Security & Privacy Disclosure, Final Report

RDFit for Android (com.rd.tengfei.bdnotification)

A policy that names four SDKs and a package that holds at least twenty, cleartext allowed for every host against a policy that says all data is encrypted, and no reply since the notice.

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

Target	Shenzhen Runde Intelligent Communication Technology Co., Ltd. (RDFit)
Versions Audited	4.1.4 / versionCode 436 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	7: 3 High, 3 Medium, 1 Info (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`cc33b28c131410ba00a04aa794b8cc591251f8b4d43606c0f61ddf50b64b6b1b`

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 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 5

6 Findings 6

6.1 C1: Cleartext traffic and user installed certificates are allowed for every host while the bundled privacy policy says all information is encrypted 6

6.2 C2: The policy names four third party SDKs and the package contains at least twenty processors, among them advertising SDKs with a plugin download capability 7

6.3 H1: A Baidu DuerOS for Kids AI voice chat integration is wired into the package, the policy names no AI voice processor, and the app is rated PEGI 3 with no age gate 9

6.4 H2: The package queries the device identifier services of at least five phone makers, a set built to survive a reset of the Google advertising ID 10

6.5 H3: A development Azure hostname for a GPT feature ships in the production package 10

6.6 H4: The local data model holds ECG, blood pressure, blood oxygen and blood sugar records, with no consent platform and no impact assessment on record 11

6.7 M1: No consent management platform exists anywhere in the package, and the ad and analytics SDKs start without any recorded decision 12

7 Impact Analysis 12

8 The Complete Chain 13

9 Platform Fingerprint and Correlation Keys 13

10 Data Protection: Article by Article 14

11 Platform Accountability & DSA 14

12 Regulatory & Legal Landscape 15

13 Indicators of Compromise & Reproducible Evidence 16

14 Disclosure Timeline & Outcome 17

15 What Was Done Well 17

16 Residual Risk & Recommendations 17

Executive Summary

RDFit is the companion app for the IW7 MAX and PS9Ultra2 smart watches with more than 5 million downloads on Google Play. The publisher is Shenzhen Runde Intelligent Communication Technology Co., Ltd. The listing shows PEGI 3 and a Data Safety card that says no data is shared with third parties and that data is not encrypted. On 23 August 2026 RFI-IRFOS sent a notice with REF RDFIT-2026-R1 to service@xinsudian.com, the only contact address found, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 4.1.4 shows that the app permits cleartext traffic and user installed certificates for every host, while its own bundled privacy policy says that all information is encrypted (C1). The policy names four third party SDKs and the package contains at least twenty processors, among them advertising SDKs of ByteDance, Baidu, Tencent, Kuaishou and JD.com, and an advertising SDK with endpoints that serve plugin bundles for loading after installation (C2). The package holds a wired Baidu DuerOS for Kids voice chat integration (H1), identifier services of five phone makers that survive an advertising ID reset (H2), and a local data model for ECG, blood pressure, blood oxygen and blood sugar (H4). It contains no consent management platform (M1) and a development hostname for a GPT feature (H3).

A reassessment by CVSS v4.0 band puts three findings at High, three at Medium and 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. Two more labels move down for the same reason and one becomes informational. C2 and H4 stay High through stated blast-radius escalations. 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. No bounce was received. This report is published on the embargo date of 21 November 2026 and records the state of the correspondence on 21 November 2026.

Scope: Root level code analysis of the Google Play release 4.1.4 (versionCode 436), an APK of 191,063,310 bytes with ten classes*.dex files (about 107.6 MB combined) and 62 native libraries for arm64-v8a. The package was obtained from the APKPure mirror and checked against the title, developer name, version, PEGI rating and size on the live Google Play listing. Work done: a resources only decode with apktool (no source decode), the manifest, network security configuration, local schema and bundled policy, and a string pass across all ten dex files for class namespaces, endpoints and keys. The live Google Play listing was 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 and user installed certificates are allowed for every host while the bundled privacy policy says all information is encrypted
C2	HIGH	The policy names four third party SDKs and the package contains at least twenty processors, among them advertising SDKs with a plugin download capability
H1	MEDIUM	A Baidu DuerOS for Kids AI voice chat integration is wired into the package, the policy names no AI voice processor, and the app is rated PEGI 3 with no age gate
H2	MEDIUM	The package queries the device identifier services of at least five phone makers, a set built to survive a reset of the Google advertising ID
H3	INFO	A development Azure hostname for a GPT feature ships in the production package
H4	HIGH	The local data model holds ECG, blood pressure, blood oxygen and blood sugar records, with no consent platform and no impact assessment on record
M1	MEDIUM	No consent management platform exists anywhere in the package, and the ad and analytics SDKs start without any recorded decision

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Plain HTTP use not observed.
C2	CRITICAL	HIGH	No reply. Presence proven, transmission and plugin execution not observed.
H1	HIGH	MEDIUM	No reply. Wiring proven, user facing status not determined.
H2	HIGH	MEDIUM	No reply. Class wiring proven, runtime use not observed.
H3	HIGH	INFO	No reply. Hygiene observation, host not contacted.
H4	HIGH	HIGH	No reply. Data model proven, storage and transmission not observed.
M1	MEDIUM	MEDIUM	No reply. Absence of a consent platform proven, call order not shown.

The findings file of 23 August 2026 labels C1 and C2 as Critical, H1 to H4 as High and M1 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. H3 is a hygiene observation without a score.

Subject & Operator Analysis

The publisher is Shenzhen Runde Intelligent Communication Technology Co., Ltd., A301, Sogood Science Park Complex Building, Sanwei Community, Hangcheng Street, Baoan District, Shenzhen, People's Republic of China. The only contact address in the package and the policy is service@xinsudian.com. The operator uses the domains rundefit.com and xinsudian.com. The Play page shows more than 5 million downloads, 3.6 stars from 34.2K reviews and the rating PEGI 3 with the label Users Interact.

The signing certificate is self-signed by the operator with the DN CN=rdtf, OU=runde, O=runde, L=shenzhen, ST=guangdong, C=86. The SHA-1 of the certificate matches the signature that the APKPure page shows for this build. No Data Protection Officer was found and the policy and package name no representative in the Union. The Austrian Datenschutzbehörde receives the notice in copy and can receive complaints directly.

Architecture & Data Flow

RDFit is a native Android app with ten classes*.dex files and 62 native libraries. The BLE protocol stack is the operator's own, com.rd.rdmtk.*, built mainly for MediaTek chips, with the Realsil SDK (com.realsil.sdk.bbpro.*) and nine Zhuhai Jieli libraries (libjl_*.so, among them libjl_ota_auth.so) as secondary vendor SDKs. The app also declares 61 permissions and 20 exported components.

The app talks to the watch over Bluetooth Low Energy and stores health, sport and location records in a local LitePal database (C1, H4). The policy states that data is stored on an Alibaba Cloud server. The dex strings name the processors of C2, a Baidu voice chat platform and its own backend host api.lizheng.design (H1), an AIGC gateway on swapi.yueqizhixiang.com and a development Azure host (H3). No data flow was observed.

Engagement Summary

The notice REF RDFIT-2026-R1 was sent on 23 August 2026 at 07:17 UTC from rfi.irfos@gmail.com to service@xinsudian.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried the findings, a statement of what the app does well and three questions. A follow-up of 12 September 2026 at 16:45 UTC restated the findings and the three questions with an answer date of 19 September 2026. A second follow-up of 17 October 2026 at 19:08 UTC came from security@rfi-irfos.com under the subject 35 days to publication: RDFit. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: Cleartext traffic and user installed certificates are allowed for every host while the bundled privacy policy says all information is 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, trust anchors for both user and system certificates, no domain-config block and no pin-set. The application element of AndroidManifest.xml also sets android:usesCleartextTraffic="true". The app targets API level 35, where cleartext HTTP is refused by default. The policy bundled inside the package (assets/privacy_policy_en.htm, Updated: June 7, 2023) says under Data Security: All information that you provide to us is encrypted. The local database schema in assets/litepal.xml (LitePal, dbname RDFit, schema version 29) defines tables for heart rate, blood oxygen, blood pressure, temperature, ECG, breathing, blood sugar, sleep, steps, sport and GPS, WiFi and cell tower location records. The app also holds SEND_SMS, READ_SMS, READ_CONTACTS, READ_CALL_LOG, ANSWER_PHONE_CALLS, ACCESS_BACKGROUND_LOCATION and CAMERA. A configuration that permits plain HTTP for every host cannot back a blanket statement that all information is encrypted. Whether any endpoint is called over plain HTTP was not observed and is UNVERIFIED. The live Data Safety card of 23 August 2026 says that data is not encrypted, so the card and the configuration agree.

```
<!-- res/xml/network_security_config.xml -->
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="user" />
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>

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

```
Policy (assets/privacy_policy_en.htm), Data Security: "All information that you
    provide to us is encrypted."

assets/litepal.xml tables: HeartRateBean, BOBean (blood oxygen), BPBean (blood
    pressure), TempBean, EcgBean,
BreatheBean, BSBean (blood sugar), SleepBean, DaySleepBean, SleepReportData, StepBean,
     SportBean,
GpsPartBean, WifiPartBean, GsmPartBean (cell tower location)
```

Impact: More than 5 million installers use an app that shows heart, blood pressure, blood oxygen, ECG and blood sugar values and reads their messages and calls. Its policy tells them that all information is encrypted, and its network settings allow plain HTTP and the interception of traffic by user installed certificates.

Fix: Remove the cleartext allowance and the user certificate trust, add a domain based network security configuration with pinned first party hosts and correct the policy.

C2: The policy names four third party SDKs and the package contains at least twenty processors, among them advertising SDKs with a plugin download capability

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 policy section on embedded third party SDKs lists four entries: Amap, Google Login, Facebook Login and Tencent Bugly. The class namespaces and hostnames in the table below are present in the dex files and the manifest. The R1 pass counts at least twenty processors, and sixteen of them are not named in the policy. The Kuaishou advertising SDK endpoints p1-lm.adkwai.com and p2-lm.adkwai.com serve versioned plugin bundles by name (adLive, adInnerEc, obiwan, tachikoma, an exception handler module and an appStatus module), and the endpoint URLs and plugin loader class references are compiled into the app. That is a capability to fetch and load code after installation. Whether any plugin was downloaded or run on a device was not observed and is UNVERIFIED. Whether data goes to any of the listed processors was not observed. The policy names no transfer mechanism for any of them. iFlytek, in the table, is a vendor that the R1 file describes as on the US Department of Commerce Entity List since October 2019. That statement was not re-checked in this evidence base. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the gap between four named and at least twenty present processors is the largest in this programme, the app has more than 5 million installs, the processors include advertising and device identifier SDKs and a code fetching capability, and the app holds health, SMS and location data.

Processor	Evidence in the package	In policy
Alibaba Amap	com.amap.api.*, key e5ec21a71a842186a37a8ae85bc911a0, libAMapSDK_NAVI_v9_8_1.so	yes
Alibaba AliAgent	com.alibaba.aliagentsdk.* (IAliBt, IAliBtSender, IAliAgentDev)	no
Alibaba Cloud OSS	oss.aliyuncs.com, oss-cn-hangzhou.aliyuncs.com	storage named, recipient not
Google Login	accounts.google.com	yes
Facebook Login	com.facebook.sdk.*, facebook_app_id, facebook_client_token	yes
Tencent Bugly	libBugly_Native.so, android.bugly.qq.com, astat.bugly.qcloud.com	yes
ByteDance Pangle (ads)	com.bytedance.sdk.*, com.byazt.*, libpanglearmor.so, libpangleflipped.so, libtt_ugen_layout.so, api-access.pangolin-sdk-toutiao.com, apps.oceanengine.com	no
ByteDance live plugin	com.bytedance.android.openliveplugin.*, DouyinAuthorizeActivityProxy, process :bytelive	no

Processor	Evidence in the package	In policy
ByteDance analytics	applog.snssdk.com, apmplus.volces.com	no
Baidu Mobads	com.baidu.mobads.sdk.*, com.baidu.oauth.*, union.baidu.com	no
Baidu DuerOS for Kids	see H1	no
Tencent GDT	com.qq.e.*, assets/gdt_plugin/gdtadv2.jar, h.trace.qq.com	no
Kuaishou ads	com.kwad.sdk.*, open.e.kuaishou.com, p1-lm.adkwai.com, static.yximgs.com	no
JD.com ads	com.jd.ad.*	no
Huawei HMS	com.huawei.hms.*, com.huawei.hwid.*	no
Microsoft Azure Speech	libMicrosoft.CognitiveServices.Speech.* (8 files), cognitiveservices.azure.com, login.microsoftonline.com	no
Vosk speech engine	libvosk.so	no
iFlytek speech	iat-api.xfyun.cn, iat-niche-api.xfyun.cn, tts-api.xfyun.cn	no
AIGC gateway, operator not identified	swapi.yueqizhixiang.com (/llm/gpt, /llm/txt2imgv2, /dmp/llm/getAzureConfig, /dmp/mvoice/pro_api)	no
China Mobile CMPassport	msg.cmpassport.com, nisportal.10010.com	no
yfanads	com.yfanads.android.*, api.yfanads.com, log.yfanads.com	no
OAID identifiers	see H2	no

Impact: More than 5 million installers are told about four processors while the package carries at least twenty, among them advertising and analytics vendors that handle device identifiers, and an SDK that can fetch code after the install.

Fix: List every processor with purpose and country in the policy, state the Chapter V mechanism for each, and remove SDKs that are not needed. Disable the plugin download of the advertising SDK.

H1: A Baidu DuerOS for Kids AI voice chat integration is wired into the package, the policy names no AI voice processor, and the app is rated PEGI 3 with no age gate

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 dex string pool holds the endpoints below, a DuerOS device interface schema (ai.dueros.device_interface.alerts, speaker_controller, video_player, voice_output and voice_input, the event ListenStarted and the audio format AUDIO_L16_RATE_16000_CHANNELS_1) and the tables AIChatBean and AsrTranslateBean appear in assets/litepal.xml. The wiring shows that the code is not an unused stub. The name duer-kids is Baidu's own name for its children's smartwatch assistant line. Its presence shows that the platform underneath the app is built on or shares a backend with that line. Whether the IW7 MAX or PS9Ultra2 interface shows the feature to users, or whether it is dormant template code, was not determined and is UNVERIFIED. The bundled policy says the service is intended for users 16 years or older, and the Play rating is PEGI 3. The resources show no age gate.

```
https://duer-kids.baidu.com/botwatch/api/operation/aigc/stream/dcschat
/api/client/dcschat/aiSign
/api/dcschat/open/cueWord
/api/dcschat/open/speechToken
/api/dcschat/open/token
https://api.lizheng.design/service/botwatch/api/errorReport
https://api.lizheng.design/service/botwatch/api/queryDevcie
https://api.lizheng.design/service/botwatch/api/thirdReq
https://api.lizheng.design/service/sdkConfigure/synTime
```

Impact: If the feature is live on a device that a child wears, the child's voice is processed by an AI pipeline that neither the consent screen nor the policy names.

Fix: Name the voice assistant processor and the age group, add an age gate and complete a data protection impact assessment for the voice feature, or remove the code.

H2: The package queries the device identifier services of at least five phone makers, a set built to survive a reset of the Google advertising ID

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 dex strings hold the references below. They cover the generic MSA unified identifier service action, Samsung, Honor, OPPO or Heytap and vivo identifier services and the Kuaishou OAID helper classes. OAID is a device identifier that stays available when a user resets or limits the Google advertising ID. The references are class level wiring and not a single stray string. Whether an identifier is queried and sent on a device in the Union was not observed and is UNVERIFIED.

```
com.uodis.opendevice.OPENIDS_SERVICE
com/yfanads/android/oaid/repackage/com/samsung/android/deviceidservice/
    IDeviceIdService$Stub
com.hihonor.cloudservice.oaid.IOAIDCallBack
com/yfanads/android/oaid/repackage/com/heytap/openid/IOpenID
content://com.vivo.vms.IdProvider/IdentifierId/OAID
Lcom/kwad/sdk/oaid/NewOAIDSDKHelper;
Lcom/kwad/sdk/oaid/OADIDSDKHelper25;
Lcom/kwad/sdk/liteapi/oaid/helpers/HONORProxy$a, $b, $c
```

Impact: A user who resets the advertising ID to stop tracking can still be recognised by the OAID, if it is sent.

Fix: Remove the OAID helpers or gate them on a recorded consent decision and name the purpose in the policy.

H3: A development Azure hostname for a GPT feature ships in the production package

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

The dex string pool holds the literal Azure App Service hostname below. The token dev-gpt suggests a development or staging deployment of a GPT backed feature. A development host in a release package is a configuration hygiene observation. The package does not show that the host is reachable or what the corresponding feature sends. The host was not contacted. The finding carries no score.

```
https://dev-gpt-aqdue3fzdtbnh9f0.eastus-01.azurewebsites.net/
```

Impact: If the host is live and receives user input from the production app, it may have weaker controls than a production system.

Fix: Remove development hosts from release builds.

H4: The local data model holds ECG, blood pressure, blood oxygen and blood sugar records, with no consent platform and 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 Play description says: Special statement: non-medical use, only for general fitness and wellness purpose. The local schema in assets/litepal.xml defines the tables EcgBean, BPBean, BOBean, BSBean, HeartRateBean, SleepBean, SleepReportData and TempBean. A person with diabetes, hypertension or a heart condition who uses the device for daily monitoring generates health data in the sense of Art. 9, and the disclaimer does not reduce its nature. The manifest requests ACCESS_BACKGROUND_LOCATION, CAMERA, READ_SMS, SEND_SMS, READ_CONTACTS, READ_CALL_LOG, ANSWER_PHONE_CALLS and PROCESS_OUTGOING_CALLS, a surface wider than biometric monitoring needs. The package holds no consent platform (M1) and the configuration permits cleartext (C1). No data protection impact assessment is published. What the app stores or sends for these tables was not observed and is UNVERIFIED. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the data model covers ECG, blood pressure, blood oxygen and blood sugar, the app has more than 5 million installs, the configuration permits cleartext and no consent mechanism of any kind exists in the package.

```
Play description: "Special statement: non-medical use, only for general fitness/
    wellness purpose."

assets/litepal.xml: EcgBean, BPBean, BOBean, BSBean, HeartRateBean, SleepBean,
    SleepReportData, TempBean
```

Impact: The data allows a third party to infer a chronic condition such as diabetes, hypertension or a cardiac condition, and it sits behind a network configuration that permits plain HTTP and a policy that says everything is encrypted.

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

M1: No consent management platform exists anywhere in the package, and the ad and analytics SDKs start without any recorded decision

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026

A search of the resource tree and all ten dex files for OneTrust, Didomi, Usercentrics and the IAB TCF markers (IABTCF, consent_string) returned no match. The manifest holds no initOrder attribute on any provider, so the ordering pattern of other targets cannot be shown the same way. Android constructs every declared provider, among them androidx.startup.InitializationProvider and the FileProviders of the ByteDance, Baidu and Tencent GDT SDKs, before any activity can show a dialog. With no consent platform present, no mechanism exists that lets a user give or refuse consent before the processors of C2 can operate. Whether each advertising SDK holds back its own initialisation behind an app level flag cannot be seen without a bytecode pass and is UNVERIFIED. No claim is made that a transmission before consent occurs.

```
OneTrust: 0 matches   Didomi: 0 matches   Usercentrics: 0 matches   IAB TCF /
    consent_string: 0 matches
Searched: full resource tree and all 10 classes*.dex files
```

Impact: A person who opens the app is never asked, and the app carries no mechanism to ask.

Fix: Add a consent management platform and delay SDK initialisation until a recorded decision.

Impact Analysis

The people affected are the more than 5 million installers, who wear a watch, grant Bluetooth, location, phone, SMS, contacts and camera access and record heart, blood pressure, blood oxygen, ECG and blood sugar values. Some may be children, since the Play rating is PEGI 3. 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 policy says that all information is encrypted while the configuration permits plain HTTP and user installed certificates for every host (C1). The policy names four SDKs while the package holds at least twenty processors (C2). The health data model covers ECG, blood pressure, blood oxygen and blood sugar and no consent platform exists (H4, M1).

What the package shows is configuration, file content and the operator’s own text. No health reading, message or identifier was observed leaving a device and the report asserts no such flow. The Data Safety card says that data is not encrypted, which matches the package.

The Complete Chain

Step 1, listing and first start: the Data Safety card says that no data is shared and that data is not encrypted. The app contains no consent platform and the SDKs of the package are present from the start (C2, M1).

Step 2, pairing and use: the user grants Bluetooth, location, SMS, contacts, call log and camera access. Health tables for ECG, blood pressure, blood oxygen and blood sugar fill (H4). Identifier helpers of five phone makers are present (H2).

Step 3, backend: the policy states storage on an Alibaba Cloud server. The configuration permits plain HTTP and user installed certificates for every host (C1). Processors in the People's Republic of China and elsewhere are present, and an SDK can fetch plugin bundles (C2). A voice chat platform and a development host are wired in (H1, H3).

Step 4, rights: the policy gives an account cancellation path and the contact service@xinsudian.com. No representative exists in the Union.

Platform Fingerprint and Correlation Keys

The R1 file compares the BLE stack with the clusters recorded earlier in this programme and finds no match. The primary namespace com.rd.rdmtk.* is the operator's own. The Bluetrum namespace of HryFine and Wearfit Pro and the Moyoung CRRepa namespace of Da Fit do not appear. The certificate CN=rdtf, O=runde matches none of the certificates of the other targets. The narrow cluster claim of an identical BLE UUID, certificate and native library fingerprint is therefore not made. Two weaker points are recorded as data points. RDFit ships libjl_ota_auth.so, the same file name as the Zhuhai Jieli library recorded in the R1 findings of FitPro, Lefun Health, MActivePro and OnWear Pro. Jieli is a chipset vendor whose SDK is redistributed to many unrelated makers, so the name proves no shared operator. RDFit also shares the Realtek and Realsil chipset family with Da Fit through a different Realsil module.

The R1 files of RDFit and OnWear Pro share several strings. These are the AIGC gateway swapi.yueqizhixiang.com, the Baidu host duer-kids.baidu.com, the iFlytek hosts iat-api.xfyun.cn and tts-api.xfyun.cn and the Alibaba package com.alibaba.aliagentsdk. The match is at the level of strings in two findings files. No byte level comparison was made and no common operator is claimed.

```
APK SHA-256
    cc33b28c131410ba00a04aa794b8cc591251f8b4d43606c0f61ddf50b64b6b1b
Signing cert SHA-256    6612
    b93ef05ea5ad004dd47abc5f31679d4c0d989a40cd01c579afdb2687f3b8
Signing cert SHA-1      b192d983db374f3d22bdb6c69bb137567cf0417a
Signing DN              CN=rdtf, OU=runde, O=runde, L=shenzhen, ST=guangdong, C=86 (
    self-signed by the operator)
Amap API key            e5ec21a71a842186a37a8ae85bc911a0
Domains                 rundefit.com, xinsudian.com, api.lizheng.design, swapi.
    yueqizhixiang.com
Native libraries        librdnordic.so, libRtkAesJni.so, libjl_*.so (9 files),
    libAMapSDK_NAVI_v9_8_1.so, libBugly_Native.so, libvosk.so
```

The findings file records hashes of the APK and the certificate and no hashes of individual native libraries. The numeric BLE manufacturer identifiers and GATT UUID values were

not extracted. Only the field names getManufacturerSpecificData, vendorId, productId, device_model and firmware_version were confirmed in the dex string pool.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2, H1 and M1.

Article 5(1)(c), data minimisation: engaged by C2, H2 and H4.

Article 5(1)(f) and Article 32(1)(a) and (b): engaged by C1 and H4. Article 32(1)(b) is open for H3.

Article 5(2), accountability: engaged by C1 and M1.

Articles 6(1)(a) and 7(1): engaged by M1. Article 7(3) is engaged by H2.

Article 8: engaged by H1.

Article 9: engaged by C1 and H4 for ECG, blood pressure, blood oxygen and blood sugar data.

Article 13(1)(e): engaged by C2 and H1.

Article 25: engaged by C1, H2 and, as an open question, H3.

Article 35: engaged by H1 and H4.

Articles 44 and 46: engaged by C2. The policy names no transfer mechanism for any of the processors.

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 lists Location, Health and fitness and Device or other IDs as collected, says No data shared with third parties and says that Data isn’t encrypted. The statement that no data is shared does not match the operator’s own policy, which names Amap, Google Login, Facebook Login and Tencent Bugly as SDKs, or the processors of C2. The statement that data is not encrypted matches the cleartext configuration of C1 and contradicts the bundled policy.

Regulatory & Legal Landscape

Shenzhen Runde Intelligent Communication 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.rd.tengfei.bdnotification
Version            4.1.4 (versionCode 436), minSdk 26, targetSdk 35
APK SHA-256        cc33b28c131410ba00a04aa794b8cc591251f8b4d43606c0f61ddf50b64b6b1b
    (191,063,310 bytes)
Signing cert SHA-256 6612b93ef05ea5ad004dd47abc5f31679d4c0d989a40cd01c579afdb2687f3b8
Signing cert SHA-1   b192d983db374f3d22bdb6c69bb137567cf0417a
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
Amap API key         e5ec21a71a842186a37a8ae85bc911a0   (AndroidManifest.xml meta-data
    )
Development host     https://dev-gpt-aqdue3fzdtbnh9f0.eastus-01.azurewebsites.net/
Voice chat host      https://duer-kids.baidu.com/botwatch/api/operation/aigc/stream/
    dcschat
AIGC gateway         swapi.yueqizhixiang.com
Contact              service@xinsudian.com
Bundled policy       assets/privacy_policy_en.htm (Updated: June 7, 2023)
```

Other observations, not scored. READ_LOGS, HARDWARE_TEST and DEVICE_POWER are declared and are not grantable to an ordinary app, which suggests a build from a broader maker template. The Amap key is client embedded by design and its restrictions were not tested. A NetEase Cloud Music open API bridge (assets/ble_analyze.js, endpoint openapi.music.163.com) is a further processor outside the twenty counted in C2. The permission BIND_ACCESSIBILITY_SERVICE is declared without a registered accessibility service, and the dex traces it to a Jetpack Compose state provider, so it was checked and cleared.

```
C1  res/xml/network_security_config.xml, AndroidManifest.xml (application element),
    assets/privacy_policy_en.htm, assets/litepal.xml
C2  assets/privacy_policy_en.htm (SDK section), AndroidManifest.xml, classes*.dex (
    namespaces and hostnames)
H1  classes*.dex (endpoints, DuerOS schema), assets/litepal.xml (AIChatBean,
    AsrTranslateBean)
H2  classes*.dex (OAID references)
H3  classes*.dex (development hostname)
H4  Google Play listing text, assets/litepal.xml, AndroidManifest.xml
M1  resource tree and classes*.dex (consent platform search)
```

Reproduction: obtain com.rd.tengfei.bdnotification 4.1.4 (436), check the SHA-256 value above, decode the manifest and resources with apktool without sources, extract strings from the ten dex files and read the bundled policy and schema. 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 RDFIT-2026-R1 at 07:17 UTC to service@xinsudian.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 16:45 UTC. It restated the findings and the three questions with answers due on 19 September 2026.

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

2026-11-14 No reply of any kind and no delivery failure. The mailbox holds no inbound message from the operator.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

What Was Done Well

The bundled policy is substantive in places. It names the Alibaba Cloud storage location, describes the self start and associated start behaviour in plain language and states a real account cancellation path with preconditions (Login APP, My Account, Setting, Account and Security, Account Cancellation). The Data Safety card is honest on the point that data is not encrypted, which matches what the package does. The policy states that clipboard content is processed on the device only, and no contradicting code path was found.

Residual Risk & Recommendations

Open at the date of publication: all seven entries. The operator has not replied and the build analysed is version 4.1.4. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, remove the cleartext allowance and the user certificate trust and correct the encryption statement in the policy (C1). Second, list every processor with purpose and country and state the Chapter V mechanism, and disable the plugin download of the advertising SDK (C2). Third, gate the health features behind explicit consent and complete a data protection impact assessment (H4). Fourth, add a consent management platform (M1). Fifth, name or remove the voice chat platform and add an age gate (H1). Sixth, remove the OAID helpers and the development host (H2, H3).

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 RDFIT-2026-R1.