Security & Privacy Disclosure, Final Report

OnWear Pro for Android (com.linwear.top)

No consent platform, cleartext allowed in two files, a paid speech feature next to Chinese speech endpoints, and nine other brands compiled into one package, with no reply since the notice.

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

Target	OnWear Pro (Play developer Watch Tech Dev, listed entity Shenzhen Guangzhui Investment Partnership, Limited Partnership)
Versions Audited	1.5.1.35 / versionCode 335 (Play update 2026-07-30, analysed 2026-08-22)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	11: 2 High, 4 Medium, 3 Low, 2 Info (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`5cfe9d781f4f51e2a46cd0c062c93921cc7909a86544bef4d857a4095c347f08`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 7

6.1 C1: Firebase and Google Mobile Ads construct at process start and no consent management platform exists anywhere in the package . . . 7

6.2 C2: Cleartext traffic is permitted globally by two configuration files while the Data Safety card says data is encrypted in transit and not shared with third parties 8

6.3 H1: A paid meeting transcription feature sits next to hardcoded iFlytek and Baidu speech endpoints and a cluster of Chinese SDK packages, and the Play listing names none of it . . . 9

6.4 H2: One exported receiver for SMS, call state and outgoing calls and a notification listener put the data of people who never installed the app into the paired watch pipeline . . . 10

6.5 H3: Menstrual cycle, ovulation and other health tracking ships in 9 or more languages on the same architecture as C1 and C2, in an app rated PEGI 3 . . . 11

6.6 S1: Backend hostnames of at least nine unrelated consumer brands are compiled into the package and the operator's two domains share one load balancer 12

6.7 M1: The operator's policy admits self start and continuous background location tracking at "a certain frequency" . . . 13

6.8 M2: The package declares QUERY_ALL_PACKAGES, which gives visibility into every installed app . . . 13

6.9 M3: More than 80 declared permissions, including legacy and duplicate entries, indicate an unpruned merged SDK toolkit . . . 14

6.10 M4: The privacy policy is dated 11 August 2021 and the analysed build dates from July 2026 . . . 14

6.11 M5: PEGI 3 rating against SMS, call and contact access and reproductive health tracking, with no age gate in the resources . . . 15

7 Impact Analysis 15

8 The Complete Chain 16

9 Backend Domain Cluster and Fingerprint Keys 16

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 18

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 21

Executive Summary

OnWear Pro is a companion app for the Bluetooth watch hardware LW61 with more than 1 million downloads on Google Play. The listed developer entity is [redacted], an investment partnership in Shenzhen. The Play page shows the developer name Watch Tech Dev, the rating PEGI 3 and a Data Safety card. On 23 August 2026 RFI-IRFOS sent a notice with REF ONWEARPRO-2026-R1 to liaoweilong@linwear.com and yishuzhang888@gmail.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 1.5.1.35 shows that Firebase and Google Mobile Ads construct at process start and that no consent management platform exists in the package (C1). Two network security configuration files permit cleartext traffic for every host, while the Data Safety card says data is encrypted in transit and not shared with third parties, and the operator's own policy names AdMob and Facebook audience sharing (C2). Reproductive health tracking ships in many languages on the same architecture (H3). A paid meeting transcription feature sits beside hardcoded iFlytek and Baidu speech endpoints and the listing names none of it (H1). The app relays SMS, call and notification data of third parties to the watch (H2). The package also holds backend hostnames of nine other consumer brands, and the operator's two domains share one load balancer (S1).

A reassessment by CVSS v4.0 band puts two findings at High, four at Medium and three at Low, with two informational entries. The two Critical labels of 23 August 2026 move down because the package shows configuration and file content and not runtime behaviour. Four more labels move down for the same reason. H3 stays High through a stated blast-radius escalation. Whether any value leaves the phone, and where it goes, is UNVERIFIED throughout.

The operator did not reply to the notice of 23 August 2026, the follow-up of 12 September 2026 or the follow-up of 17 October 2026. No bounce was received. This report is published on the embargo date of 21 November 2026 and records the state of the correspondence on 21 November 2026.

Scope: Root level code analysis of the Google Play release 1.5.1.35 (versionCode 335). The package was obtained as an XAPK bundle (207,417,146 bytes, base APK plus arm64-v8a, English and mdpi splits) from the APKPure mirror and checked against the package name, title and developer on the live Google Play listing. The Play update date is 30 July 2026. Work done: a resources only decode with apktool, no source decode, the manifest, string and network configuration files, and a string extraction across the nine classes*.dex files (about 75 MB combined) for class packages and hostnames. A DNS lookup of the operator's own domains was done to see which load balancer they point to. The live Google Play listing and the operator's English policy were read on 22 August 2026. The app was not installed, no account was created, no operator server was called and no traffic was captured. No bytecode pass was done and no dynamic analysis. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	MEDIUM	Firebase and Google Mobile Ads construct at process start and no consent management platform exists anywhere in the package
C2	HIGH	Cleartext traffic is permitted globally by two configuration files while the Data Safety card says data is encrypted in transit and not shared with third parties
H1	MEDIUM	A paid meeting transcription feature sits next to hardcoded iFlytek and Baidu speech endpoints and a cluster of Chinese SDK packages, and the Play listing names none of it
H2	MEDIUM	One exported receiver for SMS, call state and outgoing calls and a notification listener put the data of people who never installed the app into the paired watch pipeline
H3	HIGH	Menstrual cycle, ovulation and other health tracking ships in 9 or more languages on the same architecture as C1 and C2, in an app rated PEGI 3
S1	INFO	Backend hostnames of at least nine unrelated consumer brands are compiled into the package and the operator’s two domains share one load balancer
M1	MEDIUM	The operator’s policy admits self start and continuous background location tracking at ”a certain frequency”
M2	LOW	The package declares QUERY_ALL_PACKAGES, which gives visibility into every installed app
M3	INFO	More than 80 declared permissions, including legacy and duplicate entries, indicate an unpruned merged SDK toolkit
M4	LOW	The privacy policy is dated 11 August 2021 and the analysed build dates from July 2026
M5	LOW	PEGI 3 rating against SMS, call and contact access and reproductive health tracking, with no age gate in the resources

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Network activity before consent not shown.
C2	CRITICAL	HIGH	No reply. Plain HTTP use not listed, sharing contradiction proven by the policy.
H1	HIGH	MEDIUM	No reply. Audio routing to the named hostnames not observed.
H2	HIGH	MEDIUM	No reply. Disclosed core feature, backend path not shown.
H3	HIGH	HIGH	No reply. Features proven, storage and transmission not shown.
S1	HIGH	INFO	No reply. Structural observation, liveness of brand domains not shown.
M1	MEDIUM	MEDIUM	No reply. Disclosed in the policy.
M2	MEDIUM	LOW	No reply. Capability only.
M3	MEDIUM	INFO	No reply. Hygiene indicator, no live effect.
M4	MEDIUM	LOW	No reply. Date of the policy proven.
M5	MEDIUM	LOW	No reply. Age gate not found in resources.

The findings file of 22 August 2026 labels C1 and C2 as Critical, H1 to H3 and S1 as High and M1 to M5 as Medium. The report uses the CVSS v4.0 band of each finding. H3 stays High through a blast-radius escalation that the finding states. S1 and M3 are structural observations without a score.

Subject & Operator Analysis

The Google Play page lists the developer entity as [redacted] (Shenzhen Guangzhui, literally Light Cone, Investment Partnership, Limited Partnership), 2010 Overseas Friendship Building, 12 Yingchun Road, Jiabei Community, Nanhu Street, Luohu District, Shenzhen, Guangdong, 518000, People's Republic of China. The developer name shown on the page is Watch Tech Dev. An investment partnership is a legal form more often used in China as a holding vehicle than as an operating company. That is not a finding. It is noted for the question of who operates the app. A mobile phone number is published on the listing and is not reproduced here.

The support contact on Google Play is yishuzhang888@gmail.com, a personal mailbox. The privacy policy names liaoweilong@linwear.com as the contact for rights requests and promises an answer within one month. The policy is hosted at m.linwear.top, a page of the operator's domain linwear.top. The Play page also lists three sibling apps under the same developer, Ultima Smart, Monster Fit and OnWear.

The signing certificate is the Google Play App Signing certificate with the generic DN CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US, and does not identify the developer. No Data Protection Officer and no Article 27 representative is named in the listing, the policy or the package. The Austrian Datenschutzbehörde receives the notice in copy and can receive complaints directly.

Architecture & Data Flow

OnWear Pro is a native Android app with nine classes*.dex files (about 75 MB combined) and an arm64-v8a native split. The native stack holds FFmpeg, the Opus codec, two chipset toolkits, the Jieli authentication and OTA libraries and the Realtek audio, codec and AES libraries, and libxcrash for crash reporting. A library named libslm_m1_crack.so is present and its function was not identified, so it is UNVERIFIED. The BLE layer is com.szfission.wear.sdk on cn.wandersnail.bluetooth. The app carries 202 activities, 43 services, 14 receivers and 11 providers.

The app talks to the watch over Bluetooth Low Energy and receives phone events through the broadcast receiver and the notification listener (H2). The policy names two upload targets, api.watch-devs.com and api.linwear.top. Both are DNS verified aliases of Alibaba Cloud load balancers (S1). The dex strings hold region sharded endpoints for China, Europe, Singapore and India. Speech features point to iFlytek and Baidu endpoints, and an AI voice assistant points to Microsoft Azure OpenAI endpoints (H1). No data flow was observed.

Engagement Summary

The notice REF ONWEARPRO-2026-R1 was sent on 23 August 2026 at 00:04 UTC from rfi.irfos@gmail.com to liaoweilong@linwear.com and yishuzhang888@gmail.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried the findings, a statement of what the app does well and three questions. A follow-up of 12 September 2026 at 17:05 UTC restated the findings and asked the three questions with an answer date of 26 September 2026. A second follow-up of 17 October 2026 at 19:06 UTC came from security@rfi-irfos.com under the subject 35 days to publication: OnWear Pro. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: Firebase and Google Mobile Ads construct at process start and no consent management platform exists anywhere in the package

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

AndroidManifest.xml lines 459 and 461 register FirebaseInitProvider and MobileAdsInitProvider with initOrder 100. Android constructs both at process start, before any activity and so before any consent screen can render. The Firebase provider also carries directBootAware="true", which allows it to run before the device is unlocked. A search of res/values/strings.xml and of all nine classes*.dex files for OneTrust, Didomi, Usercentrics and the IAB TCF markers IABTCF_ and ConsentInformation returned no match. No consent management platform exists, so there is nothing that could hold the SDKs back. What these SDKs send before consent was not observed and is UNVERIFIED.

```
<provider android:authorities="com.linwear.top.firebaseinitprovider" android:
    directBootAware="true"
  android:exported="false" android:initOrder="100" android:name="com.google.firebase.
    provider.FirebaseInitProvider"/>
<provider android:authorities="com.linwear.top.mobileadsinitprovider" android:exported
    ="false"
  android:initOrder="100" android:name="com.google.android.gms.ads.
    MobileAdsInitProvider"/>
```

Impact: A person who opens the app for the first time has no way to refuse advertising and analytics SDKs, because the app contains no mechanism to ask. The Play listing shows in-app purchases and the policy names AdMob for advertising placement.

Fix: Delay SDK initialisation until a recorded consent decision and add a consent management platform.

C2: Cleartext traffic is permitted globally by two configuration files while the Data Safety card says data is encrypted in transit and not shared with third parties

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

res/xml/network_security_config.xml and res/xml/sm_network_security_config.xml both set cleartextTrafficPermitted="true" at base-config level, without per-domain exceptions and without a pin-set. The second file is bundled by the Tenmeter H5 game SDK (com.tenmeter.smlibrary). The app targets API level 36, where cleartext HTTP is refused by default, so the files switch that protection off for every host. The live Data Safety card of 22 August 2026 says: No data shared with third parties, Data is encrypted in transit. The operator's own policy contradicts the first statement. It says that the operator may share certain information with Facebook to create Custom or Lookalike Audiences, and its third party SDK section names AdMob and describes the collection of IMEI, Android ID, OAID, MAC address, IP address and location for advertising placement. The manifest holds the AdMob application ID below. The second statement is contradicted by the configuration only to the extent that plain HTTP is used. The policy names HTTPS addresses as upload targets and the endpoints that use plain HTTP could not be listed, so actual use of plain HTTP is UNVERIFIED.

```
<!-- res/xml/network_security_config.xml -->
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>

<!-- res/xml/sm_network_security_config.xml, bundled by com.tenmeter.smlibrary -->
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors><certificates src="system" /></trust-anchors>
    </base-config>
</network-security-config>
```

```
Google Mobile Ads application ID, AndroidManifest.xml line 230:
ca-app-pub-6157032906860767~8366748906
Policy: "User data is uploaded to https://api.watch-devs.com / https://api.linwear.top
    "
Policy: "we may share certain information with Facebook that allows us to create
    Custom or Lookalike Audiences"
```

Impact: More than 1 million installers rely on a card that says nothing is shared and that data is encrypted in transit. The same app handles SMS content, call numbers, location, contacts, camera data and health data including a menstrual cycle, and the transport settings allow anyone on the network path to read unencrypted traffic if it occurs.

Fix: Remove both cleartext allowances, pin first party hosts, and correct the Data Safety declaration to name the advertising and Facebook audience sharing that the policy describes.

H1: A paid meeting transcription feature sits next to hardcoded iFlytek and Baidu speech endpoints and a cluster of Chinese SDK packages, and the Play listing names none of it

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 (CVSS-B), disclosed as HIGH on 23 August 2026

The dex strings of all nine classes*.dex files contain the class packages in the table below and the hostnames after it. res/values/strings.xml holds a localized feature Speech Transcription (public_meeting_voice_transcription) with a billing string: the transcription time is paid according to the audio time, with seconds as the minimum settlement unit. The Play description never mentions the feature. The manifest declares RECORD_AUDIO three times and the package carries FFmpeg, Opus and a Realtek audio capture SDK. The hostnames include duer-kids.baidu.com, the domain of a Baidu children directed voice assistant platform, in an app rated PEGI 3. Whether the app calls it is UNVERIFIED. A separate feature, the AI Voice Assistant (public_ai_voice_assistant), points to Microsoft Azure OpenAI endpoints and is not part of the transfer question. That audio from the transcription feature is sent to the named hostnames, and from where, was not observed and is UNVERIFIED.

Vendor	Class package	Dex string hits
Tencent	Lcom/tencent/mm/opensdk/* (WeChat OpenSDK), Lcom/tencent/mmkv/MMKV	264
Alibaba	Lcom/alibaba/aliagentsdk/* (IAliBt, IJustDataTransportAliBt, IBtDataUploadCallback), Lcom/alibaba/android/arouter/*	110
Baidu	Lcom/baidu/mapapi/*, Lcom/baidu/location/*	97
Huawei	Lcom/huawei/hms/*, Lcom/huawei/agconnect/*	842 and 68

```
iat-api.xfyun.cn   iat-niche-api.xfyun.cn   tts-api.xfyun.cn
vop.baidu.com   tsn.baidu.com   aip.baidubce.com   openapi.baidu.com
openapi-iot.baidu.com   sandbox.iot.baidu.com   duer-kids.baidu.com

Azure OpenAI endpoints of the AI Voice Assistant (not part of the transfer question):
ashgpt.openai.azure.com   ceswatch.openai.azure.com   twhisper.openai.azure.com
```

```
public_meeting_voice_transcription  "Speech Transcription"
"The transcription time can be used for audio transcription of meeting minutes. The
    transcription time is paid according to the audio time, with seconds as the
    minimum settlement unit."
```

Impact: A buyer who pays by the second for meeting transcription does not learn from the listing that the feature exists, and cannot learn where the voices of the people in the meeting go. Meeting content can contain special category data of people who never installed the app.

Fix: Name the feature, the recipient and the country in the listing and the policy, state the Chapter V mechanism and complete a data protection impact assessment.

H2: One exported receiver for SMS, call state and outgoing calls and a notification listener put the data of people who never installed the app into the paired watch pipeline

---

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 23 August 2026

AndroidManifest.xml lines 140 to 165 register CustomBroadcastReceiver for android.provider.Telephony.SMS_RECEIVED, android.intent.action.PHONE_STATE and android.intent.action.NEW_OUTGOING_CALL, and CustomNotificationListenerService with the BIND_NOTIFICATION_LISTENER_SERVICE permission. The Play description says the app pushes SMS, numbers and messages from different applications to the watch, so this is the disclosed core feature. The receiver is exported without a permission attribute. The three actions are protected system broadcasts that only the operating system can send, so the exported flag alone is not an injection risk and the report does not claim one. The senders of SMS, the parties of calls and the senders of every mirrored notification are people who never consented to anything. Whether the content stays on the Bluetooth link or also reaches api.linwear.top or api.watch-devs.com is UNVERIFIED. Independent of transmission, who messages the user, how often and through which app can be derived from notification mirroring alone.

```
<provider android:authorities="com.linwear.top" android:exported="true"
  android:name="com.lw.commonsdk.provider.YDBlecontentProvider" android:
    protectionLevel="signature"/>
<service android:exported="true" android:label="OnWear Pro"
  android:name="com.lw.commonsdk.notification.CustomNotificationListenerService"
  android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
    NotificationListenerService"/></intent-filter>
</service>
<receiver android:enabled="true" android:exported="true" android:name="com.lw.
    commonsdk.receiver.CustomBroadcastReceiver">
    <intent-filter>
        <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
        <action android:name="android.intent.action.PHONE_STATE"/>
    </intent-filter>
    <intent-filter><action android:name="android.intent.action.NEW_OUTGOING_CALL"/></
    intent-filter>
</receiver>
```

Impact: Friends, family and colleagues of the user are processed without knowing it and the operator cannot realistically inform them under Art. 14.

Fix: State in the policy what happens to relayed message and call data, keep it on the device and limit the listener to the apps that the watch feature needs.

H3: Menstrual cycle, ovulation and other health tracking ships in 9 or more languages on the same architecture as C1 and C2, in an app rated PEGI 3

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 (CVSS-B), disclosed as HIGH on 23 August 2026, rated HIGH by blast-radius escalation

res/values/strings.xml holds the shipped and localized interface strings en_female_health, en_menstrual_period and en_ovulation. The R1 pass found them localized into at least eight further languages, among them Arabic, Chinese, Czech, German, Spanish and French. The manifest declares the Health Connect write permissions WRITE_HEART_RATE, WRITE_OXYGEN_SATURATION, WRITE_SLEEP, WRITE_STEPS, WRITE_DISTANCE, WRITE_ACTIVE_CALORIES_BURNED and WRITE_WEIGHT, and BODY_SENSORS and ACTIVITY_RECOGNITION. Reproductive health data is special category data by nature under Art. 9. It is processed inside the app that holds C1 (no consent gate before SDK start) and C2 (cleartext permitted, no pinning). What the app stores or sends for these features was not observed and is UNVERIFIED. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.9 to HIGH because the data is reproductive health data of the kind that Art. 9 protects most, the app has more than 1 million installs, the localized interface shows the feature is a full product feature, and no consent mechanism of any kind exists in the package.

```
en_female_health = "Female health"
en_menstrual_period = "Menstrual period"
en_ovulation = "Ovulation"

android.permission.health.WRITE_HEART_RATE, WRITE_OXYGEN_SATURATION, WRITE_SLEEP,
WRITE_STEPS, WRITE_DISTANCE, WRITE_ACTIVE_CALORIES_BURNED, WRITE_WEIGHT
android.permission.BODY_SENSORS, android.permission.ACTIVITY_RECOGNITION
```

Impact: A person who tracks a cycle or ovulation to plan or avoid a pregnancy enters data with acute real world sensitivity. It sits behind the same configuration as step counts, with no consent gate and a transport setting that permits plain HTTP.

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

S1: Backend hostnames of at least nine unrelated consumer brands are compiled into the package and the operator’s two domains share one load balancer

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

The dex strings hold the hostnames below, which share no visible relationship with OnWear Pro. The package does not contain the Bluetrum fingerprint (Lcom/bluetrum/abpartool/*, libabpartool.so) of the HryFine, Wearfit Pro and WearFit2.0 cluster, so OnWear Pro is not a member of that cluster. Its own BLE stack is com.szfission.wear.sdk (294 dex string hits) on cn.wandersnail.bluetooth and cn.wandersnail.commons (186 hits), with the Jieli libjl_* and Realtek libRtk* native libraries. Separately, linwear.top and watch-devs.com are DNS verified to resolve to the identical Alibaba Cloud Application Load Balancer in cn-shenzhen. The package also holds region sharded endpoints (aigc-china, aigc-europe, aigc-singapore, aigc-dev and aigc-pre-release under watch-devs.com and api-china, api-europe and api-india under linwear.top), and api.watch-devs.com resolves to a separate eu-central-1 Alibaba Cloud load balancer. Whether the nine brand domains are live and share user data with this app, or are inert template code, is UNVERIFIED. The finding is a structural observation and a lead and carries no score. The Play page lists three sibling apps under the same developer account, Ultima Smart, Monster Fit and OnWear.

```
10m.com.cn              server.10m.com.cn
ute-tech.com.cn         www.ute-tech.com.cn, ap.ute-tech.com.cn
hetangsmart.com         fitcloud.hetangsmart.com
aicaring.com            api.aicaring.com
aiwatchlw.online        api.aiwatchlw.online, video.aiwatchlw.online
openwearplay.com        www.openwearplay.com
vphband.com             www.vphband.com
yueqizhixiang.com       swapi.yueqizhixiang.com
aieliteai.com.cn        www.aieliteai.com.cn
```

```
linwear.top and watch-devs.com resolve (DNS, 2026-08-22) to  alb-kljiadtutp7b4x569r.cn
    -shenzhen.alb.aliyuncs.com
```

Impact: A user cannot tell from the listing which company controls the data of the app, and the compiled domains show that the same codebase may serve other storefronts.

Fix: State in the policy which entity is controller for which processing and which brands share the backend.

M1: The operator’s policy admits self start and continuous background location tracking at ”a certain frequency”

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The operator’s policy says that the app must use the self starting capability and that there will be a certain frequency of sending broadcasts to wake the app. On location it says that even when the user leaves the OnWear Pro interface or locks the phone, the app can use the background location permission to track the movement path, distance and speed in real time. The manifest declares RECEIVE_BOOT_COMPLETED, REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, ACCESS_BACKGROUND_LOCATION, WAKE_LOCK and SCHEDULE_EXACT_ALARM. The practice is disclosed. A certain frequency is not a number, so the user cannot bound the effect from the text.

```
Policy: "...the app must use the (self-starting) capability, and there will be a
    certain frequency of sending broadcasts through the system to wake up the app's
    self-starting or associated startup behavior."
Policy: "Even if you temporarily leave the OnWear Pro interface to use other
    applications or lock your phone, OnWear Pro can leverage the background location
    permission to track your movement path, distance, speed, and other data in real
    time."
```

Impact: Location tracking continues while the app is not in use and the person cannot predict how often the app wakes.

Fix: State the wake frequency, limit background location to active workouts and let the user switch it off in the app.

M2: The package declares QUERY_ALL_PACKAGES, which gives visibility into every installed app

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), disclosed as MEDIUM on 23 August 2026

AndroidManifest.xml line 38 declares android.permission.QUERY_ALL_PACKAGES. The permission lets the app list every other app on the device. It is disproportionate to the purpose of a companion for a Bluetooth watch and the policy data table does not explain it. Whether the app reads or sends the list was not observed.

```
<uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
```

Impact: The list of installed apps is a fingerprinting aid and reveals sensitive interests such as health, religion or dating apps.

Fix: Remove the permission or narrow the queries to the messaging apps that the notification feature needs.

M3: More than 80 declared permissions, including legacy and duplicate entries, indicate an unpruned merged SDK toolkit

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

The manifest lists more than 80 permissions, among them RESTART_PACKAGES, SET_DEBUG_APP, USE_CREDENTIALS, MOUNT_UNMOUNT_FILESYSTEMS, READ_LOGS, DISABLE_KEYGUARD, com.android.launcher.permission.READ_SETTINGS and WRITE_SETTINGS, and RECORD_AUDIO declared three times by three bundled SDKs. The package declares 202 activities, 43 services, 14 receivers and 11 providers. The legacy entries have no live effect on current Android versions, so the finding supports the white label toolkit reading of S1 and does not describe an exposure.

```
RESTART_PACKAGES, SET_DEBUG_APP, USE_CREDENTIALS, MOUNT_UNMOUNT_FILESYSTEMS, READ_LOGS
    , DISABLE_KEYGUARD,
com.android.launcher.permission.READ_SETTINGS, com.android.launcher.permission.
    WRITE_SETTINGS
RECORD_AUDIO (lines 117 to 119, three declarations)
```

Impact: The app presents a larger permission surface than a single purpose companion needs.

Fix: Prune permissions and components per brand build.

M4: The privacy policy is dated 11 August 2021 and the analysed build dates from July 2026

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026

The policy at https://m.linwear.top/private-policy/en/onwearprocompany/1/1 carries the header Last Updated: August 11, 2021. The analysed build of 30 July 2026 adds Health Connect write permissions, an AI voice assistant, a paid meeting transcription feature, WeChat Pay and Alipay integrations and the SDK cluster of H1. The policy data table is broad enough to cover most of these nominally, so the finding concerns the currency and accuracy of the information and not a proven gap in coverage. The policy contact is liaoweilong@linwear.com, which differs from the Play contact yishuzhang888@gmail.com.

```
Last Updated: August 11, 2021
Policy URL   https://api.linwear.top/manual/privacyPolicyCustom?appType=13  resolves
    to  https://m.linwear.top/private-policy/en/onwearprocompany/1/1
```

Impact: A reader cannot tell whether the policy describes the current app.

Fix: Revise the policy for the current feature set and show a current revision date.

M5: PEGI 3 rating against SMS, call and contact access and reproductive health tracking, with no age gate in the resources

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

The Play listing carries PEGI 3. A resource search found no date of birth field, no parental gate and no age check. The feature set (SMS and call relay, notification mirroring, menstrual and ovulation tracking) addresses an adult population. The dex was not searched for a server side age check beyond the resource pass, so the absence of an age gate is limited to the resources.

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

Impact: A child can install an app rated for everyone that offers reproductive health tracking.

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

Impact Analysis

The people affected are the more than 1 million installers, who wear a watch, grant Bluetooth, location, phone, SMS, contacts, camera, microphone and notification access, and some of whom log a menstrual cycle or ovulation. Some may be children, since the Play rating is PEGI 3. Senders of SMS and notifications and parties of calls are affected as well and never installed the app.

The weight of the case sits on four points. No consent platform exists and advertising and analytics SDKs start with the process (C1). The configuration permits plain HTTP for every host and the Data Safety card says the opposite (C2). Reproductive health tracking ships on that architecture (H3). A paid transcription feature sits beside Chinese speech endpoints and is absent from the listing (H1).

What the package shows is configuration, file content and the operator’s own text. No health reading, voice recording or message was observed leaving a device and the report asserts no such flow. Both the policy and the DNS results show that the operator’s backends are on Alibaba Cloud, one in cn-shenzhen and one in eu-central-1.

The Complete Chain

Step 1, listing: the user reads a Data Safety card that says nothing is shared and that data is encrypted in transit (C2).

Step 2, first start: Firebase and Google Mobile Ads construct at process creation and no consent platform exists (C1).

Step 3, pairing and use: the user grants Bluetooth, location, phone, SMS, contacts and notification access. The receiver and the listener relay the data of third parties to the watch (H2). Health features record a menstrual cycle and ovulation (H3). The meeting transcription feature is paid by the second (H1).

Step 4, backend: the policy names api.watch-devs.com and api.linwear.top as upload targets. The configuration permits plain HTTP (C2). Chinese speech endpoints are compiled into the package (H1). Brand domains of other products are compiled into the same package (S1).

Step 5, persistence: the app wakes itself and tracks location in the background at a frequency that it does not state (M1).

Backend Domain Cluster and Fingerprint Keys

The package does not belong to the Bluetrum cluster of HryFine, Wearfit Pro and WearFit2.0. Its own signals are the nine brand domains of S1, the shared Alibaba Cloud load balancer of linwear.top and watch-devs.com, the BLE stack com.szfission.wear.sdk on cn.wandersnail.bluetooth, and the Jieli and Realtek native libraries by name. The Jieli library names (libjl_auth.so, libjl_ota_auth.so, libjl_enc.so, libjl_crc.so, libjl_bmp_convert.so, libjl_fatfs.so, libjl_pack_format.so) match by name the Jieli family recorded in the R1 findings of Fere Fit, Lefun Health and MActivePro in this programme. No file level hashes of these libraries were recorded and no byte level comparison was made. The sibling apps Ultima Smart and Monster Fit are leads. Their package IDs were not resolved and no cluster membership is claimed.

```
Base APK SHA-256        5
    cfe9d781f4f51e2a46cd0c062c93921cc7909a86544bef4d857a4095c347f08
arm64 split SHA-256    758
    e2d3aa8e8e38efe75858afd5ea8b55109a5074144dafa269708d22990216a
Signing cert SHA-256   38
    ac8c9e1fffe9a6de609595063130a95bad3823c8ab856ab97d31cbcb50f010
Signing DN             CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=
    California, C=US (Google Play App Signing)
Load balancer          alb-kljiadtutp7b4x569r.cn-shenzhen.alb.aliyuncs.com
```

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2 and H2.

Article 5(1)(b) and (c), purpose limitation and data minimisation: engaged by H2, M1, M2 and M3, and as an open question by S1.

Article 5(1)(f) and Article 32(1)(a) and (b): engaged by C2 and H3.

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

Articles 6(1) and 7(1): engaged by C1 and H2.

Article 8: engaged by M5.

Article 9: engaged by H3 for reproductive health data and, as an open question, by H1 for the content of meeting audio.

Articles 12(1), 13 and 14: engaged by C2, H1, H2 and M4.

Article 25: engaged by C2, H3, M1 and M5.

Article 26 and Article 28: open for S1 on the roles of the operator and the other brands.

Article 35: engaged by H1 and H3.

Articles 44 and 46: engaged by H1 as an open question. The app contains hardcoded Chinese speech endpoints and no transfer mechanism is named.

Platform Accountability & DSA

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

The Data Safety card was read on 22 August 2026. It says: No data shared with third parties, This app may collect these data types: Personal info, Health and fitness and 3 others, Data is encrypted in transit, You can request that data be deleted. The operator’s own policy names AdMob and a Facebook audience feature, which does not match the first statement (C2). The configuration of C2 does not match the transit statement to the extent that plain HTTP is used, which is UNVERIFIED.

Regulatory & Legal Landscape

the Shenzhen developer entity offers the app to users in the Union through Google Play, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) received the notice in copy.

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user’s device.

The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.linwear.top
Version            1.5.1.35 (versionCode 335), minSdk 24, targetSdk 36
XAPK               207,417,146 bytes
base APK SHA-256   5cfe9d781f4f51e2a46cd0c062c93921cc7909a86544bef4d857a4095c347f08
    (184,075,861 bytes)
arm64 split SHA-256 758e2d3aa8e8e38efe75858afd5ea8b55109a5074144dafa269708d22990216a
Signing cert SHA-256 38ac8c9e1fffe9a6de609595063130a95bad3823c8ab856ab97d31cbcb50f010
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-22
```

```
AdMob application ID   ca-app-pub-6157032906860767~8366748906   (AndroidManifest.xml
    line 230)
JPUSH_APPKEY         82a353aa7346c754403ee6fc   (AndroidManifest.xml line 156, see
    below)
Policy               https://m.linwear.top/private-policy/en/onwearprocompany/1/1
Contacts             liaoweilong@linwear.com, yishuzhang888@gmail.com
Load balancer        alb-kljiadtutp7b4x569r.cn-shenzhen.alb.aliyuncs.com
Website              https://www.linwear.top
```

The manifest declares the JPush key above and a cn.jiguang.user.service.action intent filter on a :pushcore process service. A search of all nine classes*.dex files for Lcn/jpush/ and Lcn/jiguang/ found no class package. The key is therefore a template remnant or an unlinked SDK. It is recorded as a build hygiene observation and left UNVERIFIED, and it is not scored.

```
C1  AndroidManifest.xml lines 459 and 461, res/values/strings.xml, classes*.dex (
    consent platform search)
C2  res/xml/network_security_config.xml, res/xml/sm_network_security_config.xml,
    AndroidManifest.xml line 230, operator policy, Google Play Data Safety card
H1  classes*.dex (class packages and hostnames), res/values/strings.xml,
    AndroidManifest.xml (RECORD_AUDIO)
H2  AndroidManifest.xml lines 140 to 165
H3  res/values/strings.xml (en_female_health, en_menstrual_period, en_ovulation),
    AndroidManifest.xml
S1  classes*.dex hostnames, DNS resolution of linwear.top and watch-devs.com, Google
    Play developer page
M1  operator policy, AndroidManifest.xml
M2  AndroidManifest.xml line 38
M3  AndroidManifest.xml
M4  operator policy header
M5  Google Play listing, resources
```

Reproduction: obtain com.linwear.top 1.5.1.35 (335), check the SHA-256 values above, decode the manifest and resources with apktool without sources, extract strings from the dex files and read the policy. No device, account or network access beyond a DNS lookup is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF ONWEARPRO-2026-R1 at 00:04 UTC to liaoweilong@linwear.com and yishuzhang888@gmail.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Findings, three questions, embargo date 21 November 2026.

2026-09-12 Follow-up to both addresses at 17:05 UTC. It restated the findings and the three questions with answers due on 26 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:06 UTC, under the subject 35 days to publication: OnWear Pro.

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

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

What Was Done Well

A real and fairly detailed privacy policy exists and is linked from the listing. It names data categories, sources, purposes and recipients in a table, names AdMob as the advertising SDK with a stated purpose and states user rights of access, rectification, erasure and portability. A named rights contact, liaoweilong@linwear.com, carries a one month response commitment that matches the deletion statement of the Data Safety card. The NotificationListenerService is correctly permission gated. The operator discloses the self start and background location behaviour in plain language. The AI voice assistant points to Azure endpoints while the speech transcription points to Chinese vendors, so the two features are architecturally separable, which helps a remediation of H1.

Residual Risk & Recommendations

Open at the date of publication: all eleven entries. The operator has not replied and the build analysed is version 1.5.1.35 of July 2026. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, add a consent management platform and hold the SDKs back until consent (C1). Second, remove both cleartext allowances and correct the Data Safety declaration (C2). Third, gate the health features behind explicit consent and complete a data protection impact assessment (H3). Fourth, name the transcription feature and its recipient and state the Chapter V mechanism (H1). Fifth, state what happens to relayed message data (H2) and which entity controls which processing (S1). Sixth, revise the policy, limit background location, drop unneeded permissions and align the rating (M1 to M5).

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

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

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