Security & Privacy Disclosure, Final Report

Pubu Wear for Android (com.pubu.dafit)

A Data Safety card that says no data is collected, a policy that names no company, and a reply that asks for more time without answering any of the three questions.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. OPERATOR REPLIED ON 19 OCTOBER 2026 WITHOUT ANSWERING THE QUESTIONS AND ASKED FOR AN EXTENSION, WHICH WAS DECLINED. NO REPLY TO THE NOTICE OF 15 NOVEMBER 2026.

Target	Pubu Technology (Shenzhen) Co., Ltd. (Pubu Wear)
Versions Audited	1.0.0.39 / versionCode 46 (Play update 2025-11-07, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	9: 3 High, 4 Medium, 2 Low (R1 labels reassessed, see status table)
Status	REPLY OF 2026-10-19 WITHOUT ANSWERS, EXTENSION DECLINED, NO REPLY TO NOTICE OF 2026-11-15
SHA-256 (base APK)	`35849a84720f09be5297cab36d6cff0266a5751bd5f5c822aa6ff59f3c2dc855`

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 8

6.1 C1: Cleartext traffic is permitted globally with no pinning across at least five backend hosts, and the Data Safety card admits that data is not encrypted . . 8

6.2 C2: The Data Safety card says no user data is collected while the manifest and the operator's own privacy policy describe the collection of calls, SMS and address book data 9

6.3 H1: The privacy policy names no company, no address and no representative in the Union, and its only controller contact is a mailbox on a domain that matches neither the app nor the listed company 10

6.4 H2: The policy states that data is stored in the People's Republic of China and names no transfer mechanism, and the app is built on a licensed chipset SDK with two backend layers 11

6.5 H3: An exported boot receiver, an exported notification listener at the highest filter priority and an SMS receiver run with no consent platform in the package 12

6.6 H4: Menstrual cycle and ovulation tracking and a remotely triggerable camera share one cleartext capable app with no impact assessment on record 13

6.7 M1: A Google Maps key and an AutoNavi (Alibaba) key are hardcoded and the AMap SDK is not named in the policy 14

6.8 M2: The application allows backup of its private data 14

6.9 M3: PEGI 3 rating against SMS, call and contacts access, camera, microphone and reproductive health tracking, with no age gate in the resources 15

7 Impact Analysis 15

8 The Complete Chain 16

9 SDK Lineage and Fingerprint Keys 16

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 18

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 21

Executive Summary

Pubu Wear is a companion app for smart watches with more than one million downloads on Google Play (1M+ on the listing read on 17 November 2026, 500K+ at the notice of 23 August 2026). The listed publisher is [illegible], Pubu Technology (Shenzhen) Co., Ltd. The listing shows PEGI 3 and a Data Safety card. On 23 August 2026 RFI-IRFOS sent a notice with REF PUBUWEAR-2026-R1 to hezhiyuan55@gmail.com and weiyuxiang@yawellfit.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 1.0.0.39 shows that the Data Safety card says no user data is collected, while the manifest requests SMS, call log, contacts, background location, camera and microphone permissions and the operator's own policy says that the app receives calls, SMS and address book data (C2). The app permits cleartext traffic for every host and the card itself admits that data is not encrypted (C1). The policy names no company, no address and no representative in the Union and its controller contact sits on an unrelated domain (H1). The policy states that data is stored in the People's Republic of China without a transfer mechanism (H2). A boot receiver, an exported notification listener and an SMS receiver run without a consent platform (H3), and a cycle and ovulation tracking module sits in the same app with a camera that the watch can trigger (H4). The package carries no advertising SDK.

A reassessment by CVSS v4.0 band puts three findings at High, four at Medium and two at Low. The two Critical labels of 23 August 2026 move down because the package shows configuration and file content and not runtime behaviour. Three High labels move down for the same reason. C2 and H4 stay 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 or to the follow-up of 12 September 2026. On 19 October 2026 the support mailbox answered the follow-up of 17 October 2026. The message says that an investigation will take place, asks for an extension beyond 21 November 2026 and welcomes further technical evidence. It answers none of the three questions and gives no completion date. RFI-IRFOS declined the extension on the same day and kept the date. On 15 November 2026 RFI-IRFOS sent a notice six days before publication from security@rfi-irfos.com to both addresses. The mail relay of yawellfit.com returned it for weiyuxiang@yawellfit.com with the error 550 5.7.25 and returned no error for hezhiyuan55@gmail.com. No reply has arrived. This report records the state of the correspondence on 21 November 2026, with no reply to the notice of 15 November 2026 and no other message after 19 October 2026.

Scope: Root level code analysis of the Google Play release 1.0.0.39 (versionCode 46). The package was obtained as an XAPK bundle (85.7 MB, base APK of 52,149,234 bytes plus armeabi-v7a, mdpi and English splits) from the APKPure mirror and checked against the package name, version and update date of 7 November 2025 on the live Google Play listing. Work done: a resources only decode with apktool (no source decode), the manifest and network security configuration, a string pass across all four classes*.dex files (367,353 string table lines) and an inventory of native library names with hashes. The live Google Play listing and the operator's 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	Cleartext traffic is permitted globally with no pinning across at least five backend hosts, and the Data Safety card admits that data is not encrypted
C2	HIGH	The Data Safety card says no user data is collected while the manifest and the operator’s own privacy policy describe the collection of calls, SMS and address book data
H1	MEDIUM	The privacy policy names no company, no address and no representative in the Union, and its only controller contact is a mailbox on a domain that matches neither the app nor the listed company
H2	MEDIUM	The policy states that data is stored in the People’s Republic of China and names no transfer mechanism, and the app is built on a licensed chipset SDK with two backend layers
H3	MEDIUM	An exported boot receiver, an exported notification listener at the highest filter priority and an SMS receiver run with no consent platform in the package
H4	HIGH	Menstrual cycle and ovulation tracking and a remotely triggerable camera share one cleartext capable app with no impact assessment on record
M1	MEDIUM	A Google Maps key and an AutoNavi (Alibaba) key are hardcoded and the AMap SDK is not named in the policy
M2	LOW	The application allows backup of its private data
M3	LOW	PEGI 3 rating against SMS, call and contacts access, camera, microphone and reproductive health tracking, with no age gate in the resources

Finding Status at a Glance

ID	Disclosed	This report	State on 21 November 2026
C1	CRITICAL	HIGH	Operator reply of 19 October 2026 answers none of the questions. Plain HTTP use not listed.
C2	CRITICAL	HIGH	Operator reply of 19 October 2026 answers none of the questions. Contradiction shown by two public documents.
H1	HIGH	MEDIUM	Operator reply of 19 October 2026 does not name the controller.
H2	HIGH	MEDIUM	Operator reply of 19 October 2026 does not name a transfer mechanism.
H3	HIGH	MEDIUM	Operator reply of 19 October 2026 does not address consent. Capability only.
H4	HIGH	HIGH	Operator reply of 19 October 2026 does not state whether an impact assessment exists.
M1	MEDIUM	MEDIUM	No reply on this point. Key restrictions not visible from the package.
M2	MEDIUM	LOW	No reply on this point. Capability needing physical access.
M3	MEDIUM	LOW	No reply on this point. Age gate not found in resources.

The findings file of 23 August 2026 labels C1 and C2 as Critical, H1 to H4 as High and M1 to M3 as Medium. The report uses the CVSS v4.0 band of each finding. C2 and H4 stay High through blast-radius escalations that the findings state.

Subject & Operator Analysis

The Google Play developer panel lists [redacted] (Pubu Technology (Shenzhen) Co., Ltd.), Wuhan University Shenzhen Industry-Research Building A403, 6 Yuexing 2nd Road, Gaoxin Community, Yuehai Sub-district, Nanshan District, Shenzhen, Guangdong 518000, People's Republic of China. The support contact is hezhiyuan55@gmail.com, a personal mailbox, and the developer contact is weiyuxiang@yawellfit.com on a third domain. A mobile phone number is published on the listing and is not reproduced here.

The policy is hosted at api2.qcwxkjvip.com, the same domain that serves a backend of the app (H2). It names no company and gives the yawellfit.com mailbox as the data controller contact (H1). Who is the controller, the listed company, the operator behind yawellfit.com or the vendor of the underlying SDK, is the first of the three questions and was not answered.

The signing certificate carries the generic DN CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US. It can be the Google Play App Signing certificate or an artefact of the mirror that supplied the file, and the origin is UNVERIFIED until the file is compared with a Play install. Pubu Technology also publishes Pubu Ring (com.pubu.smart.ring), Maxx Smart Fit and Maxx Fit Pro under the same developer account. They were not audited. The Austrian Datenschutzbehörde receives the notice in copy and can receive complaints directly.

Architecture & Data Flow

Pubu Wear is a native Android app with four classes*.dex files and an armeabi-v7a native split. The visible brand is Pubu and the internal package root is com.qcwireless.qcwatch. Inside it, the BLE SDK com.crrepa.ble.* (1,313 classes) supports chipset families of Goodix, Nordic, Realtek and Huntersun. Native libraries include libRtkAesJni.so, libAMapSDK_MAP_v9_8_2.so, libhyphenate.so (Easemob messaging), libffmpeg.so and libcipherdb.so.

The app talks to the watch over Bluetooth Low Energy and receives phone events through the SMS receiver, the boot receiver and the notification listener (H3). The dex strings name two backend layers, api.moyoung.com and the hosts of qcwxkjvip.com and qcwxwire.com, an Alibaba Cloud OSS bucket and the AutoNavi and Easemob services (C1, H2). The policy states that firmware update and log data is stored in the People's Republic of China. No data flow was observed.

Engagement Summary

The notice REF PUBUWEAR-2026-R1 was sent on 23 August 2026 at 07:17 UTC from rfi.irfos@gmail.com to hezhiyuan55@gmail.com and weiyuxiang@yawellfit.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. A follow-up of 12 September 2026 at 13:02 UTC restated the findings and the three questions. A second follow-up of 17 October 2026 at 19:08 UTC came from security@rfi-irfos.com under the subject 35 days to publication: Pubu Wear. On 19 October 2026 at 06:14 UTC the support mailbox, with weiyuxiang@yawellfit.com in copy, replied. The message is signed Pubu Wear Team. It says that the operator takes the concerns seriously and will investigate, says that more time will be needed, asks for an extension of the disclosure timeline beyond 21 November 2026 and for a discussion of a revised timeline, and welcomes further technical evidence and reproducible test cases. It states no completion date and answers none of the three questions. On 19 October 2026 at 07:19 UTC RFI-IRFOS declined the extension from s.kepp@rfi-irfos.com, restated the reproduction pointers and the three questions and kept the date. On 15 November 2026 at 12:54 UTC RFI-IRFOS sent a notice six days before publication from security@rfi-irfos.com to both addresses under the subject 6 days to publication: Pubu Wear, 84 days since delivery. It listed the nine entries and the three questions. The mail relay of yawellfit.com returned the message for weiyuxiang@yawellfit.com at 12:55 UTC with the error 550 5.7.25, no valid PTR record for the sending IP. No error came back for hezhiyuan55@gmail.com. RFI-IRFOS did not resend it, since the operator received the notice through the first address. No reply has arrived by 21 November 2026.

Findings

C1: Cleartext traffic is permitted globally with no pinning across at least five backend hosts, and the Data Safety card admits that data is not encrypted

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2 (CVSS-B), disclosed as CRITICAL on 23 August 2026

res/xml/network_security_config.xml holds a single base-config with cleartextTrafficPermitted set to true and no domain-config block, and the application element of AndroidManifest.xml sets android:usesCleartextTraffic=”true”. Nothing restricts cleartext and nothing pins a certificate. The app targets API level 35, where cleartext HTTP is refused by default. The dex string pool of all four classes*.dex files names the hosts below. The app carries health measurements, SMS and call payloads and location data. The live Data Safety card of 23 August 2026 says that data is not encrypted, so the card and the configuration agree on this point. Which of the hosts the app reaches over plain HTTP could not be listed because no bytecode pass was done, and the policy page itself is served over HTTPS. Actual use of plain HTTP is therefore UNVERIFIED.

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

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

```
api1.qcwxkjvip.com   api2.qcwxkjvip.com   api1.qcwxwire.com   china.qcwxwire.com
api.moyoung.com
qcwx.oss-us-west-1.aliyuncs.com   (Alibaba Cloud object storage)
restapi.amap.com and family   (AutoNavi / AMap)
kefu.easemob.com   kefu-sdk-log.easemob.com   (Easemob customer service)
```

Impact: More than one million installers use an app whose transport settings allow anyone on the network path to read unencrypted traffic, if it occurs, for health measurements, relayed SMS and call data and location.

Fix: Remove both cleartext allowances, add a domain based network security configuration and pin first party hosts.

C2: The Data Safety card says no user data is collected while the manifest and the operator's own privacy policy describe the collection of calls, SMS and address book data

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 page also says that the app may share Device or other IDs with third parties, that Data isn't encrypted and that Data can't be deleted, so the card is inconsistent with itself. The manifest requests READ_SMS, RECEIVE_SMS, READ_CALL_LOG, READ_PHONE_STATE, ANSWER_PHONE_CALLS, READ_PHONE_NUMBERS, READ_CONTACTS, WRITE_CONTACTS, CALL_PHONE, ACCESS_BACKGROUND_LOCATION, ACCESS_FINE_LOCATION, CAMERA, RECORD_AUDIO, RECEIVE_BOOT_COMPLETED, QUERY_ALL_PACKAGES and GET_INSTALLED_APPS. The operator's policy says that the app receives the incoming call, SMS and address book data and that storage of data for a firmware update and the log file takes place in the People's Republic of China. The policy also says that this call, SMS and address book data is used for display on the watch and is not stored. That claim could not be checked from the package. 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 one million installs, it contradicts the operator's own policy point for point, and the app handles SMS, call and address book data and reproductive health tracking.

```
Data Safety card: "No data collected. The developer says this app doesn't collect user
     data."
Same page: "may share Device or other IDs with third parties", "Data isn't encrypted",
     "Data can't be deleted"
```

```
Policy: "When you connect our device and use the incoming call and SMS reminder
    function, Pubu Wear receives the incoming call, SMS, address book data and
    monitors the status of mobile phone calls... The storage of this data for a
    firmware update as well as the log file takes place in the PRC."
```

Impact: More than one million installers are told before the install that nothing is collected. The same operator tells them in its policy that calls, SMS and the address book are received.

Fix: Correct the Data Safety declaration to match the manifest and the policy and state which data is stored where.

H1: The privacy policy names no company, no address and no representative in the Union, and its only controller contact is a mailbox on a domain that matches neither the app nor the listed company

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

Section 6 of the policy, headed contact information, is the whole controller identification. It reads: Data controller in terms of the GDPR: Contact: weiyuxiang@yawellfit.com. It names no company and gives no address, no jurisdiction and no Union representative. The domain yawellfit.com matches neither the Google Play entity [illegible] (Pubu Technology (Shenzhen) Co., Ltd.) nor the brand names Pubu and dafit. The Google Play developer panel is the only place where a company name and address appear. The policy states that a Personal Data Protection Officer has been established and names no individual. The policy is dated 28 February 2022, and the app was last updated on 7 November 2025.

```
6. contact information  If you have any questions ... please contact us by email. We
    will respond to you within 15 working days ...
Data controller in terms of the GDPR: Contact: weiyuxiang@yawellfit.com
```

```
Play developer       □□□□□□()□□□□ (Pubu Technology (Shenzhen) Co., Ltd.)
Play address         6 Yuexing 2nd Road, Gaoxin Community, Yuehai Sub-district,
    Nanshan District, Shenzhen, Guangdong 518000, China
                     (Wuhan University Shenzhen Industry-Research Building A403)
Play support         hezhiyuan55@gmail.com
Play developer contact  weiyuxiang@yawellfit.com
Policy controller contact  weiyuxiang@yawellfit.com
```

Impact: A person who wants access or deletion cannot tell which company answers, and no representative exists in the Union.

Fix: Name the controlling company with address, a Union representative and a Data Protection Officer in the policy.

H2: The policy states that data is stored in the People's Republic of China and names no transfer mechanism, and the app is built on a licensed chipset SDK with two backend layers

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 policy says that the storage of data for a firmware update and the log file takes place in the PRC. No standard contractual clause, adequacy decision or other mechanism under Chapter V is named anywhere in the policy. The dex string pool shows that the application class is com.qcwireless.qcwatch.QCApplication, a package name that does not appear on the listing. Inside it, 1,313 classes live under com.crrepa.ble.*, the BLE SDK namespace that the R1 findings of Da Fit and WearPro in this programme also record. Classes such as com.qcwireless.qcwatch.ui.base.watch.dafit.MoYDeviceCmdInit and MoYBluetoothManager name a dafit and a MoY protocol variant side by side. The app calls api.moyoung.com directly and runs its own backend on qcwxkjvip.com and qcwxwire.com, including the host china.qcwxwire.com, and an Alibaba Cloud OSS bucket named qcwx. What data goes to which backend was not observed and is UNVERIFIED.

```
Policy: "The storage of this data for a firmware update as well as the log file takes
    place in the PRC."

com.qcwireless.qcwatch.QCApplication, LoadingActivity
com.crrepa.ble.*  (1,313 classes)
com.qcwireless.qcwatch.ui.base.watch.dafit.MoYDeviceCmdInit
com.qcwireless.qcwatch.ui.base.watch.dafit.MoYBluetoothManager
api.moyoung.com   api1.qcwxkjvip.com   api2.qcwxkjvip.com   api1.qcwxwire.com   china.
    qcwxwire.com
qcwx.oss-us-west-1.aliyuncs.com
```

Impact: A user in the Union cannot tell from the policy which safeguard covers the transfer of the stated data to the People's Republic of China, nor which company runs the second backend that the app also calls.

Fix: Name the Chapter V mechanism and the recipients, and describe the roles of the operator, the SDK vendor and the backend operator.

H3: An exported boot receiver, an exported notification listener at the highest filter priority and an SMS receiver run with no consent platform in the package

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

AndroidManifest.xml registers com.qcwireless.qcwatch.ui.base.receiver.BluetoothReceiver (exported, BOOT_COMPLETED and CONNECTIVITY_CHANGE) and com.qcwireless.qcwatch.ui.device.push.service.MyNotificationService, an exported NotificationListenerService with the BIND_NOTIFICATION_LISTENER_SERVICE permission and intent filter priority 0x7FFFFFFF. The dex also holds com.qcwireless.qcwatch.ui.device.push.message.SmsReceiver. The receiver starts at boot, before any screen can show a consent dialog. The listener can see the notifications of apps that the user never connected to the watch. A full binary search for OneTrust, Didomi, Usercentrics and the IAB TCF markers returned no match. The package carries no advertising SDK, so there is no advertising consent to gate, and the open question is consent to the handling of SMS, call and notification data. Whether notification content is parsed, stored or sent was not shown and is UNVERIFIED.

```
<receiver android:exported="true" android:name="com.qcwireless.qcwatch.ui.base.
    receiver.BluetoothReceiver">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
        ...
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
    </intent-filter>
</receiver>

<service android:enabled="true" android:exported="true"
    android:name="com.qcwireless.qcwatch.ui.device.push.service.MyNotificationService"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter android:priority="0x7FFFFFFF">
        <action android:name="android.service.notification.NotificationListenerService
    "/>
    </intent-filter>
</service>
```

Impact: People who write to the wearer are processed without knowing it, and the wearer is given no mechanism that records a consent decision.

Fix: Add a recorded consent step before the relay features start and limit the listener to the apps that the watch feature needs.

H4: Menstrual cycle and ovulation tracking and a remotely triggerable camera share one cleartext capable app with no impact assessment on record

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

The dex string pool holds the field and class names of a full cycle tracking module: FIELD_MENSTRUAL_FLOW, FIELD_OVULATION_TEST_RESULT, MENSTRUAL_FLOW_HEAVY, MENSTRUAL_FLOW_MEDIUM, MENSTRUAL_FLOW_LIGHT, MENSTRUAL_FLOW_SPOTTING, isMenstrualReminder, isOvulationDayReminder, isOvulationEndReminder and getMenstrualPeriod, next to heart rate, SpO2, blood pressure, sleep and temperature. com.qcwireless.qcwatch.ui.device.camera.CameraActivity implements takePicture, toggleFlash and synCameraState, which matches the Play description feature to rotate the wrist to take photos. The camera is triggered from the paired wearable. CAMERA, RECORD_AUDIO, location and the health surface are all declared. The resources show no age gate and no Article 9(2) consent flow. That is a result of a resource and string search and was not confirmed at code level, so it is UNVERIFIED as an absence. A data protection impact assessment is not published and none was found in the package. What the app stores or sends for these features was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the data is reproductive health data of the kind that Art. 9 protects most, the app has more than one million installs, the cycle module is a complete product feature, and the controller named in the policy cannot be identified.

```
FIELD_MENSTRUAL_FLOW, FIELD_OVULATION_TEST_RESULT,
MENSTRUAL_FLOW_HEAVY, MENSTRUAL_FLOW_MEDIUM, MENSTRUAL_FLOW_LIGHT,
    MENSTRUAL_FLOW_SPOTTING,
isMenstrualReminder, isOvulationDayReminder, isOvulationEndReminder,
    getMenstrualPeriod

com.qcwireless.qcwatch.ui.device.camera.CameraActivity  takePicture, toggleFlash,
    synCameraState
```

Impact: A person who tracks a cycle or ovulation, perhaps to plan or avoid a pregnancy, enters data with acute real world sensitivity into an app whose transport settings allow plain HTTP and whose controller is not named in its own policy.

Fix: Gate the health features behind explicit consent under Art. 9(2)(a), encrypt all transport, complete and publish the outcome of a data protection impact assessment and secure the camera trigger.

M1: A Google Maps key and an AutoNavi (Alibaba) key are hardcoded and the AMap SDK is not named in the policy

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

AndroidManifest.xml holds the two meta-data entries below. They are client side keys by SDK design and each is a quota or billing abuse surface if scraped. Restrictions on the keys could not be seen and were not tested. The native library libAMapSDK_MAP_v9_8_2.so and the AMap asset set ship in the build, so a PRC mapping SDK is present whether or not it is called for a user in the Union. The policy names Google Maps and AccuWeather as location recipients and does not name AMap.

```
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyDR6r3GJmTh4uf8_oe66Hc96JWptY7Y6gI"/>
<meta-data android:name="com.amap.api.v2.apikey" android:value="
    f1996a860112bbe6c9fa77381ffd26d4"/>
```

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

Fix: Restrict the keys by package name and signature and add the AMap SDK to the policy recipient list, or remove it.

M2: The application allows backup of its private data

LOW, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The application element of AndroidManifest.xml sets android:allowBackup="true". The sibling app Da Fit in this programme sets it to false. The flag allows extraction of the private application data directory by backup tooling on a device that is physically accessible or in debug mode. The app holds health, location and communications related data.

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

Impact: Extraction needs access to the unlocked device or a debug connection.

Fix: Set allowBackup to false or exclude sensitive files from backup.

M3: PEGI 3 rating against SMS, call and contacts access, camera, microphone and reproductive health tracking, with no age gate in the resources

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

The Play listing carries PEGI 3. The app description says that its key function can only be realised by using phone, contact and SMS permissions. The resources show no age gate, no date of birth field and no parental consent string. The app offers cycle tracking, camera and microphone access. A server side or code side age check cannot be seen without a bytecode pass.

```
Google Play content rating: PEGI 3
Resource search: no age gate, date of birth or parental consent string
```

Impact: A child can install an app rated for everyone that offers reproductive health tracking and intermediates calls, SMS and the address book.

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

Impact Analysis

The people affected are the more than one million installers who wear a watch and grant Bluetooth, location, phone, SMS, contacts, camera and microphone access, and some of whom log a menstrual cycle or ovulation. Some may be children, since the Play rating is PEGI 3. Senders of SMS and notifications 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 user data is collected, and the operator’s own policy says that calls, SMS and the address book are received (C2). The configuration permits plain HTTP for every host (C1). The policy names no company and states storage in the People’s Republic of China without a mechanism (H1, H2). A cycle tracking module and a remote camera trigger sit on top of that (H4).

What the package shows is configuration, file content and the operator’s own text. No health reading, message or photo was observed leaving a device and the report asserts no such flow. The package carries no advertising SDK, which is a point in favour of the app.

The Complete Chain

Step 1, listing: the user reads a Data Safety card that says no data is collected (C2).

Step 2, first start: a boot receiver and a notification listener are present and no consent platform exists (H3).

Step 3, pairing and use: the user grants SMS, call, contacts, location, camera and microphone access. The app relays calls and SMS to the watch (C2, H3). Health features record cycle and ovulation data (H4). The watch can trigger the phone camera (H4).

Step 4, backend: the app calls api.moyoung.com and the qcwxkjvip.com and qcwxwire.com hosts and the configuration permits plain HTTP (C1). The policy states storage in the People's Republic of China (H2).

Step 5, rights: a person who wants access or deletion finds a controller contact on an unrelated domain and no representative in the Union (H1).

SDK Lineage and Fingerprint Keys

The namespace com.crrepa.ble.* with 1,313 classes matches the BLE SDK namespace that the R1 findings of Da Fit (781 classes in the same namespace) and WearPro in this programme record. Da Fit and WearPro are published under different developer entities. The R1 finding is that the same Shenzhen BLE SDK sits under at least three storefront brands. Pubu Wear adds a wrapper layer between the SDK and the storefront. Its internal package com.qcwireless.qcwatch and the domains qcwxkjvip.com and qcwxwire.com name neither Pubu nor the SDK vendor. The R1 file calls that layer QC Wireless. That is a label taken from the package and domain names, and no company of that name was confirmed. The signing certificate does not match the self-signed Da Fit certificate, which is either a real difference between licensees or an artefact of the mirror.

```
Base APK SHA-256         35849
    a84720f09be5297cab36d6cff0266a5751bd5f5c822aa6ff59f3c2dc855
XAPK SHA-256             919
    ed10bf4ca238f8929705cb3f19ff3b2c073af6530a299e96fa03082125f03
libRtkAesJni.so SHA-256
    f35a6552718bcb6e1ef69ece65bf4db030689a212a920e9b607352a607e0ca39   (config.
    armeabi_v7a split)
Signing cert SHA-256
    EC8DEB38F9C5A79865D0010EED973BC758FEB0F2E8478168B5A732EE0D52E2A2
Signing DN               CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=
    California, C=US (origin UNVERIFIED, see above)
BLE UUID base            xxxxxxxx-3c17-d293-8e48-14fe2e4da212
UUID prefixes            000002fd, 00006287, 00006387, 00006487, 00006587, 0000d0ff,
    020002fd
```

The other native libraries of the split are libAMapSDK_MAP_v9_8_2.so, libcipherdb.so, libDspConfig.so, libezip.so, libffmpeg.so, libhyphenate.so, liblog4a-lib.so, liblog.so, libmediahandle.so and libminilzo.so. Their hashes are not recorded in the findings file, only the hash of libRtkAesJni.so. The UUID set was not compared with the UUID sets of Da Fit and WearPro, and the numeric company identifiers were not extracted, so the correlation holds at namespace level.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C2, H2 and H3.

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

Article 5(1)(f) and Article 32(1)(a) and (b): engaged by C1, H4 and M1. Article 32(1) is engaged by M2.

Article 5(2), accountability: engaged by C2.

Article 7(1): engaged by H3.

Article 8: engaged by M3.

Article 9: engaged by H4 for cycle and ovulation data.

Articles 12(1), 13 and 14: engaged by C2 and H1. Article 13(1)(a) is engaged by H1, Article 13(1)(e) by M1 and Article 13(1)(f) by H2.

Article 25: engaged by C1, H3, H4, M2 and M3.

Article 27: engaged by H1. No representative is named.

Article 35: engaged by H4. No impact assessment is published.

Articles 44 and 46: engaged by H2. The policy states storage in the People's Republic of China and names no transfer mechanism.

Platform Accountability & DSA

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

The Data Safety card was read on 23 August 2026. It says: No data collected, the developer says this app doesn't collect user data. The page also says that the app may share Device or other IDs with third parties, that Data isn't encrypted and that Data can't be deleted. The statement that no data is collected does not match the operator's own policy (C2). The statement that data is not encrypted matches the cleartext configuration of C1.

Regulatory & Legal Landscape

Pubu Technology (Shenzhen) 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.pubu.dafit
Version            1.0.0.39 (versionCode 46), minSdk 26, targetSdk 35, compileSdk 35
XAPK SHA-256       919ed10bf4ca238f8929705cb3f19ff3b2c073af6530a299e96fa03082125f03
    (85.7 MB)
base APK SHA-256   35849a84720f09be5297cab36d6cff0266a5751bd5f5c822aa6ff59f3c2dc855
    (52,149,234 bytes)
Signing cert SHA-256 EC8DEB38F9C5A79865D0010EED973BC758FEB0F2E8478168B5A732EE0D52E2A2
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
Google Maps API key   AIzaSyDR6r3GJmTh4uf8_oe66Hc96JWptY7Y6gI
Amap API key          f1996a860112bbe6c9fa77381ffd26d4
Policy                https://api2.qcwxkjvip.com/download/static/ppm/pubu_ppm.html  (
    dated 28 February 2022)
Contacts              hezhiyuan55@gmail.com, weiyuxiang@yawellfit.com
Hosts                 api1.qcwxkjvip.com, api2.qcwxkjvip.com, api1.qcwxwire.com, china
    .qcwxwire.com, api.moyoung.com,
                      qcwx.oss-us-west-1.aliyuncs.com, restapi.amap.com, kefu.easemob.
    com, kefu-sdk-log.easemob.com
```

```
C1  res/xml/network_security_config.xml, AndroidManifest.xml (application element),
    classes*.dex (hosts)
C2  Google Play Data Safety card, AndroidManifest.xml (permissions), operator policy
H1  operator policy section 6, Google Play developer panel
H2  operator policy, classes*.dex (com.crrepa.ble.*, com.qcwireless.qcwatch.*, hosts)
H3  AndroidManifest.xml (BluetoothReceiver, MyNotificationService), classes*.dex (
    SmsReceiver)
H4  classes*.dex (cycle fields, CameraActivity)
M1  AndroidManifest.xml (meta-data), lib (libAMapSDK_MAP_v9_8_2.so)
M2  AndroidManifest.xml (application element)
M3  Google Play listing, resources
```

Reproduction: obtain com.pubu.dafit 1.0.0.39 (46), check the SHA-256 values above, decode the manifest and resources with apktool without sources, extract strings from the four dex files and read the policy. No device, account or network access is needed. Reading call order and data flow needs a bytecode pass, which was not done.

Disclosure Timeline & Outcome

2026-08-23 Notice REF PUBUWEAR-2026-R1 at 07:17 UTC to hezhiyuan55@gmail.com and weiyuxiang@yawellfit.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Findings, three questions, embargo date 21 November 2026.

2026-09-12 Follow-up at 13:02 UTC to both addresses.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:08 UTC, under the subject 35 days to publication: Pubu Wear.

2026-10-19 Reply from hezhiyuan55@gmail.com at 06:14 UTC, signed Pubu Wear Team. It announces an investigation and requests an extension beyond 21 November 2026. It answers none of the three questions. At 07:19 UTC RFI-IRFOS declined the extension, restated the reproduction pointers and the three questions and kept the date.

2026-11-15 Notice six days before publication from security@rfi-irfos.com at 12:54 UTC to both addresses. The relay of yawellfit.com returned it for weiyuxiang@yawellfit.com at 12:55 UTC (550 5.7.25, no valid PTR record). No error for hezhiyuan55@gmail.com.

2026-11-17 No reply to the notice of 15 November 2026. The Play listing shows 1M+ downloads and the update date of 7 November 2025.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026. No message from the operator after 19 October 2026 is on record as of this date, and the extension request stays declined.

What Was Done Well

The package contains no advertising network SDK, no AD_ID permission and no billing library, so the app has no advertising surface. No hardcoded Firebase project keys or generic secret patterns were found beyond the two mapping keys of M1. The policy is specific on one point and says that call, SMS and address book data is used for display on the watch and is not stored, which is a claim that can be checked. The policy states that the Google Fit integration only writes data and does not read or store the user’s Google Fit data. The operator replied in writing and said it wishes to investigate, which is the start of the dialogue that the programme asks for.

Residual Risk & Recommendations

Open at the date of publication: all nine entries. The operator has not answered the three questions and has not named a controller. The build analysed is version 1.0.0.39 of November 2025, and the Play listing read on 17 November 2026 still shows the update date of 7 November 2025. No later build was analysed for this report, so it records the state of version 1.0.0.39.

Recommendations in order of effect. First, correct the Data Safety declaration to match the manifest and the policy (C2). Second, remove both cleartext allowances and pin first party hosts (C1). Third, name the controller with address, a Union representative and a Data Protection Officer (H1). Fourth, name the Chapter V mechanism and the recipients (H2). Fifth, gate the relay and health features behind recorded consent and complete a data protection impact assessment (H3, H4). Sixth, restrict the keys, set the backup flag and align the rating (M1 to M3).

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

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

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF PUBUWEAR-2026-R1.