Security & Privacy Disclosure, Final Report

FitCloudPro for Android (com.topstep.fitcloudpro)

Global cleartext override and a plaintext MQTT channel on an ECG and cycle tracking app, three undisclosed processing purposes and Chinese cloud processors with four different operator identities.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED 20 NOVEMBER 2026. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Shenzhen Tuobu Intelligent Big Data Co., Ltd. (Toppo, developer account topstep)
Versions Audited	2.6.3-2607041846 / versionCode 163 (Play update 2026-07-04, analysed 2026-08-23)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	8: 1 High, 4 Medium, 3 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`8c481bc5710680a661c42529a542ed1a1412538b0b0520889e88c9f5d020d37d`

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 Findings 6

5.1 C1: Global cleartext override in all three network security configurations, plaintext HTTP endpoints and a plaintext MQTT channel to Alibaba Cloud IoT Hub . 6

5.2 H1: Three implemented processing purposes that the privacy policy does not mention: partner pairing, AI chat and image generation, and an ad-serving game platform 7

5.3 H2: Maximum-priority SMS broadcast receiver with the full telephony and contacts permission bundle 8

5.4 H3: Microphone permission tied to three third-country speech backends, with an AI health advice feature on the operator's own domain 9

5.5 H4: PRC and other foreign cloud SDK cluster, and a policy that never mentions the GDPR, the EU, the EEA or a data protection officer 10

5.6 H5: Hardcoded API keys and secrets in the manifest 11

5.7 M1: PEGI 3 rating against a policy that declares the service for adults, with no age gate 11

5.8 M2: FileProvider paths declared as root directories 12

6 Impact Analysis 12

7 The Complete Chain 13

8 Shared Chipset SDK Fingerprint 13

9 Data Protection: Article by Article 14

10 Platform Accountability & DSA 14

11 Regulatory & Legal Landscape 15

12 Indicators of Compromise & Reproducible Evidence 15

13 Disclosure Timeline & Outcome 16

14 What Was Done Well 16

15 Residual Risk & Recommendations 17

Executive Summary

FitCloudPro is the Android companion app of Bluetooth smartwatches and bracelets, published on Google Play by the developer account topstep with more than 10 million downloads. It records ECG, blood pressure, blood oxygen, sleep stages and menstrual cycle data, mirrors calls, SMS and contacts to the watch and offers partner pairing, an AI chat and a game platform. On 22 August 2026 RFI-IRFOS (ZVR 1015608684, GISA 39261441) disclosed eight findings from a root level code analysis of version 2.6.3 under REF FITCLOUDPRO-2026-R1.

The most serious finding concerns transport security. All three shipped network security configurations permit cleartext traffic for the whole application with no pinning, two first-party ad endpoints use http:// and an MQTT broker URL at Alibaba Cloud IoT Hub uses the plaintext tcp:// scheme (C1). Three implemented processing purposes do not appear in the privacy policy: a Lovers partner pairing module, an AI chat and image generation module through Alibaba Cloud Bailian, and an ad-serving mini-game platform (H1). The microphone permission connects to Baidu, iFlytek and Microsoft Azure East Asia speech backends (H3), and the policy never mentions the GDPR, the EU or a representative while the app is offered in the EU store with EUR pricing (H4).

Four identities attach to the product: the developer account topstep, Shenzhen Tuobu Intelligent Big Data Co., Ltd. in the policy, the domain families hetangsmart.com and topsteptech.com, and the signing certificate O=ifirebird. The build also carries the Bluetrum chipset SDK namespace that other wearable apps in the corpus share.

The operator received the notice at two addresses and neither 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 20 November 2026, as stated in both follow-ups, and it does not depend on a reply. A final APK diff and a re-read of the policy before that date determine the state this report records.

Scope: Root level code analysis of the Google Play release 2.6.3 (versionCode 163) as an XAPK bundle: decoded manifest and resources, dex string-pool extraction across four dex files, native library inventory. Public policy page 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	Global cleartext override in all three network security configurations, plaintext HTTP endpoints and a plaintext MQTT channel to Alibaba Cloud IoT Hub
H1	MEDIUM	Three implemented processing purposes that the privacy policy does not mention: partner pairing, AI chat and image generation, and an ad-serving game platform
H2	MEDIUM	Maximum-priority SMS broadcast receiver with the full telephony and contacts permission bundle
H3	MEDIUM	Microphone permission tied to three third-country speech backends, with an AI health advice feature on the operator's own domain
H4	MEDIUM	PRC and other foreign cloud SDK cluster, and a policy that never mentions the GDPR, the EU, the EEA or a data protection officer
H5	LOW	Hardcoded API keys and secrets in the manifest
M1	LOW	PEGI 3 rating against a policy that declares the service for adults, with no age gate
M2	LOW	FileProvider paths declared as root directories

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. Cleartext configuration and the two http:// endpoints are as recorded in version 2.6.3.
H1	HIGH	MEDIUM	No reply. Location sharing between partners is UNVERIFIED.
H2	HIGH	MEDIUM	No reply. Off-device transmission of SMS content is UNVERIFIED.
H3	HIGH	MEDIUM	No reply. Backend used per feature is UNVERIFIED.
H4	HIGH	MEDIUM	No reply. Controller identity unanswered.
H5	HIGH	LOW	No reply. Key restrictions are not testable without third-party tests.
M1	MEDIUM	LOW	No reply.
M2	MEDIUM	LOW	No reply.

Subject & Operator Analysis

FitCloudPro is the Android companion app of Bluetooth Low Energy smartwatches and bracelets, published on Google Play under the package com.topstep.fitcloudpro. The Play listing shows more than 10 million downloads, a rating of 4.06 from 83,514 ratings, the category Health & Fitness, PEGI 3 and a price of 0.00 EUR on the EU store. The same developer account also publishes Flywear (com.topstep.flywearpro) and AI Buds (com.topstep.aibuds).

Four different identities attach to this one product. The Play developer account is ”topstep” with the contact person Huang Xin, the country China, no street address and the website http://www.hetangsmart.com. The English privacy policy names Shenzhen Tuobu Intelligent Big Data Co., Ltd., which it calls Toppo, reachable at suggestions@topstep-tech.com and again addressed to Huang Xin. The package is signed with a self-signed certificate dated 2014-03-15 whose subject reads C=CN, ST=guangdong, L=shenzhen, O=ifirebird, OU=ifirebird, CN=tan. The domain families hetangsmart.com, topstep-tech.com and watchfun.cn complete the picture. The original-language registration name of the policy entity was not independently verified.

No postal address, no data protection officer and no Art. 27 representative appear in the Play listing, the policy or the binary. The policy was last updated on 19 December 2025 and is hosted on Alibaba Cloud OSS in the Shenzhen region.

Architecture & Data Flow

The package is an XAPK bundle of 175 MB with a 111 MB base APK, an armeabi-v7a native library split and 19 language splits. It is a native Kotlin and Java app with four dex files (about 29 MB), minSdkVersion 21 and targetSdkVersion 35. The manifest declares 53 permissions (eight of them Android Health Connect write grants), 52 activities of which 23 are exported, 16 services, 12 receivers and 12 providers. No ContentProvider sets an initOrder.

The first-party backend is api.hetangsmart.com with an additional api.lizheng.design in the network security configuration. A consent screen (AskPolicyActivity) appears before the main activity. Around the Bluetooth link to the watch the app talks to Alibaba Cloud (IoT Hub MQTT, OSS, Bailian), Baidu (maps and speech), iFlytek and Azure (speech), Tencent (logging), MobTech (sharing), Huawei (HMS) and Sina Weibo (sharing). Health data is also written through Android Health Connect.

Which fields leave the phone toward which host is UNVERIFIED. The review decoded resources and extracted the dex string pool without a bytecode control-flow pass and without dynamic traffic capture.

Findings

C1: Global cleartext override in all three network security configurations, plaintext HTTP endpoints and a plaintext MQTT channel to Alibaba Cloud IoT Hub

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 same permissive configuration is shipped in all three network security variants, two real endpoints and an MQTT broker URL already use plaintext schemes, and the app handles Art. 9 health data of more than 10 million installs. res/xml/network_security_config.xml sets cleartextTrafficPermitted="true" in its base-config. The two other shipped variants do the same. No pin-set exists. Two first-party ad endpoints are hardcoded as http:// and an MQTT broker URL uses the plaintext tcp:// scheme.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">api.lizheng.design</domain>
    </domain-config>
</network-security-config>
```

With targetSdkVersion 35 Android denies cleartext traffic by default. The app opts back in for the whole application. network_security_config_debug.xml and sm_network_security_config.xml, the two other variants in the same build, also permit cleartext. Trust anchors are system only and nothing is pinned.

```
http://api.hetangsmart.com/v2/ad/getAdData
http://api.hetangsmart.com/v2/ad/uploadAdPv
tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
<service android:name="org.eclipse.paho.android.service.MqttService"/>
```

All other api.hetangsmart.com paths in the string pool use https://. The MQTT broker URL uses tcp:// and not ssl:// or mqtts://. The Eclipse Paho client classes (MqttClient, MqttTopic, IMqttClient) are present. Whether the broker connection carries a currently used command channel or is dormant code is UNVERIFIED. The finding is that capability and plaintext transport both exist in the shipped binary.

The app processes ECG waveforms (EcgHealthReportActivity, EcgDetailReportFragment), blood pressure, blood oxygen, sleep stages and, according to section 1.3.1(l) of the operator's policy, menstrual cycle dates with mood and physical condition. It also handles SMS, call and contact content (H2) and background location.

Impact: Anyone on the same network as a person using the app, for example public Wi-Fi, can read or alter traffic on the plaintext endpoints. The app handles ECG, blood pressure

and menstrual cycle data, and no certificate is pinned.

Fix: Remove cleartextTrafficPermitted from the base-config in all three variants, serve the ad endpoints over HTTPS, switch the MQTT broker to ssl:// and pin the first-party API hosts.

H1: Three implemented processing purposes that the privacy policy does not mention: partner pairing, AI chat and image generation, and an ad-serving game platform

---

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 binary contains a Lovers pairing module with a local database table and nine back-end endpoints, an AI chat and image module routed through Alibaba Cloud Bailian, and an HTML5 mini-game platform with first-party ad endpoints. A full-text search of the English policy for lover, partner, couple, dating, AI chat, AIGC, game and mini-game returned zero matches.

```
LoversFragment  LoverViewModel  LoversBindFragment  BoundLoversDialog
CREATE TABLE IF NOT EXISTS `LoverEntity` (`dirty` INTEGER NOT NULL,
   `syncSuccessTime` INTEGER NOT NULL,
`userId` INTEGER NOT NULL, `identityId` TEXT NOT NULL, `userName` TEXT, `nickName`
   TEXT NOT NULL,
`loverDate` TEXT, `loverBindDate` TEXT, `avatar` TEXT, `lastModifyTime` INTEGER NOT
   NULL, PRIMARY KEY(`userId`))

https://api.hetangsmart.com/v2/lovers/{bindLovers, getMyLovers, searchLovers,
   setLoverDate,
   unbindLovers, setMsgDelivery, getSocketConfig, updateBindApply, sendMsg}
```

One account's identity, nickname, avatar and relationship date are sent to and stored for a second account, and getSocketConfig points to a real-time messaging channel between the two paired accounts. The endpoint list shows binding, messaging and the relationship date. A location endpoint is not in the evidence, so location sharing between partners is UNVERIFIED and is not asserted here.

```
https://api.hetangsmart.com/v2/aiChat/get_ai_params
https://api.hetangsmart.com/v2/aigc/createAigcImage   /createAliBailianDraw
   /queryAliBailianResult
                                                       /queryAigcStyle
                                                          /addEvaluate
com.tenmeter.smlibrary  (SMGameH5Activity, SMGameListNewActivity)
https://api.hetangsmart.com/v2/game/getGameInfo
http://api.hetangsmart.com/v2/ad/getAdData
   http://api.hetangsmart.com/v2/ad/uploadAdPv
```

The policy frames the product as an application that records and analyses exercise and health data to provide sports guidance and health services (section Introduction, point 1). No purpose clause covers partner-account data, prompt processing by a generative AI backend, or advertising and game telemetry.

Impact: Couples who link their accounts share identity and relationship data with each other through a feature that the policy never names. Users who type or speak to the AI feature

send content to a Chinese cloud platform that the policy never mentions.

Fix: Describe all three purposes in the policy with their legal basis and recipients, or remove the features. Add a consent or explanation step before account pairing.

H2: Maximum-priority SMS broadcast receiver with the full telephony and contacts permission bundle

---

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)

MySmsBroadcastReceiver is exported with intent-filter priority 2147483647, the maximum, and is protected by the BROADCAST_SMS system permission. The manifest declares READ_SMS, RECEIVE_SMS, SEND_SMS, READ_CALL_LOG, CALL_PHONE, ANSWER_PHONE_CALLS, READ_CONTACTS, READ_PHONE_STATE and calendar access.

```
<receiver android:exported="true"
   android:name="com.topstep.fitcloud.pro.function.MySmsBroadcastReceiver"
          android:permission="android.permission.BROADCAST_SMS">
    <intent-filter android:priority="2147483647">
        <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
        <action android:name="android.provider.OppoSpeechAssist.SMS_RECEIVED"/>
    </intent-filter>
</receiver>
```

The priority puts the receiver ahead of every other receiver for incoming SMS. Only the system can send it the broadcast, so the exposure is interception scope and not an open component. The policy (sections 1.2 and 1.3.1(e)) describes the feature in specific terms, mirroring calls, SMS and contacts to the paired wearable and an ICCID-based SMS quick reply, and states that the app does not store this data. That commitment is checkable and specific. No persistence class for SMS or call content appears in the string pool, which fits the commitment but does not prove it. Whether any of this content leaves the phone beyond the Bluetooth link is UNVERIFIED.

Impact: Callers, senders and contacts who never installed the app have names, numbers and message metadata processed and relayed to a second device without any notice reaching them.

Fix: Keep the receiver priority at the default unless a feature needs the maximum, document the SEND_SMS and CALL_PHONE uses, and confirm in writing that content stays on the Bluetooth link.

H3: Microphone permission tied to three third-country speech backends, with an AI health advice feature on the operator's own domain

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)

The build bundles Baidu Speech, iFlytek and Microsoft Azure Speech SDKs, each with its own classes and endpoints. The Azure endpoint is in the East Asia region, which is not an EU data residency region.

```
Baidu     com/baidu/speech/*  EventManagerAsr  VoiceRecognitionService
          libBaiduSpeechSDK.so  libbdEASRAndroid.so  libBDSpeechDecoder_V1.so
             libbd_etts.so  libbdSpilWakeup.so
          https://vop.baidu.com/realtime_asr   https://tsn.baidu.com/text2audio
             https://api.hetangsmart.com/v2/tts/baiduTts
iFlytek   com/artillery/ctc/base/IflytekData  ContinuousSpeechRecognizer
          https://iat-api.xfyun.cn/v2/iat   wss://rtasr.xfyun.cn/v1/ws
             https://tts-api.xfyun.cn/v2/tts
Azure
   wss://eastasia.stt.speech.microsoft.com/speech/recognition/conversation/
    cognitiveservices/v1
```

The operator hosts an AI health advice web feature at fitcloud.hetangsmart.com/oss/static/ladder/aihealth/ (aiHealthadvice.html, analyze.html, healthDataAnalysis.html, history.html) next to the /v2/aiChat/get_ai_params endpoint from H1. Which of the three speech backends runs for which feature, and whether the voice pipeline feeds the health advice chat, is UNVERIFIED because no runtime trace was taken. The binary shows that speech captured through RECORD_AUDIO can be routed to at least three outside processors, two of them Chinese companies.

Impact: People who dictate a symptom or a health question to the app can send their voice to processors in China or in Microsoft's East Asia region, and the policy names none of them.

Fix: Name each speech processor and its region in the policy, limit the pipeline to one documented backend with a transfer safeguard, and run a data protection impact assessment for the voice feature.

H4: PRC and other foreign cloud SDK cluster, and a policy that never mentions the GDPR, the EU, the EEA or a data protection officer

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)

Class and endpoint evidence shows Baidu, Alibaba Cloud, Tencent, MobTech, Huawei and Sina Weibo components. A full-text search of the policy for GDPR, European Union, EEA, Data Protection Officer and DPO returned zero matches. The app is offered on the EU Play Store with EUR pricing.

Vendor	Evidence
Baidu	Maps SDK (libBaiduMapSDK, com/baidu/mapapi), Speech SDK (H3), digital human assets (digitalhuman.baidu.com, bj.bcebos.com)
Alibaba Cloud	IoT Hub MQTT (C1), OSS storage (the policy itself is hosted on aliyuncs.com OSS in the Shenzhen region), Bailian platform (H1)
Tencent	com.tencent.mars xlog logging framework, com.tencent.mmkv key-value store
MobTech (Shanghai Youkun Information Technology Co., Ltd.)	ShareSDK with Mob-AppKey and Mob-AppSecret (H5), named as sub-processor in section 2.1(c) of the policy
Huawei	HMS ML Kit, AGConnect, ScanKit, appid 102494185
Sina Weibo	Share SDK (com.sina.weibo.sdk, libweibosdkcore.so)
iFlytek, Microsoft Azure	Speech backends (H3)

The queries block lists QQ, WeChat and Sina Weibo next to the usual Facebook, Twitter, Instagram and Huawei entries, which fits a design for the Chinese market adapted for international distribution. The policy rights section (section 3) speaks of access, correction and account cancellation without naming any legal regime. No postal address of the controller appears in the policy or on the Play Store listing. Only suggestions@topstep-tech.com (policy) and rd@hetangsmart.com (Play Store) are given, and both are addressed to the same person, Huang Xin.

Impact: EU users who read the policy learn nothing about where data goes, who the controller is for them, or how to reach a representative, while the binary points to Chinese infrastructure.

Fix: Name the controller with a postal address, appoint an Art. 27 representative, state the destination countries and the Art. 46 safeguard, and cite the GDPR rights in the EU policy text.

H5: Hardcoded API keys and secrets in the manifest

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

AndroidManifest.xml contains a Google Maps key, a MobTech AppKey with its AppSecret, a Facebook AppId with its ClientToken and a Huawei HMS AppId. No key was tested or used.

```
Google Maps API key   AIzaSyCvisBJrCrXhu9m-SU0wnmB82lI30jJdB4
MobTech Mob-AppKey    2086ac2709498
MobTech Mob-AppSecret 1c96c051c2615b728c613f52dfd6d9be
Facebook AppId        263170919132843
Facebook ClientToken  b80f57aa50643f68758bb2316e1ab77f
Huawei HMS appid      102494185
```

A hardcoded credential is a finding whether or not the issuing platform restricts it. Restrictions were not tested, since testing would mean calling third-party services. The MobTech value is a shared secret and not only an identifier, so a third party who holds it could impersonate the app towards MobTech. The Google Maps key carries quota and billing exposure. The risk lies with the operator's accounts. No user data is exposed by this finding.

Impact: The operator carries the abuse and billing risk on four platform accounts, and users lose sharing and map features if quotas are exhausted.

Fix: Rotate the MobTech secret and the Facebook ClientToken, restrict the Maps key to the package name and signing certificate, and move secrets that must stay private to a server.

M1: PEGI 3 rating against a policy that declares the service for adults, with 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 shows PEGI 3. The first paragraph of the policy says the service object of the product is adults and asks minors to read the terms with a guardian. A string search for age gate, date of birth, COPPA and parental consent found none. The only birthday field is a profile entry used for BMI and health calculations after registration.

Nothing in the binary prevents a self-declared minor from registering and using the SMS, call, contact, camera, location and health features. The only enforcement is a sentence in a policy. PEGI 3 is the rating that tells parents there is no age concern.

Impact: A child whose parent saw PEGI 3 can register and use an app that mirrors messages, uses background location and records health measurements.

Fix: Align the content rating with the stated adult audience and add an age screen at registration.

M2: FileProvider paths declared as root directories

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/file_provider_paths.xml declares every path element with path="." for external, external-files, cache, external-cache and files storage.

```
<paths>
    <external-path name="external" path="." />
    <external-files-path name="external_files" path="." />
    <cache-path name="cache" path="." />
    <external-cache-path name="external_cache" path="." />
    <files-path name="files" path="." />
    <files-path name="album" path="." />
</paths>
```

The provider at authority com.topstep.fitcloudpro.fileprovider is not exported and uses grantUriPermissions, so exposure is limited to apps that receive a URI from the app, for example through a share or camera intent. The grant, once made, covers more than the shared file.

Impact: A file shared through a camera or share intent can open up the surrounding storage directories to the receiving app.

Fix: Scope each path element to the one subdirectory that a feature needs.

Impact Analysis

FitCloudPro has more than 10 million installs. Its users record ECG, blood pressure, blood oxygen, sleep stages and menstrual cycle data, forward calls and messages to a band, and can pair their account with a partner account.

Four groups carry the consequences. People who record cardiac and cycle data use an app whose network configuration permits plaintext everywhere (C1). Couples who pair accounts share identity and relationship data through a feature the policy does not describe (H1). People who dictate to the app send voice to processors in China and in a Microsoft region outside the EU (H3). Callers, senders and contacts who never installed the app are processed without notice (H2). A child who installs the app because of its PEGI 3 rating meets all of these features, while the policy says the service is for adults (M1).

The harm demonstrated is a harm of opacity and default configuration. EU users cannot learn from the policy who the controller is, which features exist or where data goes. Observed exposure on the wire is not claimed because no traffic was captured.

The Complete Chain

Step 1, install: a user finds an app rated PEGI 3 with a first-run consent screen and a policy that describes a health tracker for adults (M1).

Step 2, permissions: the user grants Bluetooth, location, contacts, SMS, call log, camera and microphone so that the watch can mirror calls and messages and take voice input (H2, H3).

Step 3, features beyond the policy: the user may pair with a partner, chat with an AI or open a mini game with advertising, none of which the policy names (H1).

Step 4, transmission: the network security configuration permits cleartext for every host, two ad endpoints use http:// and an MQTT broker URL uses tcp:// (C1). Voice can go to Baidu, iFlytek or Azure East Asia, and analytics and sharing components reach Tencent, MobTech, Huawei and Sina Weibo (H3, H4).

Step 5, the user tries to act: the policy does not mention the GDPR, the EU or a representative, names a controller without a postal address and gives one e-mail address that is also addressed to an individual (H4).

Shared Chipset SDK Fingerprint

FitCloudPro ships the Bluetrum reference SDK for Bluetooth chipsets in unmodified class names. The same class namespace appears in HryFine and Wearfit Pro, two apps from other operators in the RFI-IRFOS corpus with their own reports of the same date. Bluetrum is a Shenzhen vendor of Bluetooth system-on-chip products. The signing certificates differ between the apps, which is expected, because each operator signs its own build. What matches is the vendor component. A property or defect in that component is inherited by every operator that uses it, whichever brand name the buyer sees.

```
Class namespace    Lcom/bluetrum/abpartool/ParTool;  Lcom/bluetrum/abpartool/R;
   Lcom/bluetrum/abpartool/utils/ImageUtils;
Native library     lib/armeabi-v7a/libabpartool.so  116,416 bytes
libabpartool.so    SHA-256
   8b1a8e2eb782582bc9969034c6d5cf91ce3d51ed48ce4f697686f19287519f9f
Signing cert
   AA:9A:D1:CB:23:79:EB:CD:DA:B5:87:49:13:1B:06:A7:1A:8F:57:C5:3E:4E:86:44:61:84:6C
    :79:DA:50:55:DF
Signing DN         C=CN, ST=guangdong, L=shenzhen, O=ifirebird, OU=ifirebird, CN=tan
Field names        device_model, product_id, firmware_version, vendor_id (dex string
   pool)
```

A byte-level hash comparison against the libraries of the other two apps was not possible, so the match rests on identical class names. BLE manufacturer IDs and GATT UUID constants were not extracted at this depth.

Data Protection: Article by Article

Article 4(7), controller: engaged by H4. Four identities appear across the listing, the policy and the certificate and the policy names one of them.

Article 5(1)(a), (b) and (f), fairness and transparency, purpose limitation, integrity and confidentiality: engaged by H1, H2 and C1.

Article 6(1): engaged by H1 and H2. No legal basis is stated for partner pairing, AI processing or ad telemetry, and none reaches the callers and contacts of H2.

Article 8, conditions for a child's consent: engaged by M1.

Article 9, special categories: engaged by C1 and H3. ECG, blood pressure, blood oxygen, sleep and cycle data are health data and are processed in the configuration of C1.

Articles 12(1), 13(1)(a) and (c) and 14(1)(c): engaged by H1 and H4. Purposes, recipients and the controller's identity are not stated accurately.

Article 25, data protection by design and by default: engaged by C1, M1 and M2.

Article 27, EU representative: engaged by H4. None found.

Article 32(1)(a) and (b), security of processing: engaged by C1 and H5.

Article 35, impact assessment: engaged by H3. Voice processing next to health data calls for one, and none is published.

Articles 44 and 46, transfers: engaged by H3 and H4. Baidu, iFlytek, Tencent, Alibaba Cloud and MobTech are named in the evidence and no safeguard is named in the policy.

Platform Accountability & DSA

Google Play lists the app as PEGI 3 while the policy declares an adult audience (M1) and offers the app in the EU store with EUR pricing while the policy contains no EU-specific information (H4). Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice under the notice and action mechanism of Art. 16 of that Regulation. RFI-IRFOS records the contradictions here and treats a notice as a decision for the publication stage.

The Data safety declaration of the listing was not captured in the review material for this app and is not assessed.

Regulatory & Legal Landscape

Shenzhen Tuobu Intelligent Big Data Co., Ltd. offers the app to users in the Union with EUR pricing, 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 and the European Data Protection Supervisor received the notice in copy.

Infringements of Art. 5, 6 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, 32 and 35 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82.

The first notice cited Art. 7 of the PRC National Intelligence Law as context for the transfer risk, because the law obliges organisations to support national intelligence work. This report records it as context and not as a finding.

Indicators of Compromise & Reproducible Evidence

Every point is reproducible from the public Google Play build of 4 July 2026 and public web pages read by plain HTTP GET.

```
Package          com.topstep.fitcloudpro
Version          2.6.3-2607041846 (versionCode 163), Play update 4 Jul 2026
XAPK SHA-256     8c481bc5710680a661c42529a542ed1a1412538b0b0520889e88c9f5d020d37d
base.apk SHA-256 fc3d8782a42c373e3c1a9c116ed25807cf59ad9eee14c2a3ddfb732cfcef3f58
config.armeabi_v7a.apk SHA-256
   4e54c36d5346ec991262aa46fbd9740bfb7eb2ef92384e17272bc2dd6de7623d
Signing cert
   AA:9A:D1:CB:23:79:EB:CD:DA:B5:87:49:13:1B:06:A7:1A:8F:57:C5:3E:4E:86:44:61:84:6C
    :79:DA:50:55:DF
minSdk / target  21 / 35
Obtained from    APKPure XAPK, package name, version and publication date matched to
   the live Play listing
```

```
api.hetangsmart.com  api.lizheng.design  fitcloud.hetangsmart.com
   suggestions@topstep-tech.com  rd@hetangsmart.com
tcp://iot-06z00c6kgq6t1w4.mqtt.iothub.aliyuncs.com
http://api.hetangsmart.com/v2/ad/getAdData
   http://api.hetangsmart.com/v2/ad/uploadAdPv
https://api.hetangsmart.com/v2/lovers/*   /v2/aiChat/get_ai_params   /v2/aigc/*
   /v2/game/getGameInfo
https://vop.baidu.com/realtime_asr   https://iat-api.xfyun.cn/v2/iat
   wss://rtasr.xfyun.cn/v1/ws
wss://eastasia.stt.speech.microsoft.com/speech/recognition/conversation/
    cognitiveservices/v1
```

```
https://fitcloud.hetangsmart.com/oss/static/fitcloudpro/privacy-policy/index_en.html
   (last updated 19 Dec 2025, checked 22 and 23 Aug 2026)
```

Disclosure Timeline & Outcome

2026-08-22 First notice, REF FITCLOUDPRO-2026-R1, sent at 23:54 UTC to suggestions@topstep-tech.com and rd@hetangsmart.com, with the Austrian DSB and the EDPS in copy. It listed one critical and five high findings, two medium findings and three questions on the undisclosed purposes, the unencrypted transport and the third-country voice processing.

2026-09-12 First follow-up to both addresses with the findings restated and three questions with a response date of 26 September 2026. They asked why cleartext is permitted globally and when TLS with pinning will be enforced, why the partner pairing, AI chat and ad platform are not in the policy, and which of the four identities is the controller for EU users under Art. 4(7). The follow-up stated the embargo as 20 November 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com, 34 days before publication, with the three questions unchanged and the embargo repeated as 20 November 2026.

2026-11-14 No reply from either address. A search of the mailbox for inbound mail from topstep-tech.com and hetangsmart.com returned nothing. No bounce was recorded for these two addresses.

2026-11-20 Publication date as stated in both follow-ups.

What Was Done Well

allowBackup is set to false. The build contains no third-party advertising mediation SDK and no Firebase, Crashlytics or Google Analytics, which removes a common pre-consent identifier path. No ContentProvider forces an early initialisation order. A dedicated first-run consent screen exists before the main activity, and the permissions that the policy does describe come with specific purpose text. Health data is written through Android Health Connect, which routes part of the data through a consent-managed Google framework. The policy states account deletion concretely, including which records become unrecoverable.

Residual Risk & Recommendations

Open at the date of publication: all eight findings. The operator has not replied. The state recorded here is version 2.6.3 of 4 July 2026. A final APK diff and a re-read of the policy page before 20 November 2026 determine the state that the published report records.

Recommendations in order of effect. First, remove the cleartext permission from all three network security variants, move the ad and MQTT endpoints to TLS and pin the first-party hosts (C1). Second, describe the partner pairing, AI and game features with legal basis and recipients, or remove them (H1). Third, name the controller with a postal address, appoint an Art. 27 representative and state transfer countries and the safeguard in an EU policy text (H3, H4). Fourth, document the SMS receiver and the call and message permissions and confirm that content stays on the Bluetooth link (H2). Fifth, rotate and restrict the keys, align the rating with the stated adult audience and scope the FileProvider paths (H5, M1, M2).

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 FITCLOUDPRO-2026-R1.