Security & Privacy Disclosure, Final Report

Da Fit for Android (com.crrepa.band.dafit)

Privacy policy that routes erasure requests to another company, a global cleartext override, and PRC transfers on an ECG and cycle tracking app with more than 100 million installs.

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

Target	Shenzhen Moyoung Technology Co., Ltd. (Mo Young, CRRepa)
Versions Audited	2.5.0 / versionCode 300000 (Play update 2026-08-12, analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 2 High, 4 Medium, 5 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`9c4532ee8cdbce3fc71a4cd03a4582ba2437344e8de2707ff079d9f3381ba28a`

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 Findings 7

5.1 C1: Privacy policy contains leftovers from a competitor template and routes consent withdrawal and erasure to an unrelated company . . . 7

5.2 C2: Global cleartext traffic override and no network security configuration on an app that handles ECG and reproductive health data . . . 8

5.3 H1: PRC SDK endpoints and the operator's own statement of mainland China storage and onward transfer, with no Art. 46 safeguard named . . . 9

5.4 H2: Access to SMS, call log, contacts and calendar with SEND_SMS and CALL_PHONE capability that the policy does not describe . . . 10

5.5 H3: NotificationListenerService gives system-wide read access to notifications 11

5.6 H4: Special category health and reproductive health data with a locally computed pregnancy-likelihood field . . . 12

5.7 M1: Remote camera trigger from the paired band . . . 13

5.8 M2: Google Maps and AMap API keys hardcoded in the manifest . . . 13

5.9 M3: Alibaba feedback SDK FileProvider scoped to the whole external storage root . . . 14

5.10 M4: PEGI 3 rating, an age-14 threshold in the policy and no age gate . . . 14

5.11 M5: English and Chinese policies disagree, and an advertising template does not match the build . . . 15

6 Impact Analysis 15

7 The Complete Chain 16

8 Health & Reproductive Data Surface 16

9 Operator Platform & Supply-Chain Correlation 17

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 18

12 Regulatory & Legal Landscape 18

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 21

Executive Summary

Da Fit is the Android companion app of Bluetooth smartwatches and fitness bands, published on Google Play by Shenzhen Moyoung Technology Co., Ltd. with more than 100 million downloads. The app measures ECG, heart-rate variability, blood oxygen, skin temperature, sleep and stress, and contains a menstrual cycle module with a locally computed pregnancy-likelihood field. On 23 August 2026 RFI-IRFOS (ZVR 1015608684, GISA 39261441) disclosed eleven findings from a root level code analysis of version 2.5.0 under REF DAFIT-2026-R1.

The two most serious findings concern the operator's own documents and configuration. The Chinese privacy policy bundled in the app tells users who want to withdraw consent or request access to write to privacy@zepp.com, the inbox of Zepp Health Corporation, and the English policy linked from Google Play carries a link to Zepp's privacy page in its Business Partners clause (C1). The manifest sets android:usesCleartextTraffic to true for every host and the package has no network security configuration, while the Play listing says data is encrypted in transit (C2). The operator's own policy also states that data from its mainland operations is stored in China and may be transferred onward, and the English policy for EU users names no country and no safeguard (H1).

Further findings cover access to SMS, call log, contacts and notifications with send and call permissions that no policy text explains (H2, H3), the special category health data surface (H4), and five findings of lower rating on the camera trigger, two hardcoded map keys, a broad FileProvider, the PEGI 3 rating against the policy's age-14 rule, and the differences between the English and Chinese policies.

The operator received the notice at two working addresses and a third address that bounced. Two follow-ups with three written questions followed. As of 14 November 2026 no reply of any kind has arrived. The publication date is 21 November 2026, as stated in the notice and both follow-ups, and it does not depend on a reply. A final APK diff and a re-read of both policy pages before that date determine the state this report records.

Scope: Root level code analysis of the Google Play release 2.5.0 (versionCode 300000): decoded manifest and resources, dex string-pool extraction across both dex files, bundled assets and native library inventory. Public policy pages read by plain HTTP GET. No bytecode control-flow pass, no dynamic instrumentation, no traffic capture, no account, no backend call and no key test. Findings that depend on runtime behaviour are marked UNVERIFIED.

ID	Severity	Title
C1	HIGH	Privacy policy contains leftovers from a competitor template and routes consent withdrawal and erasure to an unrelated company
C2	HIGH	Global cleartext traffic override and no network security configuration on an app that handles ECG and reproductive health data
H1	MEDIUM	PRC SDK endpoints and the operator’s own statement of mainland China storage and onward transfer, with no Art. 46 safeguard named
H2	MEDIUM	Access to SMS, call log, contacts and calendar with SEND_SMS and CALL_PHONE capability that the policy does not describe
H3	MEDIUM	NotificationListenerService gives system-wide read access to notifications
H4	MEDIUM	Special category health and reproductive health data with a locally computed pregnancy-likelihood field
M1	LOW	Remote camera trigger from the paired band
M2	LOW	Google Maps and AMap API keys hardcoded in the manifest
M3	LOW	Alibaba feedback SDK FileProvider scoped to the whole external storage root
M4	LOW	PEGI 3 rating, an age-14 threshold in the policy and no age gate
M5	LOW	English and Chinese policies disagree, and an advertising template does not match the build

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

The Disclosed column shows the label used in the first notice. The This report column shows the rating after the CVSS v4.0 reassessment in this report.

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Zepp references are as recorded on 23 August 2026. Live page and bundled asset are re-checked in the final diff.
C2	CRITICAL	HIGH	No reply. Cleartext override recorded in version 2.5.0.
H1	HIGH	MEDIUM	No reply. Transfer statement and SDK end-points as recorded.
H2	HIGH	MEDIUM	No reply. Trigger for SEND_SMS is UNVER-IFIED.
H3	HIGH	MEDIUM	No reply. Scope of notification use is UN-VERIFIED.
H4	HIGH	MEDIUM	No reply. Consent capture for health screens is UNVERIFIED.
M1	MEDIUM	LOW	No reply. Origin of the camera command is UNVERIFIED.
M2	MEDIUM	LOW	No reply. Key restrictions are not testable without third-party tests.
M3	MEDIUM	LOW	No reply.
M4	MEDIUM	LOW	No reply.
M5	MEDIUM	LOW	No reply.

Subject & Operator Analysis

Da Fit is the companion app of Bluetooth Low Energy smartwatches and fitness bands. It is published on Google Play under the package com.crrepa.band.dafit by Shenzhen Moyoung Technology Co., Ltd. (Shenzhen Moyoung Technology Joint Stock Company in the Chinese Play Store entry), which also trades as Mo Young and CRRepa. The Play Store lists more than 100 million downloads, a 3.7 star average from about 402,000 reviews, the category Sports and a PEGI 3 rating.

The developer entry names an address at the Taihua Wutong Industrial Park in the Hangcheng subdistrict of Bao'an, Shenzhen, and the contact play-store@moyoung.com. The English policy gives the same industrial park, 8-9F Suite 15, Shenzhen 518126, and names Mo Young as the controller for users in the EEA, the United Kingdom and Switzerland. The package is signed by the operator itself with the certificate subject CN=moyoung, L=shenzhen, ST=shenzhen, C=cn.

No data protection officer and no Art. 27 representative appear in the binary, on the Play Store listing or in either policy. For a controller based in the People's Republic of China that names itself as controller for EEA users and processes Art. 9 data, the missing representative is a gap in its own right.

Architecture & Data Flow

Da Fit is a native Android and Java application with two dex files (about 10.4 MB), targetSdkVersion 33 and minSdkVersion 19. Native libraries are libBugly_Native.so (Tencent Bugly crash reporting), libRtkAesJni.so (a Realtek Bluetooth chipset AES bridge), libezip.so and libminilzo.so. The Bluetooth stack is the operator's own namespace com.crrepa.ble with chip classes for Goodix, Nordic and Realtek.

The backend is split over two live domain families in one binary: the legacy api.crrepa.com and api2.crrepa.com, and the current api.moyoung.com, app.moyoung.com and wr.moyoung.com. Third-party endpoints reach Tencent (android.bugly.qq.com, astat.bugly.qcloud.com, h.trace.qq.com) and Alibaba (feedback-api.aliyuncs.com, mpush-api.aliyun.com, g.tbcdn.cn, m.taobao.com). Mapping runs through Google Maps and the AutoNavi AMap platform.

Sensor data flows from the band over Bluetooth to the phone. From there the app can use the first-party backend and the SDK endpoints above. Which fields leave the phone toward which host is UNVERIFIED because the review decoded resources and extracted the dex string pool without a bytecode control-flow pass and without dynamic traffic capture.

Findings

C1: Privacy policy contains leftovers from a competitor template and routes consent withdrawal and erasure to an unrelated 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), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the defect sits in the clause that governs consent withdrawal and erasure for ECG and menstrual-cycle data of an app with more than 100 million installs, and it removes the only rights channel that the document offers. The Chinese policy bundled in the APK sends users who want to withdraw consent or request access to privacy@zepp.com, the inbox of Zepp Health Corporation. The English policy linked from Google Play links zepp.com/privacy-policy inside its Business Partners clause.

```
If you wish to request access to the personal data we hold, or believe information
   we hold about you is incorrect or incomplete, please contact us by letter or
   e-mail at: support@moyoung.com. Note that withdrawing consent may have legal
   consequences ... You may also submit a request by e-mailing privacy@zepp.com.
```

```
Business Partners. We may provide personal information to business partners to
   provide you with a product or service you have requested. We may also provide
   personal information to business partners with whom we jointly offer products or
   services.  [empty link text: one zero-width joiner]  ->
   https://www.zepp.com/privacy-policy
```

privacy@zepp.com and www.zepp.com/privacy-policy belong to Zepp Health Corporation (NYSE: ZEPP), a separate wearable company. Neither policy, the Google Play listing nor the binary discloses any relationship between Zepp and Shenzhen Moyoung Technology. The dex files contain no com.zepp or com.huami class and no zepp.com or huami.com endpoint. The paragraphs around the link, which speak of advertising partners, cross-device tracking and interest-based advertising, do not match the SDK inventory of this build, which contains no advertising SDK and no AD_ID permission.

Two readings are open and the root cause is UNVERIFIED. Either a real but undisclosed relationship with Zepp exists, which would be a separate Art. 13(1)(e) recipient disclosure failure. Or the policy for an app with Art. 9 health data was assembled from a competitor document without review. Both readings leave the same defect on the page: the document that tells users how to exercise their rights names an address the controller does not control.

Impact: A user in the EU who wants to withdraw consent for ECG or menstrual-cycle data, or to have it erased, is told in the bundled Chinese policy to write to another company. That request has no reason to reach the controller.

Fix: Remove every Zepp reference from both policy versions. Publish one policy per language that names Shenzhen Moyoung Technology as the only controller and a working privacy address. Answer whether any relationship with Zepp exists and list recipients under Art. 13(1)(e) if it does.

C2: Global cleartext traffic override and no network security configuration on an app that handles ECG and reproductive health data

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the setting applies to every request of an app that processes Art. 9 health and reproductive health data for more than 100 million installs, and a global opt-out of the platform default leaves no per-endpoint protection. AndroidManifest.xml sets android:usesCleartextTraffic="true" on the application element and the package contains no res/xml/network_security_config.xml. There is no certificate pinning anywhere in the resource tree.

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

With targetSdkVersion 33 Android blocks cleartext traffic by default. The app opts back in for every domain, present and future. A search of the decoded resources for a network security configuration returned nothing, so no per-domain rule and no pinning exists. The Google Play Data safety label states that data is encrypted in transit.

Which production endpoints actually use plain HTTP is UNVERIFIED because dynamic traffic analysis was not part of this review. The finding is the permission, which removes the platform safeguard for all traffic including health measurements and account data.

Impact: A person who logs an irregular ECG reading or a missed period relies on a connection that the app has told the operating system may run in plaintext on any network, such as public Wi-Fi.

Fix: Remove usesCleartextTraffic, add a network security configuration that denies cleartext by default, and pin the first-party API hosts. Correct the Data safety declaration if any endpoint stays on HTTP.

H1: PRC SDK endpoints and the operator's own statement of mainland China storage and onward transfer, with no Art. 46 safeguard named

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B)

The dex files contain compiled Tencent Bugly and Alibaba EMAS code with live endpoints. The bundled Chinese policy states that data collected in mainland operations is stored in mainland data centres and may be transferred to other countries. The English policy for EU users names no country and no mechanism.

```
Lcom/tencent/bugly/...                          77 hits in classes2.dex
Lcom/alibaba/mtl/...                            67 hits in classes.dex, 10 in
   classes2.dex
Lcom/alibaba/sdk/android/feedback/...           Alibaba feedback SDK with WindVane
   webview bridge

android.bugly.qq.com/rqd/async   astat.bugly.qcloud.com/rqd/async
   h.trace.qq.com/kv
feedback-api.aliyuncs.com   mpush-api.aliyun.com/v2.0/a/audid/req/
g.tbcdn.cn/mtb/lib-windvane/1.2.4/bridge.js   m.taobao.com
com.amap.api.v2.apikey = 15eb52b97b01661136e6450b460dff7c
```

The Chinese policy states in its section on transfers outside the user's jurisdiction that personal information collected and generated in mainland operations is stored in data centres in mainland China and may be transferred onward to other data centres, countries or regions where applicable law allows. This is the controller's own written statement. The English policy carries a generic International Data Transfers clause without a destination or a safeguard.

The Chinese policy also labels device identifier, firmware version and approximate location as "non-personal data". A device identifier combined with approximate location is personal data under Art. 4(1) whatever the internal label says.

What each SDK receives from EU devices (crash reports, identifiers, location) is UNVERIFIED. The finding stands on the compiled endpoints and the operator's own transfer statement. No standard contractual clauses, adequacy decision or other Art. 46 mechanism is named in either policy.

Impact: EU users read a policy that does not say where their data goes, while users in China are told that their data is stored in China and may move on to other countries.

Fix: Name the countries and the Art. 46 mechanism in the EU policy, document a transfer impact assessment, and state which data each SDK receives. Remove the "non-personal data" label from location and device identifiers.

H2: Access to SMS, call log, contacts and calendar with SEND_SMS and CALL_PHONE capability that the policy does not describe

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)

The manifest declares READ_SMS, SEND_SMS, READ_CALL_LOG, ANSWER_PHONE_CALLS, CALL_PHONE, READ_CONTACTS and READ_CALENDAR. A live code path reaches SmsManager.sendTextMessage. Both policy versions describe only the display of incoming calls and messages on the band.

The bundled policy says Da Fit obtains call, SMS and contact data for display on the band or watch and does not store it. Neither policy mentions SEND_SMS, CALL_PHONE or ANSWER_PHONE_CALLS. No UI string in strings.xml explains an outbound function such as an emergency-contact message. What triggers sendTextMessage is UNVERIFIED and open for the dynamic phase.

The data concerns people who never installed the app and saw no consent screen: callers, senders and every entry in the address book. Whether any of it reaches api.moyoung.com or api.crrepa.com before or alongside the Bluetooth push to the band cannot be settled from the binary. The operator's statement that it does not store this data is a specific commitment that this review neither confirms nor contradicts.

Impact: The contacts, callers and message senders of every Da Fit user pass through an app that holds the permissions to send messages and place calls, and the policy does not say why.

Fix: Describe every use of SEND_SMS, CALL_PHONE and ANSWER_PHONE_CALLS in the policy or remove the permissions. State in writing that call, SMS and contact data stay on the phone and the band.

H3: NotificationListenerService gives system-wide read access to notifications

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)

NotificationCollectorService is declared with the BIND_NOTIFICATION_LISTENER_SERVICE permission and can read sender, source app and text of every notification on the phone.

```
<service android:exported="true" android:label="@string/app_name"
android:name="com.crrepa.band.my.notify.service.NotificationCollectorService"
         android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action
           android:name="android.service.notification.NotificationListenerService"/>
    </intent-filter>
</service>
```

Only the operating system can bind to the service, which closes the component-exposure route. The data-access capability remains. A listener of this kind can see who writes to the user, how often, through which app and when contact stops, without storing message content. Whether parsed notification content stays on the Bluetooth link or reaches Bugly, EMAS or a first-party backend is UNVERIFIED.

Impact: Every message notification from family, a partner or a doctor passes the listener, and the privacy policy describes only calls and SMS.

Fix: Limit the listener to the notification categories the band displays, document the scope in the policy, and state that notification content is not logged or sent to any SDK.

H4: Special category health and reproductive health data with a locally computed pregnancy-likelihood field

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.8 (CVSS-B)

Activities for ECG, heart-rate variability, blood oxygen, skin temperature, sleep, stress and a menstrual calendar are declared. Dex field names show a computed pregnancy-chance output, and the app requests the Google Fit reproductive health read and write scopes.

```
BandEcgMesaureActivity   BandEcgResultActivity   BandEcgStatisticsActivity   (ECG)
BandHrvStatisticsActivity
   (heart-rate variability)
BandTimingBloodOxygenActivity   BandTimingBloodOxygenHistoryActivity
   (SpO2)
BandOnceTempStatisticsActivity
   (skin temperature)
BandSleepHistoryActivity   BandStressHistoryActivity
PeriodChooceActivity   PhysiologicalCalendarActivity
   (menstrual period and calendar)

color_pregnancy_chance   rlPregnancyChance   tvPregnancyChance
DEFAULT_MENSTRUAL_PERIOD   FIELD_MENSTRUAL_FLOW   FIELD_OVULATION_TEST_RESULT
getLastMenstrualDate   getMenstrualPeriod   getOvulation
OAuth scopes: fitness.reproductive_health.read, fitness.reproductive_health.write
```

The bundled policy states that cycle length, interval, physical condition and mood during menstruation are collected and that the app may recommend training courses from them. A derived pregnancy-likelihood score can be more sensitive than any raw value behind it. The English policy claims explicit consent obtained separately when the user takes actions that lead to data collection. This review located no in-app consent string for the ECG or period screens, which is UNVERIFIED and is not asserted as absent.

Impact: Women who track their cycle, and people who measure an ECG after a cardiac event, put the most intimate part of their health into an app whose transport and transfer position is described in C2 and H1.

Fix: Document the Art. 9(2) condition per feature, run and publish a data protection impact assessment under Art. 35, and show an explicit consent screen before the first cycle or ECG entry.

M1: Remote camera trigger from the paired band

LOW, CVSS v4.0 AV:A/AC:H/AT:N/PR:L/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B)

BandTakePhotoEvent, onTakePhoto and a takePhoto routine are present. The operator's policy describes the feature as Bluetooth photo control for supported devices.

The feature is disclosed and named, which keeps the rating low. Whether the command can originate only from the physically paired band or also from a backend or remote configuration path is UNVERIFIED and is a fair question for the operator. A camera triggered from the wrist captures whoever stands in front of the phone, not necessarily the account holder.

Impact: Bystanders in front of a phone whose camera is released from a wrist can be photographed without handling the phone.

Fix: Confirm in writing that only the paired band can release the shutter and that no network path arms the feature.

M2: Google Maps and AMap API keys hardcoded in the manifest

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 2.3 (CVSS-B)

Both keys are readable in AndroidManifest.xml with standard tooling. No key was tested or used.

```
<meta-data android:name="com.google.android.geo.API_KEY"
   android:value="AIzaSyA3LO8ldAccXfa5MzlofRkh4vO2-lnpiH0"/>
<meta-data android:name="com.amap.api.v2.apikey"
   android:value="15eb52b97b01661136e6450b460dff7c"/>
```

Mobile map keys are expected to sit in the manifest. Their protection depends on platform-side restrictions to the package name and signing certificate, which cannot be checked without testing a third-party service and was not done. The AMap key ties the app to the Chinese mapping and positioning backend discussed in H1. The finding concerns quota abuse and billing exposure for the operator, not user data.

Impact: The operator carries the cost and availability risk if the keys are not restricted, and users lose map features if quota is exhausted.

Fix: Restrict both keys to the package name and signing certificate SHA-256 and rotate them after restriction.

M3: Alibaba feedback SDK FileProvider scoped to the whole external storage root

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:L/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B)

res/xml/alifb_provider_paths.xml declares an external-path with path "." for the alifb_ fileprovider, which grants URI permissions.

```
<paths xmlns:android="http://schemas.android.com/apk/res/android">
    <external-path name="external_files" path="." />
</paths>
```

The scope is wider than a feedback attachment needs. The app's own file_paths.xml is narrower, so the breadth comes from the unmodified SDK default. Exploitation needs a second app and a user action that grants a URI, which is why the score is low.

Impact: A URI grant made for a feedback attachment could expose more files on shared storage than the user intended.

Fix: Replace the path with the dedicated feedback directory or remove the provider if the SDK feedback screen is not used.

M4: PEGI 3 rating, an age-14 threshold in the policy 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)

Google Play lists the app as PEGI 3 and Everyone. The bundled policy requires parental consent for children under 14. No date-of-birth field, age screen or parental gate was found in the resources.

```
If your child is a minor under the age of 14, before your child uses our products
   and services you, as parent or guardian, must expressly consent to Moyoung
   collecting your child's personal information under this policy.
```

The only place the number 14 appears in the evidence set is this advisory paragraph. The feature set (SMS and call forwarding, ECG, cycle and pregnancy-likelihood tracking, background location) points to adult users, so the rating and the actual audience diverge.

Impact: A child who installs the app because it is rated for everyone meets health tracking and a consent promise that nothing enforces.

Fix: Align the content rating with the features, add an age screen and route under-age users to a parental consent step, or remove the age-14 paragraph.

M5: English and Chinese policies disagree, and an advertising template does not match the build

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)

The Chinese policy names AutoNavi, Google Map, Tencent Bugly and Huawei Push. The English policy for EU users contains none of the words Bugly, AutoNavi, Huawei or China. No Huawei class exists in either dex file.

EU users receive less specific information about who processes their data than users of the same app in China. The English advertising paragraphs (advertising partners, cross-device tracking, interest-based advertising) describe SDKs that the build does not contain. The Huawei SDK named in the Chinese policy is absent from the compiled code, which mirrors the stale template pattern seen in other policies of this device class. Whether the discrepancy resolves in either direction is UNVERIFIED. The plain-language accuracy problem exists in both.

Impact: A user who relies on the English policy cannot learn that crash and analytics data go to Tencent and Alibaba infrastructure.

Fix: Publish one policy text per language with the same recipients, remove the advertising template and name the SDKs that the build contains.

Impact Analysis

Da Fit has more than 100 million installs, and the people it serves are named by its feature set. People with a cardiac concern measure ECG and heart-rate variability. People who track their cycle, plan or avoid a pregnancy enter menstrual flow, ovulation tests and mood, and the app computes a pregnancy-likelihood display from them. Everyone who forwards calls and messages to a band hands the contact details of third parties to the app.

Three groups carry the main consequences. Women who track their cycle depend on a policy whose consent withdrawal clause points at another company (C1) and on a transport setting that allows plaintext (C2). Callers, senders and contacts who never installed Da Fit are processed without any notice (H2, H3). Parents who read PEGI 3 as a signal for all ages find that the policy’s own age-14 rule has no gate (M4).

The harm demonstrated by this review is a harm of opacity and of default configuration. Users cannot find out who receives their data, where it goes or how to withdraw consent. Observed data exposure on the wire is not claimed, because no traffic was captured.

The Complete Chain

Step 1, install: a user finds an app with 100 million downloads and a PEGI 3 rating, and the Data safety label says data is encrypted in transit (C2, M4).

Step 2, permissions: the user grants Bluetooth, location, contacts, SMS, call log and notification access so that the band can show calls and messages (H2, H3).

Step 3, health features: the user records ECG, oxygen, sleep, stress and cycle data, and the app computes a pregnancy-likelihood field (H4).

Step 4, transmission: the manifest allows plaintext for every host, and the binary carries Tencent and Alibaba endpoints. The operator's own Chinese policy states mainland storage and onward transfer (C2, H1).

Step 5, the user tries to act: the Chinese policy sends consent withdrawal to privacy@zepp.com and the English policy links a competitor's privacy page. The address privacy@moyoung.com does not exist on the operator's mail server (C1, M5).

Health & Reproductive Data Surface

The table lists the data categories that the manifest and dex string pool show, with the Art. 9 relevance of each. Rows marked UNVERIFIED depend on runtime behaviour.

Feature	Evidence	Data category	Open point
ECG	BandEcgMesaureActivity, BandEcgResultActivity	Health, Art. 9	Consent screen UNVERIFIED
HRV, SpO2, skin temperature	BandHrvStatistics, BandTimingBloodOxygen, BandOnceTemp	Health, Art. 9	Destination UNVERIFIED
Sleep and stress	BandSleepHistory, BandStressHistory	Health, Art. 9	Destination UNVERIFIED
Menstrual cycle	PeriodChooceActivity, PhysiologicalCalendar	Reproductive health, Art. 9	Google Fit scopes requested
Pregnancy likelihood	tvPregnancyChance, rlPregnancyChance	Inference on reproductive health, Art. 9	Computed locally per dex names

Operator Platform & Supply-Chain Correlation

Da Fit does not share the fingerprints of the Bluetrum SDK cluster seen in other wearable apps. It is a self-operated platform with its own Bluetooth namespace and signing certificate, listed here so that other apps of the same operator can be matched.

```
Signing cert SHA-256
   37:AE:1A:B5:53:08:19:42:0A:C6:14:9D:66:EC:B0:16:7A:81:E1:FD:5B:D9:CD:06:C7:FA:17:5C
    :9E:11:61:3C
Signing cert DN        CN=moyoung, L=shenzhen, ST=shenzhen, C=cn
BLE SDK namespace      com.crrepa.ble.* (CRPScanRecordInfo with Goodix, Nordic,
   Realtek and McuPlatform classes)
Native library         libRtkAesJni.so (Realtek), no libabpartool.so, no Bluetrum
   library
Backend domains        api.crrepa.com, api2.crrepa.com, api.moyoung.com,
   app.moyoung.com, wr.moyoung.com
```

Manufacturer-specific BLE company IDs and GATT UUID constants were not extracted at this depth.

Data Protection: Article by Article

Article 4(1), personal data: engaged by H1. Device identifier with approximate location is personal data and the operator's non-personal label does not change that.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2 and M5. The policy that governs rights names an unrelated company and the two policy versions disagree.

Article 5(1)(c), data minimisation: engaged by H2 and H3. Permissions for sending messages and placing calls go beyond the described display function.

Article 5(1)(f), integrity and confidentiality: engaged by C2 and H4.

Article 6(1) and Article 14: engaged by H2 and H3 for third-party contact and message data. The app has no way to inform a caller or sender.

Article 8, conditions for a child's consent: engaged by M4.

Article 9, special categories: engaged by H4. ECG, oxygen, temperature, sleep, stress and cycle data are health data, and the pregnancy-likelihood field is derived health data. An Art. 9(2) condition is not documented in the evidence.

Article 12(1) and (2), Article 13(1)(a) and (e), Article 17: engaged by C1 and M5. Facilitating rights requires a working address of the controller.

Article 25, data protection by design and by default: engaged by C2, H3, M1, M2, M3 and M4.

Article 27, EU representative: engaged. None found.

Article 32(1)(a) and (b), security of processing: engaged by C2, M2 and M3.

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

Articles 44 and 46, transfers: engaged by H1. The Chinese policy states mainland storage and onward transfer and no safeguard is named in either version.

Platform Accountability & DSA

The Google Play Data safety section of Da Fit shows, on one page, that the app may share location, app information and performance data and device or other identifiers with third parties for analytics and app functionality, and next to it the badge that the developer says the app collects no user data. It states that data is encrypted in transit and that data cannot be deleted. The listing also shows a Contains ads badge although the build contains no advertising SDK and no AD_ID permission. The manifest permits cleartext traffic (C2) and the policy offers erasure (C1), so at least three of these statements conflict with the binary or with each other.

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

Regulatory & Legal Landscape

Shenzhen Moyoung Technology Co., Ltd. offers the app to users in the Union, publishes an English policy that addresses EEA users and so falls under Art. 3(2) of the GDPR. 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 in which users are affected is competent under Art. 55. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the notice in copy.

Infringements of the principles in Art. 5 and 9, of the data subject rights in Art. 12 to 22 and of the transfer rules in Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27, 32 and 35 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82.

Within this review wave Da Fit shows the broadest special category health surface, because it combines ECG, heart-rate variability, oxygen, temperature, sleep, stress and a cycle module with a derived pregnancy-likelihood field. Its policy text carries the Zepp leftovers described in C1.

Indicators of Compromise & Reproducible Evidence

Every point is reproducible from the public Google Play build of 12 August 2026 and public web pages read by plain HTTP GET.

Package	com.crrepa.band.dafit
Version	2.5.0-124-g92d6b1c68-dirty (versionCode 300000), Play Store update 12 Aug 2026
APK size	19,978,388 bytes
APK SHA-256	9c4532ee8cdbce3fc71a4cd03a4582ba2437344e8de2707ff079d9f3381ba28a
Signing cert	37:AE:1A:B5:53:08:19:42:0A:C6:14:9D:66:EC:B0:16:7A:81:E1:FD:5B:D9:CD:06:C7:FA:17:5C:9E:11:61:3C
minSdk / target	19 / 33
Obtained from	APKPure mirror, package name, versionName, versionCode and publication date matched to the live Play listing

com.google.android.geo.API_KEY	AIzaSyA3LO8ldAccXfa5MzlofRkh4vO2-lnpiH0
com.amap.api.v2.apikey	15eb52b97b01661136e6450b460dff7c
android.bugly.qq.com/rqd/async	astat.bugly.qcloud.com/rqd/async
h.trace.qq.com/kv	
feedback-api.aliyuncs.com	mpush-api.aliyun.com/v2.0/a/audid/req/
api.crrepa.com	api2.crrepa.com
api.moyoung.com	app.moyoung.com
wr.moyoung.com	

Bundled (Chinese)	assets/Da_Fit_Privacy.html
Live (English)	https://cdn.moyoung.com/HTML/dafit_law_and_privacy_en_0130.html (HTTP 200, checked 23 Aug 2026)
Zepp references	privacy@zepp.com (bundled), https://www.zepp.com/privacy-policy (live, empty link text)

Disclosure Timeline & Outcome

2026-08-23 First notice, REF DAFIT-2026-R1, stamped 23 August 2026 and sent at 01:54 Vienna time to play-store@moyoung.com, support@moyoung.com and privacy@moyoung.com, with the Austrian DSB and the EDPS in copy. The message states the embargo end as 21 November 2026. privacy@moyoung.com bounced within seconds with 554, address does not exist.

2026-09-12 First follow-up to play-store@moyoung.com and support@moyoung.com. It restated C1 and C2, named the Tencent and Alibaba transfers and the SEND_SMS and CALL_PHONE paths, and set a response date of 26 September 2026 for three questions. These ask whether a relationship with Zepp exists, on what basis the Data safety label states encryption in transit, and which Chapter V safeguards cover the transfers.

2026-10-17 Second follow-up from security@rfi-irfos.com, 35 days before publication, with the three questions unchanged and the publication date repeated as 21 November 2026.

2026-11-14 No reply from any address of the operator. A search of the mailbox for inbound mail from moyoung.com and crrepa.com returned nothing.

2026-11-21 Publication date as delivered to the operator in the notice and both follow-ups.

What Was Done Well

allowBackup is set to false, which blocks adb backup extraction of the private data directory. The build contains no advertising or monetisation SDK and requests no AD_ID permission, a much smaller third-party surface than other apps of the class. No Firebase keys and no generic secret patterns appeared beyond the two map keys in M2. The operator’s bundled policy makes a falsifiable commitment, that call, SMS and contact data are not stored, and this review found no binary evidence against it. The English policy names Mo Young as controller for EEA, United Kingdom and Swiss users and states the right to complain to a supervisory authority.

Residual Risk & Recommendations

Open at the date of publication: all eleven findings. The operator has not replied, and the build analysed is version 2.5.0 of 12 August 2026. A final APK diff and a re-read of both policy pages before 21 November 2026 determine the state that the published report records. Silent fixes are recorded as such.

Recommendations in order of effect. First, correct the policy: remove the Zepp references, publish one policy with the same recipients in both languages, name the SDKs and the transfer safeguard (C1, H1, M5). Second, remove the global cleartext override and add a network security configuration with pinning for first-party hosts, then correct the Data safety label (C2). Third, document every use of SEND_SMS, CALL_PHONE and notification access and cut permissions that no feature needs (H2, H3). Fourth, publish a data protection impact assessment for the health and cycle features and show an explicit consent step (H4). Fifth, appoint an Art. 27 representative, add an age gate, restrict the map keys and narrow the feedback FileProvider (M1 to M4).

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria RFI-IRFOS research focus institute · ZVR 1015608684 · GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) from the FIRST lookup tables 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 DAFIT-2026-R1.