Security & Privacy Disclosure, Final Report

VeryFit for Android (com.watch.life)

Menstrual data inside account sharing and ad networks that start before consent: the operator answered, shipped part of the fix in build 354 and plans the rest for 3.8.0.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026, STATED IN OUR MESSAGE OF 17 NOVEMBER. OPERATOR REPLIED 18 NOVEMBER 2026 ON BUILD 354, REMAINING FIXES PLANNED FOR 3.8.0.

Target	Shenzhen iDo Technology Co., Ltd., Longhua District, Shenzhen, China
Versions Audited	3.5.0 / versionCode 342 (analysed 2026-08-23). Build 3.7.1 / versionCode 354 examined statically on 2026-11-17, base.apk SHA-256 efab2aee6f507b5f09ff327fd36c711169cf064486053606e3c96eb754bc45c3.
Supervisory Authority	No EU establishment disclosed. Datenschutzbehörde (Austria) copied.
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	9: 1 High, 4 Medium, 4 Low (eight reassessed from the first notice, one unchanged)
Status	OPERATOR ANSWERED IN WRITING SEVEN TIMES, LAST ON 18 NOVEMBER 2026. BUILD 354 CONFIRMS PART OF THE FIXES. THE REMAINDER IS STATED BY THE OPERATOR, NOT VERIFIED, OR PLANNED FOR 3.8.0 (NO DATE).
SHA-256 (base APK)	`49672cc94bfe495cb4652456d47c4bfd4bfc00b4aa3f5f187ac133bec2989594`

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 4

2 Finding Status at a Glance 7

3 Subject & Operator Analysis 8

4 Architecture & Data Flow 8

5 Findings 9
- 5.1 C3: Menstrual and ovulation data sit inside the cross-account Family Account sharing feature, and no impact assessment existed for it . . . 9
- 5.2 C1: Nine ad and analytics ContentProviders construct at process start, before any consent screen, despite a bundled consent SDK . . . 11
- 5.3 C2: The network security configuration permits cleartext traffic globally, with no domain exceptions and no certificate pinning . . . 12
- 5.4 H1: A multi-region backend at idoocloud.com and veryfitplus.com, a hardcoded Alibaba Cloud log endpoint, and an unanswered question on where EU users' data goes . . . 14
- 5.5 M2: Four Google and Gaode API keys and Firebase project identifiers are hard-coded in the distributed package, and a named SDK is absent from the binary 16
- 5.6 H2: A broad dangerous-permission block for a watch and scale companion app, with each permission traceable to a disclosed feature . . . 17
- 5.7 M1: A paired watch can trigger the phone camera (bleControlTakePhoto) . . . 18
- 5.8 M3: PEGI 3 rating and a date of birth that feeds an algorithm and does not gate access, against a policy that excludes under-16s . . . 18
- 5.9 M4: The Art. 27 representative contact is a mail-only domain with no reachable website . . . 19

6 Impact Analysis 19

7 The Complete Chain 20

8 Health Data, Family Sharing & Bystanders 20

9 Data Protection: Article by Article 21

10 Regulatory & Legal Landscape 22

11 Indicators of Compromise & Reproducible Evidence 22

12 Disclosure Timeline & Outcome 23

13 What VeryFit Got Right 24

14 Residual Risk & Recommendations 25

Executive Summary

VeryFit is the companion app for Bluetooth smartwatches, bands and body-composition scales, published on Google Play as com.watch.life by Shenzhen iDo Technology Co., Ltd., with more than 10 million installs. It handles blood pressure, blood oxygen, heart rate variability, respiratory rate, skin temperature, location and menstrual and ovulation data. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF VERYFIT-2026-R1 after a root level code analysis of version 3.5.0. It described three Critical, two High and four Medium findings and asked three written questions.

Two findings carry the case. The first is that menstrual and ovulation data sit inside the Family Account feature, which lets a linked account see another person's health data, and that the operator has confirmed in writing that no impact assessment was made for that sharing. The second is that nine advertising and analytics components start before any consent screen can appear, although the app bundles a real consent platform.

VeryFit answered, and that deserves to be recorded plainly. Between 18 September and 18 November 2026 the operator sent seven dated written messages. It acknowledged the consent timing and regional endpoint points as areas to improve, confirmed that no impact assessment existed, and brought the removal of menstrual and ovulation data from Family Account sharing forward from a release planned for the first quarter of 2027 into the release now reported as v3.7.1. On 9 November 2026 the operator wrote that v3.7.1 began a staged rollout on both app stores on 7 November 2026. On 16 November 2026 it named Android versionCode 354 and iOS build 26110610 and answered our three questions on the cleartext configuration, the API keys and the version.

This report is stricter than the first notice and is careful about what is proven. Eight of nine findings are reassessed and one is unchanged. The three Critical labels become High, Medium and Medium. On 17 November 2026 RFI-IRFOS examined build 354 statically (Google Play, base.apk SHA-256 efab2aee6f507b5f09ff327fd36c711169cf064486053606e3c96eb754bc45c3). It confirms the removal of the app-wide cleartext permission, the removal of the Firebase and Google Mobile Ads providers from the manifest with consent-gated Firebase initialization, and that the Gaode branch is not taken in the Google Play build. It does not confirm the removal of the cycle upload from the Family Account path, and it shows eleven cleartext exceptions and ten further advertising providers that the manifest still declares. No finding is marked fixed in full.

The operator replied on 18 November 2026. It states that other third-party SDKs need further work on initialization and consent management and that this is planned for version 3.8.0. It confirms eleven cleartext exceptions and plans to reduce them to two domains in 3.8.0 and to remove the endpoint getdata.veryfitplus.com:8011. It states that the app no longer retrieves menstrual data of linked sub-accounts and does not share the primary account's data. That last statement is stated by the operator, not verified, and stands against the upload code found in build 354. Version 3.8.0 has no date. Earlier open points remain: the domain list was withheld on 16 November 2026 and the package supplied it, Firebase App Check is not enabled, no per-key quota exists, the permission block, the age rating and the representative contact are unanswered, and the question about the Guangzhou log endpoint is answered only as not found in build 354. The report is published on 21 November 2026, 90 days after delivery.

Scope: Root level code analysis of VeryFit 3.5.0 (versionCode 342, package com.watch.life): a base APK of 241,844,382 bytes in a 295.7 MB bundle, 14 dex files of about 110 MB and the arm64 native libraries. The analysis used aapt and aapt2 for the manifest, the network security configuration and resource values, apksigner for the signing certificate, and a full strings pass over all 14 dex files (23 MB of extracted strings) and resources.arsc. No full bytecode decompile was run, so findings that depend on call order are marked UNVERIFIED. Public pages read on 23 August 2026: the Google Play listing, the developer page of Smart Wearable Devices and the operator's privacy policy, plus a DNS lookup of vatspeed-eu.com. No account was created, no VeryFit server was called, no key was tested, no traffic was captured and no runtime instrumentation was used. The package was obtained from a public mirror (APKPure) because the audit device was not connected, and the package ID, developer name and icon were cross-checked against the Google Play listing. Version 3.7.1 (Google Play versionCode 354), the release the operator reports as fixed, was examined statically on 17 November 2026 after installation from Google Play (base.apk SHA-256 efab2aee6f507b5f09ff327fd36c711169cf064486053606e3c96eb754bc45c3). No request was sent to the operator's servers or to any third party. Its results are recorded in the findings and the timeline. CVSS v4.0 measures exploitability. Most findings here are data-governance findings with no attacker, so the printed scores are moderate and two findings carry an explicit blast-radius escalation.

ID	Severity	Title
C3	HIGH	Menstrual and ovulation data sit inside the cross-account Family Account sharing feature, and no impact assessment existed for it
C1	MEDIUM	Nine ad and analytics ContentProviders construct at process start, before any consent screen, despite a bundled consent SDK
C2	MEDIUM	The network security configuration permits cleartext traffic globally, with no domain exceptions and no certificate pinning
H1	MEDIUM	A multi-region backend at idoocloud.com and veryfitplus.com, a hardcoded Alibaba Cloud log endpoint, and an unanswered question on where EU users' data goes
M2	MEDIUM	Four Google and Gaode API keys and Firebase project identifiers are hardcoded in the distributed package, and a named SDK is absent from the binary
H2	LOW	A broad dangerous-permission block for a watch and scale companion app, with each permission traceable to a disclosed feature
M1	LOW	A paired watch can trigger the phone camera (bleControlTakePhoto)
M3	LOW	PEGI 3 rating and a date of birth that feeds an algorithm and does not gate access, against a policy that excludes under-16s
M4	LOW	The Art. 27 representative contact is a mail-only domain with no reachable website

ID	Disclosed	This report	Operator position and verification status, 21 November 2026

Finding Status at a Glance

ID	Disclosed	This report	Operator position and verification status, 21 November 2026
C3	CRITICAL	HIGH	Confirmed no DPIA. Build 354 still contains the cycle upload in the Family Account path. Operator states on 18 November that sub-account data is no longer retrieved and primary data is not shared. Stated by the operator, not verified.
C1	CRITICAL	MEDIUM	Firebase and Google providers gated in build 354, confirmed. Ten further advertising providers still declared. Operator plans the remaining SDKs for 3.8.0, no date.
C2	CRITICAL	MEDIUM	Global cleartext permission removed in build 354, confirmed. Eleven domain exceptions remain, confirmed by the operator. Reduction to two domains planned for 3.8.0.
H1	HIGH	MEDIUM	Operator names the purpose of two endpoints, stated by the operator, not verified. Guangzhou endpoint not found in build 354. logFileUrl and buriedUrl open.
M2	MEDIUM	MEDIUM	Unchanged. Operator states package and SHA-1 restriction, no API allowlist, no quota, no App Check. No key rotated.
H2	HIGH	LOW	No written statement.
M1	MEDIUM	LOW	No written statement.
M3	MEDIUM	LOW	No written statement.
M4	MEDIUM	LOW	No written statement. Address copied on the operator’s replies.

Subject & Operator Analysis

The operator is Shenzhen iDo Technology Co., Ltd. (the Chinese company name is listed on Google Play), which calls itself Shenzhen DO Intelligent Technology Co., Ltd. in the English privacy policy. That difference in name is a small accuracy point under Art. 13. The address is No. 1 Lirong Road, Xinshi Community, Dalang Street, Longhua District, Shenzhen 518000. The Play listing shows a personal e-mail address, a QQ mailbox and a mobile number as developer contacts. The privacy policy names ido@idoocn.com, and the operator's replies came from the app product team at app_pmteam@idoocn.com. No data protection officer is named.

The operator is not established in the Union. The policy names services@vatspeed-eu.com and an address in Madrid for EU users (M4). The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the notice for transparency. No lead supervisory authority exists under Art. 56 GDPR for a controller without an EU main establishment.

The Google Play developer account Smart Wearable Devices lists at least nine apps, among them VeryFit Kids, VeryFit Ultra, VerySport, VF Watch, belk watch and SilverCrest Active. The signing certificate of this build names O=ido, L=sz.

Architecture & Data Flow

- Companion app: Bluetooth LE link to watches, bands and scales through the operator's own protocol libraries (libVeryFitMulti.so, libRtkAesJni.so) and Nordic BLE and DFU libraries.
- Health data: heart rate, blood pressure, blood oxygen, sleep, respiratory rate, skin temperature, menstrual cycle and ovulation, body composition through scale algorithm libraries, stored locally with SQLCipher and synced to the operator's cloud.
- Family Account: relationship module with share, cancel-share and recover-share, including a menstrual upload method (C3).
- Cloud: region-segmented idoocloud.com and veryfitplus.com services, with a hardcoded Alibaba Cloud log endpoint (H1).
- Advertising and analytics: nine ContentProviders from Firebase, Google Mobile Ads, AppLovin, Vungle, Meta, Huawei, ironSource and Bigo, and a bundled UMP and IAB TCF consent stack (C1).
- Network configuration: cleartext permitted for every domain (C2).
- Phone integration: SMS, call, contacts, camera and location permissions for SOS, call reminders, notification mirroring and a remote shutter (H2, M1).

What this report does not show is any payload that leaves the phone. Where a statement depends on it, the finding says UNVERIFIED.

Findings

C3: Menstrual and ovulation data sit inside the cross-account Family Account sharing feature, and no impact assessment existed for it

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.8 (CVSS-B), reassessed from CRITICAL in the first notice, rated HIGH by blast-radius escalation. Build 354 examined 2026-11-17, operator reply 2026-11-18

The dex pool contains a Family Account module with a member-relation enum, a share, cancel-share and recover-share lifecycle, and a method FamilyAccountHelper.uploadMenstrualDate. The operator's privacy policy names the Menstrual Cycle Reminder feature and says it collects menstrual cycle and ovulation data. This puts Art. 9 data inside the mechanism that shares step, weight and heart-rate data between linked accounts. On 23 September 2026 the operator confirmed in writing that no DPIA, PIA or similar assessment of this sharing was conducted.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.8 to HIGH because the data is reproductive health data of a special category, the people exposed can be partners or relatives in a position to pressure the account holder, more than 10 million installs are affected, and the operator confirms that no impact assessment was made before the sharing was offered. CRITICAL, as disclosed on 23 August 2026, is withdrawn because the operator states that a linked account needs active authorization and nothing in the package contradicts it.

```
Lcom/ido/life/module/familyaccount/helper/
    FamilyAccountHelper$Companion$uploadMenstrualDate$1;
Lcom/ido/life/module/familyaccount/helper/MemberRelationEnum;
Lcom/ido/life/module/familyaccount/share/MemberShareActivity;
Lcom/ido/life/module/familyaccount/share/MemberSharePresenter;
Lcom/ido/life/module/familyaccount/info/
    MemberInfoPresenter$cancelShareMyData$1$onSuccess$1$1;
Lcom/ido/life/module/familyaccount/info/
    MemberInfoPresenter$recoveryShareMyData$1$onSuccess$1;
Lcom/ido/life/module/home/menstrualcycle/dialog/MenstrulationSettingPresenter;
queryAllMenstrualData
PlatformIntermenstrualBleedingRecordBuilder
```

Operator statement of 18 September 2026: access by a primary account to data of a linked account "is not enabled by default" and "authorization must first be actively granted by the linked account". The package analysis neither confirms nor contradicts this. Not shown from the package: the text of the authorization screen, whether it names menstrual and ovulation data as a separate category, whether the default is opt-in or opt-out, and for how long a shared record stays visible. The operator did not answer the question about the screen text and chose instead to remove the category.

Operator statements of 23 September 2026: no DPIA, PIA or similar assessment of this sharing was previously conducted. The category would be removed from Family Account in v4.0.0 (Q1 2027), and until then the existing behaviour stays in place because it cannot be removed server-side without client changes. Operator statement of 19 October 2026: the removal was brought forward into the v3.7.0 development scope. Operator statement of 9 November 2026: the release shipped as v3.7.1, staged rollout on App Store and Google Play

from 7 November 2026, including the removal. RFI-IRFOS records all of this as the operator's statement. Build 354 is compared below.

Build 354 (examined 17 November 2026): FamilyAccountHelper.uploadMenstrualDate(J) exists and is fully implemented. It sends the cycle record (start, end, prediction period, mensLength, mensCycle) through AccountManager.uploadMenstrualRemind to the operator's server and has five call sites in four classes, with no switch in front of any of them. MemberShareActivity passes mMenstrualRemind to pwdAuthAddMember, the field FamilyAccountInfo.menstrualRemind exists and HealthAlertActivity still carries the cycle reminder text for family members. A server-side switch is not visible from the package. What was verified is that the client still collects and uploads the cycle prediction in the Family Account path.

Operator statement of 18 November 2026: the menstrual data kept in 3.7.1 is limited to the primary account's own data, the app "no longer requests or retrieves" menstrual data of linked sub-accounts, and the primary account's data is not shared with linked accounts through Family Account. "Menstrual data sharing between primary and sub-accounts is no longer supported." Stated by the operator, not verified by RFI-IRFOS. The operator does not say whether the upload to its server continues. The finding keeps its grade.

GDPR: Art. 9(1), Art. 9(2)(a), Art. 35(1), Art. 35(3)(b), Art. 25, Art. 13, Art. 14

Impact: A partner, a parent or anyone accepted as a family member in the app could be given sight of another person's menstrual and ovulation history through a relationship feature that was built for step counts. The data subject is not always the person who controls the setting. The authorization the operator describes is the only barrier, and the operator confirms that nobody assessed the risk of this sharing before it was offered.

Fix: Verify in the shipped build that the category is no longer uploaded to or readable by linked accounts, delete previously shared copies on the server, run a DPIA for every remaining Family Account category, and tell existing Family Account users in writing what was shared and with whom.

C1: Nine ad and analytics ContentProviders construct at process start, before any consent screen, despite a bundled consent SDK

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), reassessed from CRITICAL in the first notice. Build 354 examined 2026-11-17, operator reply 2026-11-18

The manifest declares nine ContentProviders from advertising and analytics SDKs, among them Firebase and Google Mobile Ads at initOrder 100, AppLovin at 101, Vungle at 102 and the Huawei advertising ID provider at 500. Android constructs ContentProviders in Application.onCreate(), before any Activity, including a consent form, can render. The package does bundle Google's UMP consent SDK and an IAB TCF v2 decoder (125 class and string hits).

```
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider"
    android:authorities="com.watch.life.mobileadsinitprovider" android:initOrder
    ="100"/>
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
    android:authorities="com.watch.life.firebaseinitprovider" android:initOrder="100"
    android:directBootAware="true"/>
<provider android:name="com.applovin.sdk.AppLovinInitProvider"
    android:authorities="com.watch.life.applovininitprovider" android:initOrder
    ="101"/>
<provider android:name="com.vungle.ads.VungleProvider"
    android:authorities="com.watch.life.vungle-provider" android:initOrder="102"/>
<provider android:name="com.huawei.hms.aaid.InitProvider"
    android:authorities="com.watch.life.aaidinitprovider" android:initOrder="500"/>
<provider android:name="com.facebook.internal.FacebookInitProvider"
    android:authorities="com.watch.life.FacebookInitProvider"/>
<provider android:name="com.facebook.ads.AudienceNetworkContentProvider"
    android:authorities="com.watch.life.AudienceNetworkContentProvider"/>
<provider android:name="com.ironsource.lifecycle.IronsourceLifecycleProvider"
    android:authorities="com.watch.life.IronsourceLifecycleProvider"/>
<provider android:name="sg.bigo.ads.controller.provider.BigoAdsProvider"
    android:authorities="com.watch.life.BigoAdsProvider"/>
```

```
Lcom/google/android/ump/ConsentInformation
Lcom/google/android/ump/ConsentForm
Lcom/iabtcf/decoder/TCStringDecoder
Lcom/iabtcf/v2/PublisherRestriction
IABTCF_GDPR_APPLIES
```

Observed fact: object construction before any UI is guaranteed by the platform. Not shown: whether the SDKs' network activity, as distinct from construction, is held back until a consent decision is recorded. That is UNVERIFIED. The presence of a real consent platform is a mitigating fact. It does not resolve the timing problem, which is the same pattern as in other apps of this wave. The first notice rated this CRITICAL. This report rates it MEDIUM because the evidence is a manifest fact and no transmitted payload was observed.

Operator statement of 18 September 2026, under the heading SDK Initialization and Network Requests Prior to User Consent: the operator "identified areas where the technical imple-

mentation can be further improved" and included the issue in an upcoming version. Operator statements of 23 September and 9 November 2026: the improvement is part of the release that shipped as v3.7.1 from 7 November 2026. The operator's statements did not say which providers were changed. Build 354 is compared below.

Build 354 (examined 17 November 2026), confirmed: FirebaseInitProvider, MobileAdsInitProvider, the Huawei aaid InitProvider and IronsourceLifecycleProvider are no longer declared in the manifest. The Firebase collection flags are false, FirebasePrivacyInit.initializeAfterConsent runs after the privacy agreement and disableAfterRevoke runs on revocation. Still declared and constructed at process start: AppLovinInitProvider (initOrder 101), VungleProvider (102), FacebookInitProvider, AudienceNetworkContentProvider and BigoAdsProvider, plus TraminiContentProvider (100), YandexAdsInitializeProvider, MBComponentLifecycleProvider (Mintegral), TUInitializationProvider (ThinkUp), SDMInitializationProvider, the AppMetrica PreloadInfoContentProvider (exported true), the Alibaba SLSContentProvider and the JPush DataProvider and InitProvider. No explicit initialize call for these advertising SDKs was found in the app code, so their start depends on the providers and the SDK defaults. What they send before consent is runtime behaviour and was not tested.

Operator statement of 18 November 2026: Google and Firebase components are gated by a consent step in 3.7.1, and "some other third-party SDKs still require further optimization in terms of initialization and consent management. These items are planned for further improvement in version 3.8.0." The operator gives no release date. The remaining providers are therefore open by the operator's own account.

GDPR: Art. 5(1)(a), Art. 5(2), Art. 6(1), Art. 7(1), ePrivacy Directive Art. 5(3)

Impact: A person who pairs a watch to track blood pressure, heart rate or a menstrual cycle has nine advertising and analytics components running before they see a consent choice. What those components transmitted in version 3.5.0 was not measured.

Fix: Remove the automatic provider entries from the manifest and start each SDK from application code after the consent state is known, and show with a traffic capture that no SDK request precedes a recorded decision.

C2: The network security configuration permits cleartext traffic globally, with no domain exceptions and no certificate pinning

---

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), reassessed from CRITICAL in the first notice. Build 354 examined 2026-11-17, operator reply 2026-11-18

The entire network_security_config.xml is one element, base-config with cleartextTrafficPermitted set to true. This overrides the secure default of a targetSdkVersion 36 build for an app that handles blood pressure, blood oxygen, heart rate variability, respiratory rate, skin temperature, precise location and menstrual data. No traffic was captured, so no cleartext transmission is shown.

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

This is a configuration finding and not a demonstrated interception. Its weight depends on whether any request that carries health, location or account data uses plain HTTP, and that

depends on the app and its SDKs at runtime. The vector assumes an attacker on the local network and a cleartext request, and rates the confidentiality of the data at stake as high because of what the app holds. The first notice rated this CRITICAL. This report rates it MEDIUM because the exploit conditions are not shown.

The operator answered this item on 16 and 18 November 2026. The findings above describe version 3.5.0. The result for build 354 follows.

Build 354 (examined 17 November 2026), confirmed: network_security_config.xml sets the base-config cleartextTrafficPermitted to false, so the app-wide permission is gone. One domain-config with cleartext permitted remains, with eleven entries each with includeSubdomains: ali-iot.idoocloud.com, cn-iot.idoocloud.com, eu-iot.idoocloud.com, us-iot.idoocloud.com, in-iot.idoocloud.com, offline-live1.services.u-blox.com, online-live1.services.u-blox.com, starcourse.location.io, starcourse.rx-networks.cn, life-content.veryfitplus.com and life-content.idoocloud.com. No pin-set and no certificate pins were found. The five iot hosts are addressed with https in the code. The http uses found are GNSS assistance downloads from u-blox and location.io and a Strava H5 page on life-content.veryfitplus.com, and no http use matching a historical-data scenario was found. Two u-blox AssistNow tokens sit in the offline and online URLs. AccountApi also declares http://getdata.veryfitplus.com:8011/blood/getUserInfo and /blood/calibrate, a host outside the allowlist, so either the feature does not work or the allowlist is incomplete. Which of the two was not tested.

Operator statements: on 16 November 2026 the retained exceptions ”cannot be cleanly separated into a complete standalone list of domains.” On 18 November 2026 the operator confirms that ”11 domains are still explicitly configured as exceptions permitting cleartext traffic” and plans, for version 3.8.0, to reduce the list to two domains required for historical data compatibility and to remove the endpoint getdata.veryfitplus.com:8011 with the blood-related API paths. The operator states that the reduction ”has not yet been completed in version 3.7.1.” The plan is stated by the operator, not verified, and has no date.

GDPR: Art. 32(1)(a), Art. 32(1)(b), Art. 25(1)

Impact: On a shared or hostile network, any health or account request that falls back to plain HTTP could be read or changed by someone nearby. Which requests do so is not established.

Fix: Set cleartextTrafficPermitted to false, add a domain-config only for hosts that cannot use TLS, and pin the certificate for the operator’s own cloud endpoints.

H1: A multi-region backend at idoocloud.com and veryfitplus.com, a hardcoded Alibaba Cloud log endpoint, and an unanswered question on where EU users' data goes

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), reassessed from HIGH in the first notice. Build 354 examined 2026-11-17, operator reply 2026-11-18

The dex pool hardcodes a region-segmented platform at idoocloud.com with ali, cn, eu, in and us prefixes for badge, buried-event tracking, gateway, device, health, IoT, log, running, user and web-content services, and a parallel veryfitplus.com domain. A live Alibaba Cloud Log Service endpoint, cn-guangzhou.log.aliyuncs.com, and an Alibaba object storage endpoint are hardcoded in the same pool. The developer account Smart Wearable Devices (ID 8831072274319617170) lists at least nine apps, including com.ido.slivercrest, SilverCrest Active, and com.belk.app, belk watch.

Hosts hardcoded in the VeryFit 3.5.0 dex pool: ali-badge.idoocloud.com, cn-badge.idoocloud.com, eu-badge.idoocloud.com, in-badge.idoocloud.com, us-badge.idoocloud.com, ali-buried.idoocloud.com, cn-buried.idoocloud.com, eu-buried.idoocloud.com, in-buried.idoocloud.com, us-buried.idoocloud.com, ali-custom-gateway.idoocloud.com, cn-custom-gateway.idoocloud.com, eu-custom-gateway.idoocloud.com, in-custom-gateway.idoocloud.com, us-custom-gateway.idoocloud.com, ali-device.idoocloud.com, cn-device.idoocloud.com, in-device.idoocloud.com, us.device.idoocloud.com, ali-health.idoocloud.com, cn-health.idoocloud.com, in-health.idoocloud.com, us.health.idoocloud.com, ali-healthmanage.idoocloud.com, ali-iot.idoocloud.com, cn-iot.idoocloud.com, eu-iot.idoocloud.com, in-iot.idoocloud.com, us-iot.idoocloud.com, ali-log.idoocloud.com, cn-log.idoocloud.com, eu-log.idoocloud.com, in-log.idoocloud.com, us-log.idoocloud.com, ali-oss.idoocloud.com, ali-running-api.idoocloud.com, cn-running-api.idoocloud.com, eu-running-api.idoocloud.com, in-running-api.idoocloud.com, us-running-api.idoocloud.com, ali-user.idoocloud.com, cn-user.idoocloud.com, in-user.idoocloud.com, us.user.idoocloud.com, ali-veryfit-h5.idoocloud.com, cn-veryfit-h5.idoocloud.com, eu-veryfit-h5.idoocloud.com, in-veryfit-h5.idoocloud.com, us-veryfit-h5.idoocloud.com, life-content.idoocloud.com, life-cn-content.idoocloud.com, life-in-content.idoocloud.com, life-us-content.idoocloud.com, getdata.veryfitplus.com, cloud.console.veryfitplus.com, cloud.user.veryfitplus.com, life-content.veryfitplus.com.

```
cn-guangzhou.log.aliyuncs.com
unad.oss-accelerate.aliyuncs.com
com.aliyun.sls.android.producer.provider.SLSContentProvider
libsls_producer.so
```

```
com.watch.life        VeryFit
com.sikey.veryfit     VeryFit Kids
com.sport.fitplus1    VeryFit Ultra
com.ido.watch         VerySport
com.ido.weather       VeryFitWeather
com.fitness_ota       Fitness OTA
com.jimi.publicwatch  VF Watch
com.belk.app          belk watch
com.ido.slivercrest   SilverCrest Active
```

Observed fact: the backend scheme above is read from the VeryFit binary. The other eight apps were not downloaded. That they use the same backend is an inference from the shared developer account and is UNVERIFIED. The first notice stated it as a fact for all nine. This report narrows the claim to what the evidence supports. Not shown: whether the region prefix keeps EU users on eu hosts or whether the Guangzhou log endpoint is a default or fallback for users outside China. The operator replied on 18 September 2026 that VeryFit "adopts a region-based data service strategy" and had "scheduled further improvements for an upcoming version to strengthen the handling of regional data and related network requests". It did not answer the question whether Guangzhou is a default or fallback. The operator reports the improvement in v3.7.1. Build 354 is compared below. The first notice rated this HIGH. This report rates it MEDIUM because no transfer was demonstrated.

Build 354 (examined 17 November 2026): all 57 idoocloud.com and veryfitplus.com hosts of the original finding are still compiled in, and 22 further hosts not recorded there are present, among them the regional ai-cs-service and social hosts (ali, cn, eu, in, us), backstage, user, device, health, h5 and healthmanage hosts. No change to regional handling was found in the compiled-in host set. cn-guangzhou.log.aliyuncs.com is no longer present in the dex code, native libraries, resources or assets, which is recorded as not found at the old location, so removal is not established. The Alibaba SLS SDK is still bundled, and a first-party telemetry path exists: TrackingPointProvider in its own process com.ido.event_log with the fields logFileUrl and logType, the base URL https://cloud.user.veryfitplus.com/ and a buriedUrl string in libapp.so. Where these point at runtime is decided by the server.

Operator statement of 18 November 2026: unad.oss-accelerate.aliyuncs.com "is called after SDK initialization and is used only to retrieve advertising configuration" and "does not upload user data"; eu-central-1.log.aliyuncs.com "is used to upload advertising event tracking data, which is stored in Germany." The Guangzhou endpoint was not found in build 354, and the operator is still verifying its historical use and whether it was removed, replaced or delivered at runtime. The values and regional destinations of logFileUrl and buriedUrl "require further technical confirmation." Stated by the operator, not verified by RFI-IRFOS. The question whether Guangzhou was a default for users outside China remains open.

China Mobile health assist (not named in the notice): build 354 contains an integration that calls https://ivs.chinamobiledevice.com:11443/ (v2/customer/device/secret/info and v2/customer/device/report). AlarmBroadReceiver.cmccReport runs when the paired watch supports it and the operator's server has delivered a configuration. In the lines read, the report call carries device information and no health values, and the full field list was not decoded. No region gate was found. The operator states on 18 November 2026 that the function is designed exclusively for the Chinese market and that the associated devices can only be used in China. Stated by the operator, not verified. The operator is still checking the data fields and reporting conditions.

GDPR: Art. 44, Art. 46, Art. 13(1)(f), Art. 5(1)(a)

Impact: Health, device and event data of EU users may be handled on infrastructure in mainland China, and a person who buys a retailer-branded watch may be on the same platform without knowing it. Which of these is true for an EU user was not tested.

Fix: State which region serves each user, document that EU accounts never write to cn or ali hosts or to the Guangzhou log service, and name the Art. 46 mechanism for any transfer that does occur.

M2: Four Google and Gaode API keys and Firebase project identifiers are hardcoded in the distributed package, and a named SDK is absent from the binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), severity unchanged from the first notice. Operator answered 2026-11-16, build 354 examined 2026-11-17

resources.arsc holds two Google API keys, a Gaode (Amap) key and the Firebase project identifiers. All are extractable with aapt2 from any download. The privacy policy also names Tencent Bugly as a crash-reporting SDK, and a targeted search across all 14 dex files found no com/tencent/bugly namespace.

```
google_api_key                AIzaSyCwwIDwX3W7EvI25cCgMQxGkf1Tt7D9nrg
google_crash_reporting_api_key  AIzaSyCwwIDwX3W7EvI25cCgMQxGkf1Tt7D9nrg
google_map_key                AIzaSyAXGbXeJiZER6o06WTBl7nh8D6lkY7w234
gaode_map_key                 2b391362f8bac7bcf61a50f500347399
google_app_id                 1:921432128009:android:343815b5fb984aa91e16d8
gcm_defaultSenderId           921432128009
google_storage_bucket         veryfit-ios.appspot.com
project_id                    veryfit-ios
google_client_id              207506948739-*.apps.googleusercontent.com
```

The Firebase and Maps keys are client identifiers. Google does not treat them as secrets, and the reportable risk is availability and integrity (quota and billing exhaustion, event pollution), plus the burden on the operator under Art. 5(2) to show that key restrictions and backend rules are in place. The storage bucket was not touched and is not claimed to be open. No key was tested. The google_client_id value is recorded in the working notes only with a wildcard after the project number, so the full value is not reproduced here. The Amap SDK is wrapped under the operator's own com.ido.map package. The Bugly mismatch reads as stale policy text and not as hidden code, and it is a transparency inaccuracy under Art. 13. The severity is unchanged from the first notice.

Operator statements of 16 November 2026: the Google Maps key is restricted to the package com.watch.life and the SHA-1 of the release certificate, and the Google API key has no separate API allowlist. "No separate per-key usage quota or spending limit has been configured." "Firebase App Check is not currently enabled or enforced," and the client integrates neither App Check nor Play Integrity. The Gaode key is restricted by package name and SHA-1, has no API allowlist or quota, and is used only in the China-market version. On 18 November 2026 the operator refers to this answer and reports no further change. Build 354 (examined 17 November 2026): the key values are identical to those recorded above, so no key was rotated. In the Google Play build MapHelper.getMapSource() logs that the overseas version forces Google Map, BuildConfig.IS_FOREIGN is true and the Amap branch is not taken, while the Gaode key and the com.amap classes remain in the package. The package name and SHA-1 values can be read from the public APK, and without an API allowlist the key is valid for every API enabled in the project. The restrictions are stated by the operator, not verified by RFI-IRFOS.

GDPR: Art. 32(1)(b), Art. 5(2), Art. 13

Impact: Anyone can read the keys from the public app. The effect on users is indirect: analytics and map services could be disrupted or polluted, and a policy that names an SDK the app does not contain makes the recipient list harder to trust.

Fix: Restrict each key by package name and signing certificate, enforce App Check for Firebase, review the storage bucket rules for veryfit-ios.appspot.com, and bring the policy's SDK list in line with the build.

H2: A broad dangerous-permission block for a watch and scale companion app, with each permission traceable to a disclosed feature

---

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), reassessed from HIGH in the first notice

The manifest declares SEND_SMS, READ_SMS, RECEIVE_SMS, READ_CALL_LOG, ANSWER_PHONE_CALLS, CALL_PHONE, READ_PHONE_STATE, READ_CONTACTS, CAMERA, RECORD_AUDIO, precise and background location, BODY_SENSORS, ACTIVITY_RECOGNITION, READ_LOGS, WRITE_SETTINGS, QUERY_ALL_PACKAGES and the Health Connect read and write set, more than 60 entries in all.

- SEND_SMS traces to the fall-detection SOS feature (IFallingDetectionView, EmergencyContactsPresenter, setEmergencyContactsV3).
- READ_SMS and RECEIVE_SMS trace to notification mirroring to the watch, which the policy describes.
- READ_CONTACTS, READ_CALL_LOG and ANSWER_PHONE_CALLS trace to the Call Reminder feature (CallReminderActivity.startSyncContact).
- CAMERA traces to the remote shutter feature (M1).
- READ_LOGS cannot be granted to a normal install, so it reads as a template-inherited declaration and not a working capability.
- The HelloDaemon library registers boot receivers for process persistence, in line with a multi-vendor push stack.

Not shown: whether SMS content, call-log entries or synced contacts reach the operator's backend in addition to the local Bluetooth link. The policy says device information is stored locally and uploaded to the server. The first notice rated this HIGH. This report rates it LOW because every permission traces to a disclosed feature and no transmission was shown. The aggregate remains worth a data minimisation review.

GDPR: Art. 5(1)(c), Art. 25(1)

Impact: A person deciding whether to grant telephony, contacts and location to a watch app sees one block of permissions and not the feature behind each. The risk to them depends on what leaves the phone, which was not measured.

Fix: Request each permission at the moment its feature is first used, document the data flow for each in the policy, and remove READ_LOGS and any permission without a working feature.

M1: A paired watch can trigger the phone camera (bleControlTakePhoto)

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), reassessed from MEDIUM in the first notice

A dialog TakePhotoControlDialog and a handler bleControlTakePhoto let the paired watch or band command the phone to take a photo. This is a disclosed remote shutter feature of the kind many wearables ship.

```
Lcom/ido/life/dialog/TakePhotoControlDialog;
bleControlTakePhoto
com.ido.life.dialog.TakePhotoControlDialog$initUI$1
com/ido/life/imgpicker/process/TakePhotoProcessor
```

Not shown: whether the trigger can only originate from the physically paired Bluetooth device or whether a backend-relayed command can also arm it. That is UNVERIFIED. The first notice rated this MEDIUM. This report rates it LOW because a disclosed feature is the only evidence.

GDPR: Art. 25(1), Art. 32(1)

Impact: If the trigger were reachable by anyone other than the paired device, the phone camera could be used to capture a person nearby. Nothing in the package shows that it can.

Fix: Document that only the bonded device can send the command, and show in the policy whether any server-side path exists.

M3: PEGI 3 rating and a date of birth that feeds an algorithm and does not gate access, against a policy that excludes under-16s

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), reassessed from MEDIUM in the first notice

The Play listing carries PEGI 3. Account creation collects a date of birth. The policy says the products are not available to children under 16 (or 13 in some jurisdictions) and that collected data of a child will be deleted. No app-level age check or date-of-birth block was found in the dex pool apart from ad SDK flags that the app could set (Vungle COPPA, TagForUnderAgeOfConsent).

The date of birth appears to feed the heart-rate algorithm with age, height and weight, as the policy explains, and not to decide eligibility. PEGI rates content and not data processing. The first notice rated this MEDIUM. This report rates it LOW because the absence of a gate is a statement about what was not found in a string dump and because no minor account was observed.

GDPR: Art. 8, Art. 25(1), Art. 5(1)(c)

Impact: A young person could create an account for a device that records heart rate, blood pressure and cycle data, with no check against the operator’s own rule.

Fix: Use the date of birth to enforce the stated minimum age or state a different rule, and review PEGI and Data Safety answers against the feature set.

M4: The Art. 27 representative contact is a mail-only domain with no reachable website

LOW, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from MEDIUM in the first notice, rated LOW by blast-radius escalation

Section 12 of the privacy policy names services@vatspeed-eu.com and an address in Madrid as the contact for EU users. The domain vatspeed-eu.com has an MX record that routes mail through AWS SES and no A or AAAA record, so no website resolves. RFI-IRFOS sent no mail to the address in the analysis and later copied it on the notice and on every follow-up.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS has no metric for a representative contact and gives 0.0. The finding is rated LOW because the representative is the route for EU data subjects of an app that processes health data on more than 10 million installs. MEDIUM, as disclosed on 23 August 2026, is withdrawn because the address appears to be in use.

A mail-only domain does not prove that the representative is not staffed, and the entity behind it is not independently visible in a company register in the analysis. The operator's own replies of 18 and 23 September, 19 October and 9 November 2026 list the same address among the copied recipients, and no delivery failure was found for any message that carried it. The first notice rated this MEDIUM. This report rates it LOW because the address appears to work and the point is one of verifiability.

GDPR: Art. 27(1), Art. 13(1)(a)

Impact: A person in the Union who wants to exercise a right against a company in Shenzhen has one e-mail address and no way to check who reads it.

Fix: Publish the representative's legal name, registration and a working website or postal contact in the policy and in the Play developer information.

Impact Analysis

- Users of the Family Account feature. Menstrual and ovulation data was part of what a linked family member could be given sight of, with no impact assessment behind the sharing (C3).
- Everyone who installed the app. Nine advertising and analytics components start before a consent choice (C1), the network configuration allows cleartext (C2), and keys are public (M2).
- EU users. Their data may be handled on a platform with hosts in mainland China, and the representative contact cannot be verified from outside (H1, M4).
- Young people. The policy excludes under-16s and the app collects a date of birth without using it as a gate (M3).

The Complete Chain

- 1. A person buys a watch under the VeryFit brand or another brand on the same developer account and installs the app. Nine ad and analytics providers start before any consent screen (C1).
- 2. The app syncs heart, blood pressure, sleep and menstrual data to a cloud platform with regional hosts, and a log endpoint in Guangzhou is hardcoded (H1). The network configuration allows plain HTTP (C2).
- 3. The user links a family member in Family Account. In version 3.5.0 menstrual and ovulation data belongs to the categories handled by that module (C3).
- 4. The operator confirms in writing that no impact assessment was made. It then reports removal of the category in v3.7.1. Build 354 still contains the cycle upload in the Family Account path, and the operator states on 18 November 2026 that sub-account data is no longer retrieved and primary data is not shared. That statement is stated by the operator, not verified.
- 5. The user asks who is responsible. The policy points to a Shenzhen company and a mail-only EU address (M4).

Each later section of this report refers to one of these links. The harm in version 3.5.0 is that the most intimate health data a watch app holds was offered to a second person through a feature that nobody had assessed.

Health Data, Family Sharing & Bystanders

Art. 9(1) GDPR covers data concerning health. Menstrual cycle and ovulation data is reproductive health data and ranks among the most sensitive categories. Sharing it with a second natural person requires a basis under Art. 9(2) of its own, and the information duties of Art. 13 and Art. 14 apply. Art. 35(3)(b) points to a DPIA where special-category data is processed on a large scale. The operator confirmed on 23 September 2026 that none existed for this sharing.

The authorization step the operator describes is the barrier that matters. A generic family-sharing consent is not the same as informed consent to share reproductive health data, and the person who authorizes may be under pressure from the person who asks. The operator did not say what the authorization screen shows. Its answer was to remove the category, which answers the underlying risk more completely than a better screen would. Build 354 still contains the cycle upload in the Family Account path, and the operator’s statement of 18 November 2026 that no sharing remains is not verified by RFI-IRFOS.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a), 5(2)	Transparency and accountability. Policy names an SDK that the build does not contain (M2). Keys without shown controls (M2).
Art. 5(1)(c)	Data minimisation. Permission block and date of birth (H2, M3).
Art. 6(1), 7(1)	Lawful basis and consent before processing. Providers start before the consent form (C1).
Art. 8	Child's consent. No age gate located (M3).
Art. 9(1), 9(2)(a)	Menstrual and ovulation data in Family Account sharing (C3).
Art. 13, 14	Information on recipients, authorization scope and the representative (C3, H1, M4).
Art. 25	Data protection by design. Sharing scope, cleartext, age gate (C3, C2, M3).
Art. 27	Representative of a controller outside the Union (M4).
Art. 32(1)	Security of processing. Cleartext setting and public keys (C2, M2).
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.
Art. 35	DPIA for large-scale special-category sharing. None existed (C3).
Art. 44, 46	Possible transfer to mainland China. Not demonstrated (H1).
ePrivacy Directive Art. 5(3)	Access to information on the terminal device before consent (C1).

Regulatory & Legal Landscape

The operator has no EU main establishment, so the one-stop-shop does not apply and any EU authority may act on a complaint. The Datenschutzbehörde and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: a policy that names the legal entity, an address, per-feature data categories and a GDPR contact is better than most in this wave. The weaker points are the mismatch between policy and build and the representative contact that cannot be verified from outside.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The bundle was obtained from APKPure (apkpure.com/veryfit/com.watch.life, version 3.5.0, versionCode 342).

```
Package       com.watch.life
Version       3.5.0 / versionCode 342
XAPK bundle   295.7 MB
XAPK bundle   SHA-256 f0012a3cc3ac6a5edaae98a20b7c4a39997b8cbe881e58504fbd8f998f666206
base.apk      241,844,382 bytes
base.apk      SHA-256 49672cc94bfe495cb4652456d47c4bfd4bfc00b4aa3f5f187ac133bec2989594
Signing cert  SHA-256 aacc73116501987d86070e47125b6acb588f6f64c6d7579e2c149dd56a59510d
              DN O=ido, L=sz (self-signed)
libVeryFitMulti.so  SHA-256 3
    cfd1ca488c8216adbe99aca21de0e68e252a59a13e5d7461690ba9f6e916a4b
libRtkAesJni.so     SHA-256 8
    f1310eeb4b697ac6e56bbac92ab81c56165a53ac66144cdd1e781aa05c03314
Google project veryfit-ios, sender 921432128009
              app 1:921432128009:android:343815b5fb984aa91e16d8
              google_api_key AIzaSyCwwIDwX3W7EvI25cCgMQxGkf1Tt7D9nrg
              google_map_key AIzaSyAXGbXeJiZER6o06WTBl7nh8D6lkY7w234
Gaode (Amap)  2b391362f8bac7bcf61a50f500347399
Storage       veryfit-ios.appspot.com
```

```
https://idoocloud.com (region hosts listed in H1)
https://veryfitplus.com: getdata, cloud.console, cloud.user, life-content
cn-guangzhou.log.aliyuncs.com
unad.oss-accelerate.aliyuncs.com
vatspeed-eu.com (MX only, mail through inbound-smtp.eu-west-1.amazonaws.com)
```

```
Operator contacts  ido@idoocn.com, app_pmteam@idoocn.com, services@vatspeed-eu.com
Postal address     No. 1 Lirong Road, Xinshi Community, Dalang Street, Longhua
    District, Shenzhen 518000, China
Representative     Calle Antonio Salvador N99. 1, 28026 Madrid, Spain (per the privacy
     policy)
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 3.5.0. Notice REF VERYFIT-2026-R1 sent to ido@idoocn.com, copied to the Play-listed contacts, the representative address, the Datenschutzbehörde and the EDPS. Three written questions.
2026-09-12	Follow-up on the same thread, 20 days after the notice.
2026-09-18	First written reply from the VeryFit team (app_pmteam@idoocn.com), 26 days after the notice. It acknowledges consent timing and regional configuration as areas to improve and says Family Account access needs authorization by the linked account. RFI-IRFOS replies the same day and asks for version targets, for the text of the authorization screen and for the DPIA status.
2026-09-23	Operator names v3.7.0, targeted for mid-November 2026, for consent timing and regional handling, confirms that no DPIA, PIA or similar assessment of the sharing was conducted, and plans removal of menstrual and ovulation data from Family Account in v4.0.0 (Q1 2027). RFI-IRFOS asks about the interim period and the release date. A second reply the same day says an interim server-side removal is not possible without client changes and that v3.7.0 should be fully released before 21 November 2026.
2026-10-17	Reminder, 35 days before publication. RFI-IRFOS asks for the build version name and versionCode, for an in-app notice and for early notice of a schedule change.
2026-10-19	Operator decides to stop the menstrual and ovulation sharing in v3.7.0 instead of v4.0.0 and says it will send the version name and versionCode on submission. RFI-IRFOS records the earlier date the same day.
2026-11-09	Operator writes that the release shipped as v3.7.1, not v3.7.0, with a staged rollout on App Store and Google Play from 2026-11-07, containing the changes for consent timing, regional handling and the Family Account removal. No versionCode is given.
2026-11-14	All fix statements up to this date are the operator's. No bounce received for any message.
2026-11-15	RFI-IRFOS sends a follow-up on the disclosure (13:01 UTC, from s.kepp@rfi-irfos.com), 84 days after delivery of the notice, with three questions on the cleartext configuration, the API keys and the version.
2026-11-16	Operator reply (09:45 UTC). Names Android 3.7.1, versionCode 354, and iOS 3.7.1, build 26110610, both fully released. States that cleartext is removed app-wide with retained allowlist entries that cannot be listed, that the Google key has a package and SHA-1 restriction, no API allowlist, no quota and no App Check, and that the Gaode key is used only in the China-market version.

Date	Event
2026-11-17	RFI-IRFOS sends the examination of build 354 (09:40 UTC, from security@rfi-irfos.com), four days before publication. It records confirmed fixes for the cleartext base configuration, the Firebase and Google providers and the Gaode branch. It reports the cycle upload still present, the eleven-entry allowlist, the remaining advertising providers and the CMCC integration, and asks five questions.
2026-11-18	Operator reply (08:22 UTC). Remaining SDK initialization and consent work, the reduction of the cleartext exceptions to two domains and the removal of getdata.veryfitplus.com:8011 are planned for version 3.8.0. States that sub-account menstrual data is no longer retrieved and that no sharing remains. Names the purpose of two regional endpoints, reports that the Guangzhou endpoint was not found in build 354 and restricts the CMCC function to China.
2026-11-21	Publication of this final report, 90 days after delivery of the notice. Embargo date reached. No request to extend the embargo was received.

The operator received the same embargo date in every message. No request to extend it was made and none was granted.

What VeryFit Got Right

- The operator answered in writing seven times and gave dated version targets, including a plan for 3.8.0.
- It said plainly that no DPIA, PIA or similar assessment of the Family Account sharing was conducted.
- It decided to remove the sensitive category from sharing and brought that change forward from the first quarter of 2027 to November 2026, and it explained a version-number change when the release shipped as v3.7.1.
- The app bundles a real consent platform (Google UMP and an IAB TCF v2 decoder), so the consent problem is one of timing and not of absence.
- The privacy policy is specific. It names the legal entity, a physical address, per-feature data categories and an EU contact.
- The notification listener service is protected by the system BIND_NOTIFICATION_LISTENER_SERVICE permission, and SQLCipher protects the local database as the policy describes.
- Build 354 removes the app-wide cleartext permission and gates the Firebase and Google providers behind the privacy agreement, as the operator stated.

Residual Risk & Recommendations

Findings stay open to the extent that build 354 does not close them, as set out in the status table. Versions after 3.7.1 are not covered by this report. The operator plans version 3.8.0 without a release date.

- Publish a date for version 3.8.0 and ship the planned changes for the remaining SDKs and the cleartext exceptions.
- Show that no advertising or analytics SDK sends a request before a recorded consent decision.
- Confirm that menstrual and ovulation data is no longer uploaded to or readable by linked accounts, and that earlier shared copies are gone.
- Reduce the cleartext exceptions as planned for 3.8.0, remove the endpoint getdata.veryfitplus.com:8011 and pin the operator’s own endpoints.
- Document which region serves each user and whether the Guangzhou log service is used for EU accounts.
- Restrict the client keys and align the SDK list in the policy with the build.
- Publish a verifiable representative contact in the Union.

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 Root level code analysis of the published application and public pages. No VeryFit servers or accounts were probed and no key was tested. Fix statements are the operator’s and are stated by the operator, not verified by RFI-IRFOS, except where the examination of build 354 is named. Severity per CVSS v4.0 (CVSS-B) with explicit escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF VERYFIT-2026-R1.