Security & Privacy Disclosure, Final Report

WearPro for Android (com.dtno1.WearPro)

A Data Safety card that says no data is collected, a policy that names eight processors, and no reply since the notice reached a second address.

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

Target	Shenzhen Wanruxia Technology Co., Ltd. (WearPro)
Versions Audited	3.8.4.0 / versionCode 244 (Play update 2026-07-29, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 1 High, 6 Medium, 3 Low, 1 Info (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`b47049ba438693786046ac0d722bb7948fade0a0953e2919fb8e419e0d6be603`

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 6

6 Findings 7
- 6.1 C1: The Data Safety card says no data is collected while the permissions and the operator's own policy describe SMS, call, contact, device identifier and location collection and eight named processors . . . 7
- 6.2 C2: Google Mobile Ads and ML Kit construct at process start, before the app's own privacy agreement dialog can appear . . . 8
- 6.3 H1: Two exported services without a permission and a remote camera command chain that the operator's policy discloses . . . 9
- 6.4 H2: A private network address and a raw public IP address are compiled into the release package as plain HTTP endpoints . . . 10
- 6.5 H3: The policy names eight third party SDKs, several of them Chinese, and a transfer clause without a mechanism, and no representative in the Union is named . . . 10
- 6.6 H4: Contacts, SMS and call data of people who never installed the app are synchronised through the app to the watch . . . 11
- 6.7 M1: Cleartext traffic is permitted for the whole app and nothing is pinned . . . 12
- 6.8 M2: A Google API key is hardcoded in the dex files . . . 12
- 6.9 M3: PEGI 3 rating against payment rails, advertising permissions and a minors notice that nothing enforces . . . 13
- 6.10 M4: The Pangle open ad SDK permission is declared and no Pangle class was found in the dex files . . . 13
- 6.11 M5: An exported provider of the bundled 3-D Secure SDK has no permission . 14

7 Impact Analysis 14

8 The Complete Chain 15

9 Engine Fingerprint and Correlation Keys 16

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 18

14 Disclosure Timeline & Outcome 19

15 What Was Done Well 19

16 Residual Risk & Recommendations 20

Executive Summary

WearPro is a companion app for a family of white label Bluetooth watches of the DT series with more than 5 million downloads on Google Play. The publisher is Shenzhen Wanruxia Technology Co., Ltd. ([redacted]). The listing shows PEGI 3 and a Data Safety card. On 23 August 2026 RFI-IRFOS sent a notice with REF WEARPRO-2026-R1 to developer@dtone.cc and support@dtone.cc with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy. The message to support@dtone.cc bounced and the notice was redelivered to info@dtno1.com and developer@dtone.cc the same day.

A root level code analysis of version 3.8.4.0 shows that the Data Safety card says no data is collected, while the manifest declares 63 permissions including SMS, call log, contacts, microphone, camera and background location, and the operator's own policy names eight third party SDKs and the collection of device identifiers (C1). Google Mobile Ads and ML Kit construct at process start before the app's own agreement dialog, although a Google consent platform is integrated (C2). Two exported services and a remote camera command chain exist (H1). Two plain HTTP endpoints, one of them a private network address, ship in the release build (H2), and cleartext is permitted for every host (M1). The policy names eight processors and no transfer mechanism (H3) and the app relays contacts and messages of third parties to the watch (H4).

A reassessment by CVSS v4.0 band puts one finding at High, six at Medium and three at Low, with one entry at informational level. The two Critical labels of 23 August 2026 move down because the package shows configuration and file content and not runtime behaviour. Seven more labels move down for the same reason or because the exposure is a capability. C1 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 3.8.4.0 (versionCode 244). The package was obtained as an XAPK bundle (122,756,532 bytes, base APK plus arm64-v8a, English and hdpi splits) from the APKPure mirror, whose published hash matches, and checked against the version and developer name on the live Google Play listing. The Play update date is 29 July 2026. Work done: a resources only decode with apktool (no source decode), the manifest, strings and network configuration, a string pass across all six classes*.dex files (44 MB combined), and an inventory of native library names from the arm64 split. 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 was done and no dynamic analysis. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	HIGH	The Data Safety card says no data is collected while the permissions and the operator's own policy describe SMS, call, contact, device identifier and location collection and eight named processors
C2	MEDIUM	Google Mobile Ads and ML Kit construct at process start, before the app's own privacy agreement dialog can appear
H1	LOW	Two exported services without a permission and a remote camera command chain that the operator's policy discloses
H2	MEDIUM	A private network address and a raw public IP address are compiled into the release package as plain HTTP endpoints
H3	MEDIUM	The policy names eight third party SDKs, several of them Chinese, and a transfer clause without a mechanism, and no representative in the Union is named
H4	MEDIUM	Contacts, SMS and call data of people who never installed the app are synchronised through the app to the watch
M1	MEDIUM	Cleartext traffic is permitted for the whole app and nothing is pinned
M2	MEDIUM	A Google API key is hardcoded in the dex files
M3	LOW	PEGI 3 rating against payment rails, advertising permissions and a minors notice that nothing enforces
M4	INFO	The Pangle open ad SDK permission is declared and no Pangle class was found in the dex files
M5	LOW	An exported provider of the bundled 3-D Secure SDK has no permission

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Contradiction shown by public documents.
C2	CRITICAL	MEDIUM	No reply. Network activity before consent not shown. A consent platform is present.
H1	HIGH	LOW	No reply. Exported state proven, behaviour not tested.
H2	HIGH	MEDIUM	No reply. Strings proven, calls not observed.
H3	HIGH	MEDIUM	No reply. Policy text proven, PRC server sentence not re-read.
H4	HIGH	MEDIUM	No reply. Disclosed core feature, backend path not shown.
M1	MEDIUM	MEDIUM	No reply. Configuration proven, plain HTTP use not observed.
M2	MEDIUM	MEDIUM	No reply. Key restrictions not visible from the package.
M3	MEDIUM	LOW	No reply. Age gate not found in resources.
M4	MEDIUM	INFO	No reply. Unresolved observation, no score.
M5	MEDIUM	LOW	No reply. Routine SDK component, exposure not shown.

The findings file of 23 August 2026 labels C1 and C2 as Critical, H1 to H4 as High and M1 to M5 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. M4 is an unresolved observation without a score.

Subject & Operator Analysis

The Play developer of record is Shenzhen Wanruxia Technology Co., Ltd. (深圳市万睿智能科技有限公司), People's Republic of China. The developer contact on Google Play is developer@dtone.cc and the policy names support@dtone.cc for customer service. The policy and the public site are hosted at dt1pro.cn (policy of 2023-11-16). The production backend host in the dex strings is dt1pro.wanruxia.com, which ties the wanruxia.com domain to the developer name. The notice was redelivered to info@dtno1.com, which the findings file does not list. The package name is com.dtno1.WearPro. The Play page also lists a sibling app, WearJoy, under the same developer. It was not audited.

The signing certificate is self-signed with the DN CN=zh and no other field. No Data Protection Officer and no Article 27 representative were found. The Austrian Datenschutzbehörde receives the notice in copy and can receive complaints directly.

Architecture & Data Flow

WearPro is a native Android app with six classes*.dex files (44 MB combined) and an arm64-v8a native split. The hardware layer is com.wear.lib_core (371 classes) wrapping com.crrepa.ble.* (781 classes), with Realtek and Sifli chipset update support, and the multi device library behind WearEngineService (libglyphix-mas-android.so, libmasExtraFeature.so).

The app talks to the watch over Bluetooth Low Energy and relays contacts, SMS, calls and notifications (H4). The dex strings name the production API host dt1pro.wanruxia.com, two plain HTTP endpoints (H2), the host api.moyoung.com and an Alibaba Cloud IoT Hub MQTT broker (H3). The policy names the eight SDKs of H3. No data flow was observed.

Engagement Summary

The notice REF WEARPRO-2026-R1 was first sent on 23 August 2026 at 00:08 UTC from rfi.irfos@gmail.com to developer@dtone.cc and support@dtone.cc with dsb@dsb.gv.at and edps@edps.europa.eu in copy. At 00:08 UTC the mail system of dtone.cc returned a permanent failure notice for support@dtone.cc, whose mailbox does not exist. No failure notice is recorded for developer@dtone.cc. The same notice was redelivered unchanged at 07:17 UTC to info@dtno1.com and developer@dtone.cc with dsb@dsb.gv.at and edps@edps.europa.eu in copy. A follow-up of 12 September 2026 at 12:58 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 19:09 UTC came from security@rfi-irfos.com under the subject 35 days to publication: WearPro. No inbound message from the operator exists in the mailbox.

Findings

C1: The Data Safety card says no data is collected while the permissions and the operator's own policy describe SMS, call, contact, device identifier and location collection and eight named processors

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 collected, the developer says this app doesn't collect user data. The same card also says that the app may share App info and performance and Device or other IDs with third parties, so the card is inconsistent with itself. The manifest of the XAPK declares 63 permissions, among them READ_SMS, RECEIVE_SMS, READ_CALL_LOG, READ_CONTACTS, ANSWER_PHONE_CALLS, RECORD_AUDIO, CAMERA, ACCESS_FINE_LOCATION, ACCESS_BACKGROUND_LOCATION, USE_BIOMETRIC, eight Health Connect write permissions and the advertising ID permissions. The operator's policy at dt1pro.cn, linked from the same listing, says that on the first run it collects IMEI, SIM serial number, Android ID, MAC address and OAID, that SMS and notification data is synchronised to smart watches, and that call records are used for call reminders. Section 5 of the policy names eight third party SDKs (Pangle Partner Data SDK, BeiZi, Umeng, AMap, QQ Interconnection, Alipay Client, WeChat and Bugly), each with its own list of collected device identifiers. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the card is the first and often only disclosure for an app with more than 5 million installs, it contradicts the operator's own policy point for point, and the app handles SMS, call, contact, location and health permissions.

```
Data Safety card: "No data collected. The developer says this app doesn't collect user
     data."
Same card: "This app may share these data types with third parties: App info and
    performance and Device or other IDs"
```

```
android.permission.READ_SMS   RECEIVE_SMS   READ_CALL_LOG   READ_CONTACTS
    ANSWER_PHONE_CALLS
android.permission.RECORD_AUDIO   CAMERA   ACCESS_FINE_LOCATION
    ACCESS_BACKGROUND_LOCATION
android.permission.USE_BIOMETRIC   USE_FINGERPRINT
android.permission.health.WRITE_HEART_RATE   WRITE_STEPS   WRITE_EXERCISE
com.google.android.gms.permission.AD_ID   android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION   android.permission.
    ACCESS_ADSERVICES_TOPICS
```

```
Policy 1.1: "In the first run... we will collect the following equipment information:
    IMEI, SIM serial number, AndroidID, MAC address, OAID information"
Policy 1.5: "SMS notification, application notice: for SMS and other information
    synchronization to smart watches"
Policy 1.5: "Call Record: For functions such as call reminder, unknown call reminder,
    etc."
```

Impact: More than 5 million installers are told before the install that nothing is collected. The same operator tells them in its policy that identifiers, messages and call records are processed and that eight companies receive device identifiers.

Fix: Correct the Data Safety declaration to match the manifest and the policy.

C2: Google Mobile Ads and ML Kit construct at process start, before the app's own privacy agreement dialog can appear

---

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 both at process start, before any activity and so before the SplashActivity that hosts the first run dialog (string privacy_policy_agree_desc, res/values/strings.xml line 2814). The package also integrates the Google User Messaging Platform (com.google.android.ump.ConsentInformation, UserMessagingPlatform and the IABTCF_ key set), so a consent platform for the advertising stack exists. Whether the Mobile Ads SDK holds back its requests until the consent result is available was not observed and is UNVERIFIED. No network call before consent was observed.

```
<provider android:authorities="com.dtno1.WearPro.mlkitinitprovider" android:exported="
    false"
          android:initOrder="99" android:name="com.google.mlkit.common.internal.
    MlKitInitProvider"/>
<provider android:authorities="com.dtno1.WearPro.mobileadsinitprovider" android:
    exported="false"
          android:initOrder="100" android:name="com.google.android.gms.ads.
    MobileAdsInitProvider"/>

<string name="privacy_policy_agree_desc">By clicking Agree, you agree to the above
    content and view</string>
```

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

Fix: Delay SDK initialisation until the consent result is available and show that the advertising SDK waits for it.

H1: Two exported services without a permission and a remote camera command chain that the operator’s policy discloses

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

AndroidManifest.xml declares com.wear.lib_core.mvp.view.service.LocationService (foreground service of type location) and com.glyphix.mas.service.WearEngineService (action com.xfaith.glyphix.WEAR_ENGINE_ACTION) as exported without an android:permission attribute, so any other app on the device can start them with an explicit intent. The native backing is libglyphix-mas-android.so and libmasExtraFeature.so. The dex strings of all six classes*.dex files hold the camera command names icon_device_take_photo, onTakePhoto, remotecapture, take_photo and take_photo_success. The operator’s policy section 1.5 says: Mobile phone status (only part of the model): for remote photography. The camera trigger from the paired watch is therefore a disclosed feature. The services were not invoked, and what WearEngineService accepts once invoked is UNVERIFIED.

```
<service android:enabled="true" android:exported="true" android:foregroundServiceType
    ="location"
         android:name="com.wear.lib_core.mvp.view.service.LocationService"/>
<service android:enabled="true" android:exported="true" android:name="com.glyphix.mas.
    service.WearEngineService">
    <intent-filter>
        <action android:name="com.xfaith.glyphix.WEAR_ENGINE_ACTION"/>
    </intent-filter>
</service>

icon_device_take_photo   onTakePhoto   remotecapture   take_photo   take_photo_success
```

Impact: Another app on the same phone can start the services, and the effect depends on what the services accept.

Fix: Protect both services with a signature permission or set them to not exported, and document the commands that the watch can send.

H2: A private network address and a raw public IP address are compiled into the release package as plain HTTP endpoints

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

The dex strings of the release build hold the two literal endpoints below next to the production path of the same API at dt1pro.wanruxia.com/xky-api/. The first is an address of a private network, which is almost certainly a developer test server. The second is a raw public address in an Alibaba Cloud range. Both use plain HTTP. Whether the live build calls either of them was not observed and is UNVERIFIED. The host dt1pro.wanruxia.com also ties the wanruxia.com domain to the developer name Shenzhen Wanruxia Technology.

```
http://192.168.110.182/xky-api/
http://39.108.214.143/wearpro/
https://dt1pro.wanruxia.com/xky-api/   (production host named in the same strings)
```

Impact: If the app calls the public address, its traffic is readable on the network path. In any case the addresses help a person who studies the build.

Fix: Remove test addresses from release builds and call only HTTPS hosts.

H3: The policy names eight third party SDKs, several of them Chinese, and a transfer clause without a mechanism, and no representative in the Union 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 HIGH on 23 August 2026

Sections 4 and 5 of the operator's policy name Pangle (ByteDance), BeiZi, Umeng, AMap (Alibaba), QQ (Tencent), Alipay, WeChat (Tencent) and Bugly (Tencent), each with its own list of collected identifiers. The dex strings confirm class packages for six of the eight, shown below. Class evidence for Pangle was not located (see M4). The dex strings also hold an Alibaba Cloud IoT Hub MQTT broker endpoint, a persistent two way channel. Whether the app uses it for commands or only for telemetry is UNVERIFIED. Section 4 of the policy says that the information collected about the user is stored on the servers of WearPro and its affiliates and may be transmitted to the user's country or region or overseas. It names no transfer mechanism. The findings file and the notice attribute to the policy a sentence that information is stored on servers within the People's Republic of China. That sentence is not reproduced verbatim in the findings file and was not re-read, so the point is UNVERIFIED. The policy was last updated on 2023-11-16. No Union representative was found in the manifest, resources or policy.

```
Policy section 4: "The information and profile collected by WearPro about you will be
    stored on the servers of WearPro and/or its affiliates. This information and
    profile may be transmitted to your country, region or overseas where WearPro
    collects the information and data and accessed abroad, storage and display."
```

```
Lcom/alipay/sdk/            Lcom/amap/api/              Lcom/tencent/bugly/
Lcom/tencent/connect/avatar/  Lcom/tencent/mm/opensdk/   Lcom/tencent/open/c/
Lcom/umeng/analytics/        Lcom/umeng/commonsdk/       Lcom/umeng/umzid/

tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
```

Impact: A user in the Union cannot tell from the policy which safeguard covers a transfer of identifiers to eight companies, several of them in the People's Republic of China.

Fix: Name the Chapter V mechanism for each recipient and appoint a Union representative.

H4: Contacts, SMS and call data of people who never installed the app are synchronised through the app to the watch

---

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 onboarding string app_pair_success_des says that sports, health, messages, location, contacts, device configuration and device information are synchronised between the phone and the wearable through the app. The contacts screens carry the strings Sync cards to watch and Manage contacts. The manifest declares READ_CONTACTS, READ_SMS, RECEIVE_SMS, READ_CALL_LOG and ANSWER_PHONE_CALLS, a ContactsActivity and a NotificationReceiver that holds the BIND_NOTIFICATION_LISTENER_SERVICE permission. People in the contact list, senders of SMS and parties of calls never saw any consent screen of the app. The string says that the data passes through the app process. Whether it is also stored or sent to the backend beyond the Bluetooth hop is UNVERIFIED.

```
<string name="app_pair_success_des">Your sports, health, messages, location, contacts,
     device configuration,
device information and other data will be synchronized between your phone and wearable
     device through the %s App.</string>
app_contact_find_des = "Sync cards to watch"
app_contract_des = "Manage contacts"
com.wear.lib_core.mvp.view.activity.ContactsActivity
com.wear.lib_core.notification.NotificationReceiver (
    BIND_NOTIFICATION_LISTENER_SERVICE)
```

Impact: Friends, family and colleagues of the user are processed without knowing it.

Fix: State what happens to relayed data, keep it on the device and limit the listener to the apps that the watch feature needs.

M1: Cleartext traffic is permitted for the whole app 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 MEDIUM on 23 August 2026

The application element of AndroidManifest.xml sets android:usesCleartextTraffic= ”true” and points to res/xml/network_config.xml, which holds one base-config with clear-textTrafficPermitted set to true. There is no domain-config and no pin-set, so the setting applies to every host. The app targets API level 36, where cleartext HTTP is refused by default. H2 shows two concrete plain HTTP endpoints in the same build. The data that the plain HTTP endpoints carry was not observed, so the impact metrics of the vector are set to limited and not high.

```
<application ... android:networkSecurityConfig="@xml/network_config" android:
    usesCleartextTraffic="true">

<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

Impact: Anyone on the network path can read or alter unencrypted traffic of the app, if it occurs.

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

M2: A Google API key is hardcoded in the dex files

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

The dex strings hold the Google API key below. It is a client side key by design and a quota or billing abuse surface if it is not restricted. Whether it is restricted by package name, signature or API was not tested because that needs a live call.

```
AIzaSyDyVbOBuy7XPAbGjU738-EHXfABozjqMSY
```

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

Fix: Restrict the key by package name, signature and API.

M3: PEGI 3 rating against payment rails, advertising permissions and a minors notice that nothing enforces

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

The Play listing carries PEGI 3. The only age related string is a notice that a minor under 14 should read the terms with a guardian and use the products with the guardian's consent. The resources and the dex strings show no date of birth field, no blocking gate and no parental consent class. The package integrates PayPal checkout (com.paypal.pyplcheckout.*), Alipay (com.alipay.sdk.*) and WeChat Pay (com.dtno1.WearPro.wxapi.WXPayEntryActivity), the advertising ID permissions, and the screens GameDetailsActivity, GameVipActivity and VipActivity. A server side age check cannot be seen.

```
Google Play content rating: PEGI 3
res/values/strings.xml line 2821: "Please note: If you are a minor under 14 years old,
     you need to read %4$s carefully with your guardian, and use our products and
    services with your guardian's consent. or provide information to us."
```

Impact: A child can install an app rated for everyone that carries payment rails and advertising permissions.

Fix: Align the rating with the feature set and add an age gate with a parental consent path.

M4: The Pangle open ad SDK permission is declared and no Pangle class was found in the dex files

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

The manifest declares the package specific permission below. It is generated by the manifest merger of the Pangle Open Ad SDK, so the SDK was in the dependency graph at build time. A string search of all six classes*.dex files for pangle, bytedance, pangolin, openadsdk and TTAdSdk found no match. Two explanations fit. Code shrinking may have removed unused SDK classes while the generated permission remained, or the classes exist under names that a literal search does not find. The finding is unresolved and is recorded without a claim either way. It carries no score.

```
com.dtno1.WearPro.openadsdk.permission.TT_PANGOLIN
```

Impact: The policy names Pangle as a recipient of device identifiers. If the SDK is present, the recipient is real, and if it is not, the policy overstates the processors.

Fix: Confirm whether the SDK ships in the build and align the policy.

M5: An exported provider of the bundled 3-D Secure SDK has no permission

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

AndroidManifest.xml line 670 declares the provider com.cardinalcommerce.a.setShadowLayer with authority com.dtno1.WearPro.CCInitProvider as exported without a permission. CardinalCommerce is a 3-D Secure 2 authentication SDK that supports the PayPal and card checkout. The provider is a routine part of that SDK and typically holds configuration. No exposure of user data was shown, and what is queryable through it is UNVERIFIED.

```
<provider android:authorities="com.dtno1.WearPro.CCInitProvider" android:enabled="true
    "
          android:exported="true" android:name="com.cardinalcommerce.a.setShadowLayer
    "/>
```

Impact: The effect depends on what the provider exposes, which was not examined.

Fix: Check the provider with the SDK vendor and restrict it if possible.

Impact Analysis

The people affected are the more than 5 million installers, who wear a watch and grant Bluetooth, location, phone, SMS, contacts, camera and microphone access. Some may be children, since the Play rating is PEGI 3. People in the contact lists, senders of SMS and parties of calls are affected as well and never installed the app.

The weight of the case sits on three points. The Data Safety card says that no data is collected, and the operator's own policy names eight processors and the collection of device identifiers (C1). The app permits plain HTTP for every host and ships two literal plain HTTP endpoints (M1, H2). Contacts and messages of third parties pass through the app (H4).

What the package shows is configuration, file content and the operator's own text. No contact, message or identifier was observed leaving a device and the report asserts no such flow. A check of Health Connect permission constants for pregnancy data found them in the permission catalogue of the bundled Health Connect library and not in the manifest. No finding rests on them.

The Complete Chain

Step 1, listing: the user reads a Data Safety card that says no data is collected (C1).

Step 2, first start: Google Mobile Ads and ML Kit construct at process creation and the agreement dialog follows (C2).

Step 3, pairing and use: the user grants SMS, call, contacts, location, camera and microphone access. The app relays contacts, messages and calls to the watch (H4). The watch can trigger the phone camera and two exported services can be started by other apps (H1).

Step 4, backend: the app calls the production host, may call two plain HTTP test endpoints, and holds an IoT Hub MQTT channel (H2, H3). The configuration permits plain HTTP (M1).

Step 5, rights: the policy names eight recipients and a transfer clause without a mechanism. No representative exists in the Union (H3).

Engine Fingerprint and Correlation Keys

WearPro does not belong to the Bluetrum cluster of HryFine and Wearfit Pro. The string com.bluetrum.abpartool and the library libabpartool.so are absent. Its engine is com.wear.lib_core (371 classes) wrapping com.crrepa.ble.* (781 classes, with Realtek and Sifli update support). The same com.crrepa.ble namespace is recorded in the R1 findings of Da Fit and Pubu Wear in this programme, which are published by other developers. WearPro therefore belongs to the Moyoung CRRepa family and not to the Bluetrum family. The Nordic DFU library, which looked like a discriminator, is present in both WearPro and Wearfit Pro and is a generic library, so it is not used as a key. Signing certificates differ between storefronts and are not a cluster key.

Key	WearPro	Wearfit Pro
com.bluetrum.abpartool / libabpartool.so	absent	present (23 string matches)
com.wear.lib_core.*	present (371 classes)	absent
com.crrepa.ble.*	present (781 classes)	absent
no.nordicsemi.* (generic DFU library)	present	present (136 string matches)
Operator	Shenzhen Wanruxia Technology Co., Ltd.	Shenzhen Weike Technology Co., Ltd.

```
XAPK SHA-256
    fcdf186717ce532be94ed11d090b5983f0f43f1ed47ac7e62d63e420c2d646b4
Base APK SHA-256
    b47049ba438693786046ac0d722bb7948fade0a0953e2919fb8e419e0d6be603
Signing cert SHA-256
    5f505d51de8f2fc30ac8da3c141bf1af8cda9d30b9712e0933923b782f60d400
Signing DN              CN=zh (self-signed, no other field)
Backend                 https://dt1pro.wanruxia.com/xky-api/
MQTT broker             tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
Moyoung API host        api.moyoung.com
```

The Wearfit Pro comparison rests on the on-disk decompile that the findings file names and on the R1 files of HryFine and WearFit2.0, which are not part of this package. The numeric BLE manufacturer identifiers and UUID values were not extracted. The correlation therefore holds at namespace level.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2 and H4.

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

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

Article 6(1) and Article 7(1): engaged by C2. Article 6(1) is engaged by H4.

Article 8: engaged by M3.

Articles 12 to 14: engaged by C1. Article 13(1)(e) is open for M4 and Article 14 is engaged by H4.

Article 25: engaged by H1 and M3.

Article 27: engaged by H3. No representative is named.

Article 32: engaged by H1, H2, M1, M2 and, as an open question, M5.

Articles 44 and 46: engaged by H3. The policy names a transfer clause and no 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 collected, and separately that the app may share App info and performance and Device or other IDs with third parties. The statement that no data is collected does not match the operator’s own policy and the permission set (C1).

Regulatory & Legal Landscape

Shenzhen Wanruxia 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.dtno1.WearPro
Version            3.8.4.0 (versionCode 244), minSdk 24, targetSdk 36
XAPK SHA-256 (122,756,532 bytes)
    fcdf186717ce532be94ed11d090b5983f0f43f1ed47ac7e62d63e420c2d646b4
Base APK SHA-256
    b47049ba438693786046ac0d722bb7948fade0a0953e2919fb8e419e0d6be603
Signing cert SHA-256
    5f505d51de8f2fc30ac8da3c141bf1af8cda9d30b9712e0933923b782f60d400
Audit device       none, the app was not installed
Acquisition        APKPure mirror (published hash matches), checked against the Google
     Play listing, 2026-08-23
```

```
Google API key
    AIzaSyDyVbOBuy7XPAbGjU738-EHXfABozjqMSY
Plain HTTP endpoints
    http://192.168.110.182/xky-api/
    http://39.108.214.143/wearpro/
Production host
    https://dt1pro.wanruxia.com/xky-api/
MQTT broker
    tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
Policy              https://dt1pro.cn/wearpro_privacy_en.html  (last updated
    2023-11-16)
Contacts            developer@dtone.cc, support@dtone.cc, info@dtno1.com
```

```
C1  Google Play Data Safety card, manifest.json (permissions), operator policy
    sections 1, 4 and 5
C2  AndroidManifest.xml (providers), res/values/strings.xml line 2814
H1  AndroidManifest.xml (LocationService, WearEngineService), classes*.dex (camera
    strings), policy section 1.5
H2  classes*.dex (literal endpoints)
H3  operator policy sections 4 and 5, classes*.dex (class packages, MQTT endpoint)
H4  res/values/strings.xml line 1274, AndroidManifest.xml
M1  AndroidManifest.xml, res/xml/network_config.xml
M2  classes*.dex (API key)
M3  Google Play listing, res/values/strings.xml line 2821
M4  manifest.json (TT_PANGOLIN permission), classes*.dex (negative search)
M5  AndroidManifest.xml line 670
```

Reproduction: obtain com.dtno1.WearPro 3.8.4.0 (244), check the SHA-256 values above, decode the manifest and resources with apktool without sources, extract strings from the six dex files and read the policy. 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 WEARPRO-2026-R1 at 00:08 UTC to developer@dtone.cc and support@dtone.cc, CC dsb@dsb.gv.at and edps@edps.europa.eu. A permanent failure notice for support@dtone.cc followed at 00:08 UTC.

2026-08-23 Unchanged redelivery at 07:17 UTC to info@dtno1.com and developer@dtone.cc, CC dsb@dsb.gv.at and edps@edps.europa.eu. Embargo date 21 November 2026.

2026-09-12 Follow-up at 12:58 UTC to info@dtno1.com and developer@dtone.cc with the three questions and an answer date of 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:09 UTC, under the subject 35 days to publication: WearPro.

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 Google User Messaging Platform is integrated (ConsentInformation, UserMessagingPlatform and the IABTCF key set), which is a real consent platform for the advertising stack. A first run agreement dialog exists and a plain notice asks minors under 14 to involve a guardian. The policy names its eight third party SDKs individually, each with a list of collected data and a link to the partner’s policy, which is more granular than most policies in this programme and made the cross-checking possible. The application element sets allowBackup to false. The Data Safety card states that data deletion can be requested.

Residual Risk & Recommendations

Open at the date of publication: all eleven entries. The operator has not replied and the build analysed is version 3.8.4.0 of July 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 manifest and the policy (C1). Second, remove the cleartext allowance and the test endpoints (M1, H2). Third, hold the advertising SDK back until the consent result is available (C2). Fourth, name the Chapter V mechanism per recipient and appoint a Union representative (H3). Fifth, state what happens to relayed contact and message data (H4). Sixth, protect the exported services and restrict the keys and the rating (H1, M2, M3, M5).

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) 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 WEARPRO-2026-R1.