Security & Privacy Disclosure, Final Report

CO-FIT for Android (com.codingiot.co.fit)

A signing certificate shared with Haylou Watch, a policy that stores all data on Alibaba Cloud, and no reply to three messages.

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

Target	Shenzhen Kou Ding Technology Co., Ltd. (CO-FIT)
Versions Audited	2.1.0.5 / versionCode 8064 (Play update 2026-08-10, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	10: 1 High, 6 Medium, 3 Low (R1 labels reassessed, see status table)
Status	NO REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`764729b34c7f834de1d1aeb384c2fb12ce629270b29220c9d8d420f2dba957cb`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 7

6.1 C1: Cleartext traffic is permitted in all three network security configurations, one of them trusts user installed certificates, and nothing is pinned 7

6.2 H1: The signing certificate, internal package family and SDK module pairing are identical to those of Haylou Watch, a product listed under another company name 8

6.3 H2: The policy states that all data is stored only on Alibaba Cloud and names no Chapter V mechanism, and the package calls Alibaba Cloud endpoints in two PRC regions 9

6.4 H3: Messenger specific send classes and server enable flags sit in the notification listener next to a policy that promises that message content is never uploaded 10

6.5 H4: The notification listener reads the text of every notification, as its own log strings show 11

6.6 M1: Three advertising SDKs construct at process start before any consent screen can run, although a consent platform is integrated 12

6.7 M2: An AdMob application ID and a Baidu Maps API key are stored in the app resources 13

6.8 M3: A remote camera command is compiled in and the findings file did not locate it in the listing or the policy 13

6.9 M4: PEGI 3 rating against a stated minimum age of 16 and no age gate 14

6.10 M5: The Data Safety card says no data is shared with third parties while the policy describes cloud provider and partner sharing 15

7 Impact Analysis 15

8 The Complete Chain 16

9 Engine Fingerprint and Correlation Keys 17

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 18

12 Regulatory & Legal Landscape 19

13 Indicators of Compromise & Reproducible Evidence 20

14 Disclosure Timeline & Outcome 21

15 What Was Done Well 21

16 Residual Risk & Recommendations 21

Executive Summary

CO-FIT is the companion app of a family of Bluetooth watches and fitness bands with more than 1 million downloads on Google Play. The Play developer is listed as Shenzhen Kou Ding Technology Co., Ltd. in the About the developer entry, and the bundled policy names the controller Shenzhen Kouding Technology Co., Ltd. On 23 August 2026 RFI-IRFOS sent a notice with REF COFIT-2026-R1 to winson@codingiot.net and appsupport@codingiot.net with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 2.1.0.5 shows that the package is signed with a certificate whose fingerprint is recorded as identical to that of Haylou Watch, a product listed under a different company, and that it shares an internal package family, a notification listener class name and an SDK module pairing with it (H1). The operator's own policy states that all user data is stored only on Alibaba Cloud and names no Chapter V mechanism, while the package calls Alibaba Cloud endpoints in Shanghai and Guangzhou (H2). Cleartext traffic is permitted in all three network configuration files and one trusts user installed certificates (C1). The notification listener reads the text of notifications (H4), and it sits next to WeChat and WhatsApp send classes with server enable flags that stand against the policy promise that message content is never uploaded (H3).

A reassessment by CVSS v4.0 band puts one finding at High, six at Medium and three at Low. The Critical label of 23 August 2026 moves down because the package shows configuration and not runtime traffic. Six more labels move down for the same reason or because the exposure is a capability. H2 stays High through a stated blast-radius escalation. Whether any value leaves the phone, and where it goes, is UNVERIFIED throughout.

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. 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 2.1.0.5 (versionCode 8064). The package was obtained as an XAPK bundle (246,713,046 bytes, base APK of 229,702,178 bytes plus arm64-v8a and mdpi splits) from the APKPure mirror and cross-checked against the package name, app name, developer name and version on the live Google Play listing. APKPure shows an update date of 18 August 2026 and Google Play shows 10 August 2026 for the same version, a difference that does not affect the chain of custody. Work done: manifest and resource decode with aapt2, the signing certificate with apksigner, and a string pass across all 17 classes*.dex files and the 2 embedded Facebook Audience Network dex files (about 120 MB combined). The live Google Play listing and the operator's English policy were read on 23 August 2026. No bytecode pass, no baksmali, no jadx project decompile and no dynamic analysis was done. The app was not installed, no account was created, no operator server was called and no traffic was captured. Findings that depend on runtime behaviour or call order are marked as such.

ID	Severity	Title
C1	MEDIUM	Cleartext traffic is permitted in all three network security configurations, one of them trusts user installed certificates, and nothing is pinned
H1	MEDIUM	The signing certificate, internal package family and SDK module pairing are identical to those of Haylou Watch, a product listed under another company name
H2	HIGH	The policy states that all data is stored only on Alibaba Cloud and names no Chapter V mechanism, and the package calls Alibaba Cloud endpoints in two PRC regions
H3	MEDIUM	Messenger specific send classes and server enable flags sit in the notification listener next to a policy that promises that message content is never uploaded
H4	MEDIUM	The notification listener reads the text of every notification, as its own log strings show
M1	MEDIUM	Three advertising SDKs construct at process start before any consent screen can run, although a consent platform is integrated
M2	MEDIUM	An AdMob application ID and a Baidu Maps API key are stored in the app resources
M3	LOW	A remote camera command is compiled in and the findings file did not locate it in the listing or the policy
M4	LOW	PEGI 3 rating against a stated minimum age of 16 and no age gate
M5	LOW	The Data Safety card says no data is shared with third parties while the policy describes cloud provider and partner sharing

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Configuration proven, plain HTTP use not observed.
H1	HIGH	MEDIUM	No reply. Certificate and package identity proven for this app, Haylou side not re-checked.
H2	HIGH	HIGH	No reply. Policy text proven, data flow not observed.
H3	HIGH	MEDIUM	No reply. Names and policy text proven, behaviour not observed.
H4	HIGH	MEDIUM	No reply. Capability proven, outflow not observed.
M1	MEDIUM	MEDIUM	No reply. Initialisation order proven, network activity before consent not shown. A consent platform is present.
M2	MEDIUM	MEDIUM	No reply. Key restrictions not visible from the package.
M3	MEDIUM	LOW	No reply. Strings proven, origin of the command not tested.
M4	MEDIUM	LOW	No reply. Age gate not found in the package.
M5	MEDIUM	LOW	No reply. Both texts proven, the definition of sharing is open.

The findings file of 23 August 2026 labels C1 as Critical, H1 to H4 as High and M1 to M5 as Medium. The report uses the CVSS v4.0 band of each finding. H2 stays High through a blast-radius escalation that the finding states.

Subject & Operator Analysis

The Play entry About the developer names Shenzhen Kou Ding Technology Co., Ltd., Huafeng Headquarters Economic Building, No. 288 Xixiang Avenue, Xixiang Street, Bao'an District, Shenzhen, Guangdong, China 518000, with the contact winson@codingiot.net. The findings file also gives the developer name on the listing as Shenzhen Coding IOT Technology Limited. The bundled policy names the controller Shenzhen Kouding Technology Co., Ltd., a second romanisation of the same name, with the privacy contact appsupport@codingiot.net and the company site codingiot.net, which was not fetched. A third support address, smartwatch@yeah.net, appears in the same source. The domain yeah.net is a free consumer webmail service and not a corporate domain. The notice went to the first two addresses.

The policy is hosted at api.iot-solution.net and is rendered in the browser from an i18n bundle keyed by the app parameter, so a plain download returns an empty shell. The backend names in the package carry the sma and smawatch brand and not the names of the listed companies. No Data Protection Officer and no Article 27 representative were found in the package or the policy. No main establishment in the Union was identified, so no one-stop-shop exists and the Austrian Datenschutzbehörde is the competent authority for a matter that began in Austria.

Architecture & Data Flow

CO-FIT is a native Android app in Kotlin with 17 classes*.dex files and 2 embedded Facebook Audience Network dex files. The native stack holds libraries of at least seven hardware and SDK vendors, among them Realtek (libRtkAesJni.so), Zhuhai Jieli (the libjl_ prefix set), iFlytek (libSparkChain.so), Baidu Maps (libBaiduMapSDK_base_v7_5_3.so and libBaiduMapSDK_map_v7_5_3.so), the Pangle protection libraries and the Alibaba Cloud log producer (libsls_producer.so).

The app talks to the watch over Bluetooth Low Energy through the Bluetrum abota and fota modules and relays notifications, calls and messages (H3, H4). The dex strings name the backend api.smawatch.cn and its test host ceshi.smawatch.cn, two Alibaba Cloud OSS buckets, an IoT authentication endpoint in Shanghai and a log endpoint in Guangzhou (H2). Voice components (iFlytek, Baidu) and the Baidu location service sit next to the audio and location permissions. The advertising stack and the WeChat and Weibo integrations complete the picture. No data flow was observed.

Engagement Summary

The notice REF COFIT-2026-R1 was sent on 23 August 2026 at 07:17 UTC from rfi.irfos@gmail.com to winson@codingiot.net and appsupport@codingiot.net with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated six points, put three questions in writing and gave the embargo date. The thread notes record no delivery failure notice for either address. A follow-up of 12 September 2026 at 17:01 UTC went to the same two addresses and restated the findings and the three questions with an answer date of 19 September 2026. A second follow-up of 17 October 2026 at 19:01 UTC came from security@rfi-irfos.com under the subject 35 days to publication: CO-FIT. No inbound message from the operator exists in the mailbox.

Findings

C1: Cleartext traffic is permitted in all three network security configurations, one of them trusts user installed certificates, and nothing is pinned

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

The package carries three network security configuration files. Each one sets cleartextTrafficPermitted to true at base-config level, and the application element of the manifest also sets android:usesCleartextTraffic to true. One file, network_config.xml, adds user installed certificates as a trust anchor next to the system store for all traffic that it covers. None of the three files holds a pin-set and a search of the resource tree found no pinning configuration. The Play Data Safety card says that data is encrypted in transit. The configuration permits plain HTTP, but which endpoints the app actually calls over plain HTTP and what data they carry was not observed and is UNVERIFIED, so the impact metrics of the vector are set to limited and not high.

```
res/xml/network_config.xml:
  base-config: cleartextTrafficPermitted=true
    trust-anchors: certificates src="system", certificates src="user"

res/xml/network_security_config.xml:
  base-config: cleartextTrafficPermitted=true

res/xml/sm_network_security_config.xml:
  base-config: cleartextTrafficPermitted=true
    trust-anchors: certificates src="system"
```

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

Impact: Anyone on the network path, or anyone who can install a certificate on the device, could read or alter traffic of the app, if such traffic occurs.

Fix: Remove the cleartext allowance and the user trust anchor and pin first party hosts.

H1: The signing certificate, internal package family and SDK module pairing are identical to those of Haylou Watch, a product listed under another company name

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 package is signed with a self-signed certificate whose SHA-256 fingerprint and distinguished name are given below. The findings file records the same fingerprint and name for Haylou Watch (com.smart.haylou), which is listed under a different company, and that report is not part of this package. The internal Java package family is com.sma.smartv3, the notification listener is the class com.sma.smartv3.ble.MyNotificationListenerService, and the package embeds the Bluetrum abota and fota SDK modules. A Croatian locale resource resolves the app label to SmartV3-Android, and the backend hosts are named api.smawatch.cn and ceshi.smawatch.cn, the latter meaning test in Chinese. Nothing in the Play listing or in the policy discloses the relationship to a consumer who sees two unrelated companies. The legal relationship between the two publishers is not demonstrated and cannot be resolved by static analysis. Two explanations fit equally. The two companies may be one group, or both may license a build and signing pipeline from a common platform vendor.

```
SHA-256: 22f1cfbef897405e5de13d0e86d42e939b8de7c0789025eb9d2d26b8cda54083
DN: CN=sma, OU=smalife, O=sma, L=shenzhen, ST=guandong, C=86
```

```
com.sma.smartv3.App                                    (Application class)
com.sma.smartv3.co_fit.wxapi.WXEntryActivity           (WeChat callback, exported)
com.sma.smartv3.ble.MyNotificationListenerService
com.sma.smartv3.ble.DfuService
com.bluetrum.abota.bluetooth.BleManager   BluetoothSppService   SppManager
    BluetoothManager
com.bluetrum.fota.manager.OtaDataProvider   OtaManager   ABOtaManager
```

```
https://api.smawatch.cn
https://ceshi.smawatch.cn
https://sma-product.oss-accelerate.aliyuncs.com
https://sma-test.oss-accelerate.aliyuncs.com
lib/arm64-v8a/libsmawatchface.so
res/values-hr-rHR: application label "SmartV3-Android"
```

Impact: A buyer who compares two listings sees two companies. The same signing key stands behind both, so one party controls the build of both.

Fix: State in the listing and the policy which entity builds, signs and operates the app.

H2: The policy states that all data is stored only on Alibaba Cloud and names no Chapter V mechanism, and the package calls Alibaba Cloud endpoints in two PRC regions

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

Section 12.9 of the operator's bundled policy states that the product service side uses servers of Alibaba Cloud and that user information is stored only on those servers. Section 12.6 claims regional storage without saying which regions exist or how the region is enforced. The policy names no standard contractual clause, adequacy decision or other Article 46 mechanism and no representative in the Union. The dex string pool holds an IoT device authentication endpoint in the Shanghai region and a log service endpoint in the Guangzhou region. Two speech recognition components sit in the package next to the RECORD_AUDIO permission, an iFlytek SparkChain recognition SDK and a Baidu voice input recorder. The package also embeds Baidu Maps and location components. Whether either speech component is invoked in this product, and what audio would be sent where, was not observed and is UNVERIFIED. So is the region that receives the data of a user in the Union. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the policy itself states that all user data sits only with one cloud provider outside the Union, the app declares SMS, call log, contacts, location and health permissions, and it has more than 1 million installs.

```
Policy Section 12.9: "CO-FIT'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 CO-FIT's App products
    are only stored on Ali Cloud servers, and CO-FIT does not store relevant materials
     locally."
```

```
https://iot-auth.cn-shanghai.aliyuncs.com
https://cn-guangzhou.log.aliyuncs.com
lib/arm64-v8a/libsls_producer.so
```

```
Lcom/iflytek/sparkchain/core/asr/AudioRecorder
Lcom/iflytek/sparkchain/media/MediaRecorderHelper
Lcom/baidu/vi/AudioRecorder
com.sma.smartv3.util.audio_recorder.AudioRecordManager
lib/arm64-v8a/libSparkChain.so   libspark.so
res/xml/filepaths.xml: smart_watch_recording/   aigc/
com.baidu.lbsapi.API_KEY   com.baidu.location.f (process :remote)
```

Impact: The operator documents that every user record lives with one provider and gives a person in the Union no legal basis for the transfer.

Fix: Name the Chapter V mechanism, the storage region offered to Union users and a Union representative.

H3: Messenger specific send classes and server enable flags sit in the notification listener next to a policy that promises that message content is never uploaded

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

Section 14 of the operator's policy says that call and SMS content is pushed to the smart watch only and that the operator will not upload or process any phone and text message content. The dex string pool names two manager classes with a send text message method, one for WeChat and one for WhatsApp, and two boolean flags with the words NotificationServerEnable in their names. They appear in the same listener class that reads notifications. A purely local relay to a paired band has no use for a server flag, so the platform seems to provide a server path for this content. The destination, the default state of the flags and whether message content or only metadata ever leaves the phone were not observed and are UNVERIFIED. The finding is the tension between the written promise and the names in the code.

```
Policy Section 14: "These permissions are limited to the implementation of information
     push function, the phone received by the call and SMS messages and content,
    pushed to the smart watch side, so as to remind users with new messages for users
    to view. CO-FIT solemnly affirms that we will not upload or process any phone and
    text message content, and will never abuse these permissions, apply for these
    permissions only to implement the message push function."
```

```
com.sma.smartv3.biz.wx.WxManager$sendTextMessage$1        (Wx = WeChat)
com.sma.smartv3.biz.wa.WAManager$sendTextMessage$1         (WA = WhatsApp)
MyNotificationListenerService  WxNotificationServerEnable
MyNotificationListenerService  WANotificationServerEnable
MyNotificationListenerService  onNotificationPosted -> new content
MyNotificationListenerService  handleIncomingCall -> Send Notification =
```

Impact: If the flags are active, message content of the user and of the people who write to the user leaves the phone, against the written promise.

Fix: Explain what the server flags do and align the code or the policy.

H4: The notification listener reads the text of every notification, as its own log strings show

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 as exported. The system permission BIND_NOTIFICATION_LISTENER_SERVICE protects it, so only the operating system can bind it. A bound listener can read sender, source app and text of every notification on the device, beyond calls, SMS, WeChat and WhatsApp. Log strings in the dex show that the service parses notification text and not only package and sender, for example onNotificationPosted with new content, repeat textline and notification extras. From that data a person could derive who writes to the user, how often, through which app and when. Whether the content leaves the phone is covered by H3 and is UNVERIFIED.

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

```
MyNotificationListenerService  onNotificationPosted -> new content
MyNotificationListenerService  onNotificationPosted -> repeat textline
MyNotificationListenerService  onNotificationPosted -> in interval time
MyNotificationListenerService  onNotificationPosted -> notification.extras ->
```

Impact: Everything that appears in the notification shade of the user, including messages of third parties, passes through the app.

Fix: Limit the listener to the apps that the watch feature needs and document what happens with the text.

M1: Three advertising SDKs construct at process start before any consent screen can run, although a consent platform is integrated

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 package carries a six network advertising stack made of Google AdMob, AppLovin, IronSource, Vungle, Meta Audience Network and ByteDance Pangle. Three of them register content providers with an explicit initOrder, which Android runs at process start before any activity. The package also holds a real consent integration, GoogleMobileAdsConsentManager with the IABTCF key set (IABTCF_GDPR_APPLIES, IABTCF_TCString and IABTCF_AddtlConsent). Whether personalised requests wait for the consent result is a call order question that was not examined and is UNVERIFIED. The app declares the BILLING permission and its listing shows in-app purchases, so paying users meet the same stack.

```
MobileAdsInitProvider (Google)     initOrder=100
AppLovinInitProvider               initOrder=101
VungleProvider                     initOrder=102

com.sma.smartv3.biz.ad.GoogleMobileAdsConsentManager
IABTCF_GDPR_APPLIES   IABTCF_TCString   IABTCF_AddtlConsent
```

```
com.bytedance.sdk.openadsdk.activity.TTAdActivity
lib/arm64-v8a/libpglarmor.so   libbuffer_pgl.so   libfile_lock_pgl.so
    libtt_ugen_layout.so
api16-access-sg.pangle.io
api16-access-ttp.tiktokpangle.us
www.pangleglobal.com
```

Impact: The advertising SDKs exist in the process before the user answers any dialog. Whether they send anything before the answer is not shown.

Fix: Delay SDK initialisation until the consent result is available.

M2: An AdMob application ID and a Baidu Maps API key are stored in the app resources

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

Both values resolve from res/values/strings.xml with aapt2. The AdMob application ID is a public identifier by design. The Baidu key is a client side key and a quota or billing abuse surface if it is not restricted. Whether the key is restricted by package or signature was not tested because that needs a live call.

```
string/adp_admob_id
    ca-app-pub-2338591241473415~7969088651
string/bai_du_key
    iQZn3sgEgM4fAtuPcjmGXi8nnGqYMalu
```

Impact: A key in a public package can be reused by others at the operator's cost.

Fix: Restrict the Baidu key by package name and signature.

M3: A remote camera command is compiled in and the findings file did not locate it in the listing or the policy

LOW, CVSS v4.0 AV:L/AC:L/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 holds the command names below, which fit the CAMERA permission of the manifest. The findings file reports that the feature is named neither in the Play description nor in the policy. That absence was not re-read for this report. Whether the command can only come from the paired watch or can also be armed by a backend path is UNVERIFIED. If it can capture bystanders, the open question is whether Article 9 is engaged. This report does not assert that.

```
COMMAND_TAKE_PHOTO
TAKE_PHOTO
```

Impact: A camera triggered from the wrist is likely to capture whoever stands in front of the phone.

Fix: Document the feature and state who can trigger it.

M4: PEGI 3 rating against a stated minimum age of 16 and 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 Play listing carries PEGI 3 (Everyone on the mirrored listing). Section 13 of the policy says that the services are for people of at least 16 years. A birthday field exists in the registration flow and fits the profile fields of Section 8.1.2. It is a self-entered value and no blocking mechanism was located. The only COPPA related logic found belongs to the Vungle SDK request schema and flags a session as child directed to that ad server. It is not an account level parental consent gate. A server side age check cannot be seen.

```
Policy Section 13: "CO-FIT services are available for people at least 16 years of age
    or above. If you are the guardian of a child under the age of 16, you acknowledge
    and warrant your consent and consent to the use of the Platform and to this
    Privacy Policy."
```

```
consent_coppa   COPPA_DISABLE_AD_ID   COPPA_ENABLED   COPPA_DISABLED   COPPA_NOTSET
```

Impact: A child can install an app rated for everyone that the operator itself limits to people from 16.

Fix: Align the rating with the stated minimum and add an age gate.

M5: The Data Safety card says no data is shared with third parties while the policy describes cloud provider and partner sharing

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

The live Data Safety card says No data shared with third parties and lists collected categories of messages, photos, personal info, fitness info and contacts, and says that data is encrypted in transit and can be deleted on request. The policy says in Section 6.2 that data is shared with service providers such as cloud providers and in Section 9.1.4 with authorised partners. Whether a transfer to a cloud provider that acts for the operator counts as sharing on the Play form is a question of definition, so the contradiction may be narrower than it first looks. The policy also holds two drafting artefacts. Section 6.2 reads Alibaba AWS and Section 8.2.5 has a stray Ali prefix, both of which suggest templated text.

```
Data Safety card: "No data shared with third parties"
Policy Section 6.2: "We only share data with third parties in the following
    circumstances: - Service providers: Our cloud service providers and data analysis
    companies (such as Alibaba AWS) will store our data."
Policy Section 9.1.4: "Share with authorized partners... our authorized partners
    include the following types: authorized distributors, service providers, and other
     partners."
```

Impact: The card is the first disclosure a buyer reads and the policy describes more.

Fix: Align the Data Safety declaration with the policy and correct the templated text.

Impact Analysis

The people affected are the more than 1 million installers, who wear a watch and grant Bluetooth, location, phone, SMS, contacts, camera and microphone access, and who may be children, since the Play rating is PEGI 3. People who write to the user or call the user are affected as well and never installed the app.

The weight of the case sits on four points. The operator states that all user data lives only on Alibaba Cloud and names no transfer mechanism (H2). The same signing key stands behind two listings that present as unrelated companies (H1). The notification listener reads message text and sits next to messenger send classes with server flags, against a written promise (H3, H4). The configuration permits plain HTTP and trusts user installed certificates (C1).

What the package shows is configuration, file content and the operator’s own text. No message, contact or identifier was observed leaving a device and the report asserts no such flow.

The Complete Chain

Step 1, listing: the user sees a company name and a Data Safety card that says no data is shared with third parties (M5).

Step 2, first start: three advertising SDKs construct at process creation and the consent dialog follows (M1).

Step 3, pairing and use: the user grants SMS, call, contacts, location, camera and microphone access. The listener reads notification text and the package holds messenger send classes with server enable flags (H3, H4). The watch can trigger the phone camera (M3).

Step 4, backend: the app calls hosts under the sma brand and Alibaba Cloud endpoints in Shanghai and Guangzhou, and the policy says all data is stored only there (H1, H2). The configuration permits plain HTTP (C1).

Step 5, rights: the policy names no Chapter V mechanism and no Union representative (H2).

Engine Fingerprint and Correlation Keys

CO-FIT belongs to the SmartV3 platform family. The findings file records that the same fingerprint, package family and module pairing appear in Haylou Watch (com.smart.haylou), so the correlating key is a code signing identity and not a shared third party SDK. The Haylou Watch report is not part of this package and the values in the right column come from the findings file. They were not re-checked.

Key	CO-FIT	Haylou Watch (per R1)
Signing certificate SHA-256	see code block below	identical
Signing DN	CN=sma, OU=smalife, O=sma, L=shenzhen, ST=guandong, C=86	identical
Internal package family	com.sma.smartv3.*	com.sma.smartv3.*
Listener class	com.sma.smartv3.ble. MyNotificationListenerService	identical class name
Bluetrum SDK modules	abota and fota	abota and fota
Croatian locale label	SmartV3-Android	same string content
Listed company	Shenzhen Kou Ding Technology Co., Ltd.	Dongguan Liesheng Electronic Technology Co., Ltd.

```
Signing cert SHA-256
    22f1cfbef897405e5de13d0e86d42e939b8de7c0789025eb9d2d26b8cda54083
XAPK SHA-256
    b8bd8d6a1d091d8436694d8429b7649f6677c17cc28768b0da500710695278c4
Base APK SHA-256
    764729b34c7f834de1d1aeb384c2fb12ce629270b29220c9d8d420f2dba957cb
Backend                 api.smawatch.cn   ceshi.smawatch.cn
OSS buckets             sma-product.oss-accelerate.aliyuncs.com
                        sma-test.oss-accelerate.aliyuncs.com
```

Two further observations are recorded without a claim. The Arabic locale resolves the app label to Pangle Demo, which points to a build from the demo project of the Pangle SDK, and live Pangle endpoints in the package fit that. The set of Zhuhai Jieli library names (libjl_auth.so, libjl_ota_auth.so, libjl_enc.so, libjl_crc.so, libjl_bmp_convert.so, libjl_fatfs.so, libjl_pack_format.so) matches the set that the findings file records for OnWear Pro. That is a filename match only and no hash was compared. Numeric BLE manufacturer identifiers and GATT UUID values were not extracted at this depth, so the correlation holds at namespace and certificate level.

Data Protection: Article by Article

Article 4(1): engaged by H2.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1, H2, H3 and M5.

Article 5(1)(c), data minimisation: engaged by H3 and H4.

Article 6(1): engaged by H3 and H4.

Article 7(1): engaged by M1.

Article 8: engaged by M4.

Article 9: an open question for M3 and not asserted.

Articles 12 and 13: engaged by M5. Article 13(1)(a) is engaged by H1 and Article 13(1) by M3.

Article 25: engaged by C1, H4, M1, M2, M3 and M4.

Article 27: engaged by H2. No representative is named.

Article 32: engaged by C1 and M2.

Articles 44 and 46: engaged by H2. The policy names no Chapter V 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, lists collected categories, says that data is encrypted in transit and says that deletion can be requested. The statement about sharing does not match the policy in Sections 6.2 and 9.1.4 (M5), and the statement about encryption in transit meets a configuration that permits plain HTTP (C1).

Regulatory & Legal Landscape

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

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

The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.codingiot.co.fit
Version            2.1.0.5 (versionCode 8064), minSdk 26, targetSdk 35, compileSdk 36
XAPK SHA-256 (246,713,046 bytes)
    b8bd8d6a1d091d8436694d8429b7649f6677c17cc28768b0da500710695278c4
Base APK SHA-256 (229,702,178 bytes)
    764729b34c7f834de1d1aeb384c2fb12ce629270b29220c9d8d420f2dba957cb
config.arm64_v8a.apk SHA-256 (16,605,291 bytes)
    b050d6e3f2d57e72b32c4f2bcbd5ad5cc18865fcd6580e14019394074ba1b042
Signing cert SHA-256
    22f1cfbef897405e5de13d0e86d42e939b8de7c0789025eb9d2d26b8cda54083
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
AdMob application ID
    ca-app-pub-2338591241473415~7969088651
Baidu Maps API key
    iQZn3sgEgM4fAtuPcjmGXi8nnGqYMalu
Backend hosts
    https://api.smawatch.cn
    https://ceshi.smawatch.cn
Alibaba Cloud endpoints
    https://iot-auth.cn-shanghai.aliyuncs.com
    https://cn-guangzhou.log.aliyuncs.com
Pangle endpoints
    api16-access-sg.pangle.io
    api16-access-ttp.tiktokpangle.us
    www.pangleglobal.com
Policy
    https://api.iot-solution.net/web/help/webs/privacy.html?app=CO-FIT
Contacts
    winson@codingiot.net   appsupport@codingiot.net   smartwatch@yeah.net
```

```
C1  res/xml/network_config.xml, network_security_config.xml,
    sm_network_security_config.xml, AndroidManifest.xml
H1  apksigner certificate output, AndroidManifest.xml, classes*.dex (class names,
    hosts), res/values-hr-rHR
H2  operator policy Sections 12.6 and 12.9, classes*.dex (endpoints, SDK classes),
    library inventory
H3  operator policy Section 14, classes*.dex (WxManager, WAManager, flags)
H4  AndroidManifest.xml, classes*.dex (log strings)
M1  AndroidManifest.xml (providers, initOrder), classes*.dex
M2  res/values/strings.xml (adp_admob_id, bai_du_key)
M3  classes*.dex (COMMAND_TAKE_PHOTO, TAKE_PHOTO)
M4  Google Play listing, operator policy Section 13, classes*.dex (Vungle strings)
M5  Google Play Data Safety card, operator policy Sections 6.2, 8.2.5 and 9.1.4
```

Reproduction: obtain com.codingiot.co.fit 2.1.0.5 (8064), check the SHA-256 values above, dump the manifest and resources with aapt2, read the certificate with apksigner, extract strings from the dex files and read the policy in a browser. No device, account or network access is needed. Reading call order needs a bytecode pass, which was not done.

Disclosure Timeline & Outcome

2026-08-23 Notice REF COFIT-2026-R1 at 07:17 UTC to winson@codingiot.net and app-support@codingiot.net, CC dsb@dsb.gv.at and edps@edps.europa.eu. Embargo date 21 November 2026.

2026-09-12 Follow-up at 17:01 UTC to the same two addresses with the three questions and an answer date of 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:01 UTC, under the subject 35 days to publication: CO-FIT.

2026-11-14 No reply of any kind. 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 application element sets allowBackup to false. A real consent integration is present (GoogleMobileAdsConsentManager with the IABTCF key set). Section 14 of the policy gives a specific promise that can be tested, which is a stronger statement than generic privacy wording. Section 11.3.5 describes a login-free mode in which all data stays on the phone, and Section 10.1.1 states that the user owns the motion data. The Data Safety card states that data deletion can be requested.

Residual Risk & Recommendations

Open at the date of publication: all ten entries. The operator has not replied and the build analysed is version 2.1.0.5 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, state which entity builds, signs and operates the app (H1). Second, name the Chapter V mechanism, the storage region for Union users and a Union representative (H2). Third, explain the server enable flags and align the code or the policy (H3). Fourth, remove the cleartext allowance and the user trust anchor and pin first party hosts (C1). Fifth, hold the advertising SDKs back until the consent result is available (M1). Sixth, limit the listener, restrict the keys and align the rating and the Data Safety declaration (H4, M2, M4, M5), and document the camera command (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 COFIT-2026-R1.