true"
         android:name="org.eclipse.paho.android.service.MqttService"/>
```

Impact: A component that handles the microphone and one that holds the link to the cloud command channel are open to every app on the phone. The user has no way to see or close that door.

Fix: Set exported to false on both services or protect them with a signature permission.

H5: Live voice pipeline to a fixed United States Azure region

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 app requests RECORD_AUDIO. The dex files hold the Azure Speech audio classes, native AudioRecord use and the region string eastus in classes9.dex. The speech SDK, the OpenAI endpoint of C1 and the AI user interface package com.sma.smartv3.ui.ai point to a voice assistant or dictation feature. A search of the dex strings for audio feature extraction found four matches for mfcc, and all four sit inside obfuscated class names that have nothing to do with audio. No audio classification path is asserted. With a fixed region string, the voice of a user in the Union is processed in a United States datacenter, which is a transfer beside the PRC storage of C3. Voice for dictation is not special category data without evidence of health inferences, and the analysis found none. Whether the feature is reachable in the user interface was not tested.

```
RECORD_AUDIO (manifest)
Lcom/microsoft/cognitiveservices/speech/audio/AudioConfig, AudioInputStream,
    MicrophoneArrayGeometry, PullAudioInputStream
region string: eastus   (classes9.dex)
```

Impact: What a person says to the watch assistant goes to a datacenter in the United States, and the notice names neither the country nor the safeguard.

Fix: State the region, the recipient and the transfer mechanism, and offer an EU region.

M1: The bundled text names two minimum ages, 18 and 16, in a PEGI 3 app with no age gate

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 bundled privacy text says that the app is only for users who are at least 18 years old and, in another clause, that services are available for people at least 16 years of age. Google Play rates the app PEGI 3. A search of the resources found no birth date field, age check or parental step. Neither stated age is enforced in the resources. An age check on the server would not appear in the package.

```
"this App Is Only For Users Who Are At Least 18 Years Old And Above. If You Are Under
    18 Years Of Age, Please Do Not Use This App."
"... We Services Are Available For People At Least 16 Years Of Age Or Above."
Google Play content rating: PEGI 3
```

Impact: A child can install a product rated for everyone and finds two different age limits in its legal text.

Fix: State one minimum age, enforce it and align the rating.

M2: Google Maps key in the resource table

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), disclosed as MEDIUM on 23 August 2026

res/values/strings.xml carries a Google Maps key that apktool extracts in under a minute. The restriction state of the key cannot be seen from the package, and the burden of showing it lies with the operator under Art. 5(2). No Firebase project ID, sender ID or Crashlytics key was found. The five Firebase namespace hits trace to relocated build tooling classes. No request was made with the key.

```
<string name="google_map_common_key">AIzaSyBBKD9ZhHDhS4lUL0_Aa2WHCeUhzW680Aw</string>
```

Impact: A key for maps lets a third party use the operator's quota, which affects availability and cost and not user data.

Fix: Restrict the key by package name and signing certificate, set a quota and rotate it.

M3: Development, test and staging artifacts compiled into the production build

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), disclosed as MEDIUM on 23 August 2026

The dex string pool of the published build holds at least three development or test hosts and four private or loopback addresses. None of them is reachable from outside the developer network. They show that the release process does not remove development artifacts.

```
ceshi.smawatch.cn          (ceshi means test)
dev.iot-solution.net   dev-oss.iot-solution.net   test-oss.iot-solution.net
zewadev.smartdevices.health
192.168.50.12   192.168.0.240   192.168.1.88   127.0.0.1   localhost
```

Impact: A release that carries test hosts shows weak separation between test and production, which is where mistakes in data handling start.

Fix: Strip test hosts and private addresses in the release build.

M4: Signature-level permissions declared that a Play-distributed app cannot be granted

INFO, no CVSS v4.0 score assigned, observation, not rated, disclosed as MEDIUM (informational) on 23 August 2026

The manifest requests READ_PRIVILEGED_PHONE_STATE and BLUETOOTH_PRIVILEGED, which are signature or privileged permissions, and DISABLE_KEYGUARD. Android denies the first two to any app that is not signed with the platform key or installed as a privileged system app, so they have no function in a Play build. A search of the dex strings found no dedicated handling code. The entries look like manifest inheritance from a source tree that also exists as preloaded firmware. The report records the entries as provenance and does not rate them.

```
<uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATE"/>
<uses-permission android:name="android.permission.BLUETOOTH_PRIVILEGED"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
```

Impact: No processing capability follows from the declarations on a standard device.

Fix: Remove permissions that have no function on the target platform.

Impact Analysis

The people affected are the users of a smartwatch companion app with more than 100 thousand installs, which includes minors under the PEGI 3 rating. The app handles contacts, call log, text messages, location, voice and fitness data, and shows message content from other people on a second device.

The weight of the case sits on three points. The Play label says that nothing is shared while the package links six third-party platforms (C1). The operator’s own text says that all data lives on Alibaba Cloud servers in mainland China, with no safeguard and no representative named (C3). Cleartext traffic is permitted for every host (C2).

The package shows integrations, endpoints, permissions and text. No voice recording, message or location was observed leaving a device, and the report asserts no such flow.

The Complete Chain

Step 1, install: a user installs the app after reading a label that says no data is shared (C1).

Step 2, pairing: the app pairs a watch over Bluetooth through the Bluetrum stack (H1).

Step 3, features: call and message content is pushed to the watch (H2), notifications are mirrored (H3) and a voice assistant sends audio to a United States Azure region (H5).

Step 4, network: traffic goes to Alibaba, Baidu, Tencent, Microsoft and OpenAI hosts (C1) and cleartext is allowed for all of them (C2). The operator states that data is stored only in mainland China (C3).

Step 5, local exposure: other apps on the phone can start the microphone service and the MQTT service (H4).

Step 6, rights: a person who wants to ask who holds the data finds a private Gmail address and a template text with no operator name (C3).

Shared Chipset or Platform Fingerprint

Haylou Watch is a SmartV3 platform build. The Bluetrum reference SDK appears as the abota and fota modules, which are different modules from the abpartool module of HryFine and Wearfit Pro. The vendor identity is the fingerprint and each licensee enables its own modules. The signing certificate does not match the certificates of HryFine or Wearfit Pro, which each sign their own builds. The malformed country code C=86 (a calling code, not an ISO 3166-1 code) echoes the code C=81 in the certificate of WearFit2.0. Whether this points to a shared certificate tool is an open observation. The GATT UUID family below is recorded as a candidate fingerprint and was not compared with the other apps.

```
Bluetrum classes      Lcom/bluetrum/abota/bluetooth/BleManager, BluetoothSppService,
    SppManager, Lcom/bluetrum/fota/abota/ABOta, ABOtaManager, Lcom/bluetrum/fota/
    manager/OtaCommandGenerator, OtaConstants
GATT UUID family      a6ed0401-d344-460a-8075-b9e8ec90d71b to a6ed0404-d344-460a-8075-
    b9e8ec90d71b, a6ed0701-d344-460a-8075-b9e8ec90d71b to a6ed0703-d344-460a-8075-
    b9e8ec90d71b
Short vendor UUIDs    0000ff12-0000-1000-8000-00805f9b34fb, 0000ff14
    -0000-1000-8000-00805f9b34fb, 0000ff15-0000-1000-8000-00805f9b34fb
Hardware fields       device_model, product_id, productId, vendorId, firmware_version,
    getManufacturerSpecificData
Other chip vendors    wepodownload.mediatek.com (MediaTek OTA), alp.u-blox.com (u-blox
    GNSS assistance)
Signing cert SHA-256  22
    f1cfbef897405e5de13d0e86d42e939b8de7c0789025eb9d2d26b8cda54083
Signing DN            CN=sma, OU=smalife, O=sma, L=shenzhen, ST=guandong, C=86
Internal package      com.sma.smartv3.* (application ID com.smart.haylou)
Cross-brand route     https://ali-cloud.beatxp.com/kotlinweb (resource string
    beatxp_new_app_tip)
Brand fragments       www.codingiot.net/cofit/, 10mlove.oss-cn-shenzhen.aliyuncs.com,
     server.10m.com.cn, vtbia.vtio.cn, vtutil-factory.vtio.cn, zewadev.smartdevices.
    health
```

Data Protection: Article by Article

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

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

Article 5(2), accountability: engaged by C1, H1 and M2.

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

Article 8, children: engaged by M1.

Articles 12(1), 13(1) and 14: engaged by C1 and H2. Article 13(1)(f) is engaged by H5.

Article 25: engaged by C2, H3, H4, M1, M2 and M3.

Article 27: engaged by C3. No representative is named.

Article 32(1)(a) and (b): engaged by C2, H4 and M2.

Article 35: engaged by C3 and H1. A data protection impact assessment is not published.

Articles 44 and 46: engaged by C3 and H5.

Platform Accountability & DSA

The Data Safety label of Haylou Watch says that no data is shared with third parties, that data is encrypted in transit and that deletion can be requested. It lists Contacts, Personal info, Photos, Audio, Health and fitness and Messages as collected. The package links six third-party platforms (C1) and permits cleartext for every host (C2), so the first two statements stand against the package. The label was not re-read after 23 August 2026.

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

Regulatory & Legal Landscape

The operator 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 and 8, 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.

The notice raised the access powers that PRC law gives to PRC-domiciled processors as a risk factor for Chapter V. The report records it as context and does not assess PRC law. 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.smart.haylou
Version            2.0.5.3 (versionCode 7308), minSdk 21, targetSdk 35
XAPK SHA-256       30ed150e397fd47e8b2da352d14e36b0566b536582a38a7802c3140be756df8e
    (110,059,853 bytes)
Base APK SHA-256   f440df40de1236634a400b44855b267a0111dff50be3abb73bf6b4e4efa31128
    (89,729,013 bytes)
Signing cert SHA-256  22f1cfbef897405e5de13d0e86d42e939b8de7c0789025eb9d2d26b8cda54083
Audit device       none, the app was not installed
```

```
Google Maps key      AIzaSyBBKD9ZhHDhS4lUL0_Aa2WHCeUhzW680Aw
MQTT broker        tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
Alibaba IoT        https://iot-auth.cn-shanghai.aliyuncs.com, iothub.aliyuncs.com
Alibaba storage    oss.aliyuncs.com, oss-cn-hangzhou.aliyuncs.com, oss-cn-shenzhen.
    aliyuncs.com, oss-accelerate.aliyuncs.com, sma-product.oss-accelerate.aliyuncs.com
    , 10mlove.oss-cn-shenzhen.aliyuncs.com
OpenAI             https://api.openai.com/v1/chat/completions
Azure Speech       region string eastus (classes9.dex)
Baidu              api.map.baidu.com, loc.map.baidu.com, yingyan.baidu.com, openapi.
    baidu.com, app.navi.baidu.com
Tencent            open.weixin.qq.com, cgi.connect.qq.com, openmobile.qq.com,
    appsupport.qq.com
Sina Weibo         api.weibo.com, open.weibo.cn
Cross-brand        https://ali-cloud.beatxp.com/kotlinweb, https://api-c.iot-solution.
    net/kotlinweb, https://api-eg.iot-solution.net/kotlinweb
Test hosts         ceshi.smawatch.cn, dev.iot-solution.net, dev-oss.iot-solution.net,
    test-oss.iot-solution.net, zewadev.smartdevices.health, 192.168.50.12,
    192.168.0.240, 192.168.1.88, 127.0.0.1, localhost
Contacts           haylouls123@gmail.com, service@haylou.com, asmsservice@outlook.com
```

```
C1  dex string pool (SDK namespaces and hosts), Google Play Data Safety page
C2  res/xml/network_config.xml, AndroidManifest.xml (networkSecurityConfig)
C3  res/values/strings.xml (privacy_info_content), dex string pool
H1  AndroidManifest.xml, signing certificate, res/values-hr-rHR/strings.xml, dex
    string pool
H2  AndroidManifest.xml (permissions), Google Play description
H3  AndroidManifest.xml (MyNotificationListenerService)
H4  AndroidManifest.xml (VoiceService, MqttService)
H5  AndroidManifest.xml (RECORD_AUDIO), dex string pool (Azure Speech, eastus)
M1  res/values/strings.xml (privacy_info_content), Google Play listing
M2  res/values/strings.xml (google_map_common_key)
M3  dex string pool
M4  AndroidManifest.xml (uses-permission)
```

Reproduction: obtain com.smart.haylou 2.0.5.3 (7308), check the SHA-256 values above, decode the manifest and resources with apktool and extract the dex string pools with strings. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF HAYLOUWATCH-2026-R1 at 00:28 UTC to haylouls123@gmail.com, service@haylou.com and asmsservice@outlook.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Three questions, response requested.

2026-09-12 Follow-up at 13:40 UTC, 20 days after the notice, with the open findings restated and the three questions due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:05 UTC, 35 days before publication, with the three questions unchanged in substance.

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 manifest sets allowBackup to false, which blocks backup extraction of local app data. The package holds no advertising ID permission and no major Western ad mediation stack. The app has no billing library and no paid tier. The Data Safety label states that deletion can be requested. A Play listing text that names the call and message push feature and says that it needs the user’s authorisation is a plain statement of purpose.

Residual Risk & Recommendations

Open at the date of publication: all findings except the observations. The operator has not replied and the build analysed is version 2.0.5.3. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, remove the global cleartext allowance (C2). Second, align the Data Safety declaration with the integrations and name each recipient (C1). Third, name the controller, an Article 27 representative and a transfer mechanism for the Alibaba Cloud storage (C3). Fourth, set the microphone and MQTT services to not exported (H4). Fifth, restrict the notification listener, state where call and message content goes and name the region and mechanism for voice processing (H2, H3, H5). Sixth, state one minimum age, restrict the Maps key and strip test artifacts (M1 to M3). Seventh, assess the SmartV3 platform as one processing operation (H1).

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 HAYLOUWATCH-2026-R1.