Security & Privacy Disclosure, Final Report

Ottai Share (com.ottai.share)

The follower app for a continuous glucose monitor: another person's blood glucose over three channels, a store label that says no data, and a policy that stores it in China.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	Ottai Technology (Wuxi) Co., Ltd., Xinwu District, Wuxi, Jiangsu Province, People's Republic of China
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	1.17.0 / versionCode 263021 (analysed 2026-08-21)
Findings	10: 3 Critical, 4 High, 3 Medium
Regulators in copy	Austrian DSB and EDPS (first notice)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`87dd15a8f9baa94446e6bd23c699019c996f55e9888eb73672d079b417034f81`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 6

6.1 C1: Glucose data received over three hardcoded channels, Play label says no data collected . . . 6

6.2 C2: Policy stores data in China under PRC law and never mentions the GDPR . 7

6.3 C3: Firebase starts before any consent, no consent platform present 8

6.4 H1: Firebase API key hardcoded for the glucose database project 9

6.5 H2: Cleartext traffic permitted app-wide, no network security configuration . . 10

6.6 H3: Advertising ID and attribution permissions against a no-data label 10

6.7 H4: SMS and call alert for extreme glucose values with no named processor . 11

6.8 M1: No Bluetooth permission although the policy calls it mandatory 12

6.9 M2: PEGI 3 rating against an adults-only policy, no age gate found 13

6.10 M3: Medical-device panel names a Singapore entity, no EU representative . . 14

7 Impact Analysis 14

8 The Complete Chain 15

9 Health Data & Medical Device Context 15

10 Child Protection & Age Rating 16

11 Data Protection: Article by Article 16

12 Consumer Protection & Platform Disclosures 17

13 Regulatory & Legal Landscape 17

14 Indicators of Compromise & Reproducible Evidence 18

15 Disclosure Timeline & Outcome 19

16 What Ottai Got Right 19

17 Residual Risk & Recommendations 19

Executive Summary

Ottai Share (com.ottai.share) is the Family Care companion to the Ottai continuous glucose monitor. The person wearing the sensor uses the main Ottai app. A relative or carer installs Ottai Share, is invited by email and follows the wearer's real-time glucose values and alerts, including an Urgent Low alert. The operator is Ottai Technology (Wuxi) Co., Ltd. in Jiangsu, China. On 21 August 2026 RFI-IRFOS disclosed ten findings from a root level code analysis of version 1.17.0 under REF OTTAI-2026-R1.

The central finding is a gap between what the app does and what it says. The app exists to receive blood glucose data, which is health data under Art. 9 GDPR, and the binary carries three hardcoded channels for it: a Firebase Realtime Database, a REST backend and an MQTT client. Google Play's Data Safety section for the listing says no data is collected and none is shared. The operator's own privacy policy then says data is stored in the People's Republic of China, is governed by PRC law, names no GDPR safeguard, no data protection officer and no EU representative, and never mentions the GDPR.

Around that core sit three further groups. Firebase starts before any consent screen can exist and no consent platform is present. The build carries a hardcoded Firebase key for the project behind the glucose database, permits cleartext traffic app-wide and enables advertising-identifier and attribution permissions. And the policy describes an SMS and phone-call alert for extreme glucose values without naming the processor that sends it.

RFI-IRFOS sent the notice to privacy@service.ottai.com, service@ottai.com and ottai-dev@ottai.com with the Austrian DSB and the EDPS in copy. A follow-up went out on 12 September 2026 and a reminder on 17 October 2026. No reply of any kind has arrived as of 14 November 2026. Publication stays at 19 November 2026, independent of any reply. The analysis is static, so the report states what the binary, the policy and the store listing show and marks what only the operator can show.

Scope: Root level code analysis of Ottai Share version 1.17.0 (versionCode 263021), base APK and XAPK bundle from the APKPure mirror, because the test device did not have the app and Google Play does not allow unauthenticated retrieval: manifest, resources, the three dex files and the Flutter AOT library libapp.so (armeabi-v7a). Version and versionCode were cross-checked against the mirror listing metadata and against aapt dump badging on the extracted base APK. Public web pages read by plain HTTP GET on 21 August 2026: the operator's privacy policy at seas.ottai.com/seas-privacy-policy/ and the Google Play listing with its Data Safety section and developer panel. No endpoint was called, no key was used, no account was created, no traffic was intercepted and no runtime instrumentation was used.

ID	Severity	Title
C1	CRITICAL	Glucose data received over three hardcoded channels, Play label says no data collected
C2	CRITICAL	Policy stores data in China under PRC law and never mentions the GDPR
C3	CRITICAL	Firebase starts before any consent, no consent platform present
H1	HIGH	Firebase API key hardcoded for the glucose database project
H2	HIGH	Cleartext traffic permitted app-wide, no network security configuration
H3	HIGH	Advertising ID and attribution permissions against a no-data label
H4	HIGH	SMS and call alert for extreme glucose values with no named processor
M1	MEDIUM	No Bluetooth permission although the policy calls it mandatory
M2	MEDIUM	PEGI 3 rating against an adults-only policy, no age gate found
M3	MEDIUM	Medical-device panel names a Singapore entity, no EU representative

Finding Status at a Glance

ID	Severity	CVSS-B	Status on 14 November 2026
C1	CRITICAL	0.0	Not answered. Open.
C2	CRITICAL	0.0	Not answered. Open.
C3	CRITICAL	6.9	Not answered. Open.
H1	HIGH	6.9	Not answered. Open.
H2	HIGH	6.0	Not answered. Open.
H3	HIGH	6.9	Not answered. Open.
H4	HIGH	0.0	Not answered. Open.
M1	MEDIUM	0.0	Not answered. Open.
M2	MEDIUM	0.0	Not answered. Open.
M3	MEDIUM	0.0	Not answered. Open.

Subject & Operator Analysis

The operator is Ottai Technology (Wuxi) Co., Ltd., with the address No. 196 Jinghui East Road, Wuxi International Life Science Innovation Park (Phase II), Building J, 3rd to 4th Floor, Xinwu District, Wuxi City, Jiangsu Province, China, 214111. The privacy policy and the developer panel of the Google Play listing agree on this entity.

The companion app belongs to a continuous glucose monitoring system that the Play listing registers as a medical device with an SRN and a UDI-DI. The responsible party named on that panel is Syai Health Technology PTE. LTD, Singapore. How Syai relates to Ottai Technology (Wuxi) is not stated in the sources RFI-IRFOS read.

The privacy policy names no data protection officer and no EU representative, and the policy's only contact channel is a mainland Chinese customer-service number. Mail addresses for the operator come from the app and the Play listing: privacy@service.ottai.com and service@ottai.com appear in the string table and ottai-dev@ottai.com on the Play developer panel. No EU establishment was identified, so the Austrian Datenschutzbehörde is the authority RFI-IRFOS would approach for an Austrian-initiated matter.

Architecture & Data Flow

Ottai Share is a Flutter app. Business logic is compiled to native code in libapp.so (16.9 MB). Three dex files hold only plugin glue for Firebase, Google Sign-In, camera, geolocator and barcode scanning. minSdkVersion is 24 and targetSdkVersion is 35. The dependency manifest recovered from NOTICES.Z lists 330 packages.

A wearer of the sensor uses the main Ottai app. In Ottai Share a follower receives the wearer's values and alerts after an email invitation. Three channels are hardcoded for this: the Firebase Realtime Database ottaishare-default-rtdb.firebaseio.com, the REST backend at ottai.seas.synapsor.com/ai-api/ and seas.ottai.com/ai-api/, and an MQTT client with a stored credential key. Alert text is localised in seven languages. An AI companion feature is named Ottai AI, your smart AI glucose companion.

The policy describes an SMS and phone-call alert for extreme glucose values. The manifest contains no telephony permission, so that flow can only run on the server side. A client-side login flow with SMS codes exists, and the policy names AliCloud SMS Service as the SMS vendor for login. The app contains no ad-mediation SDK and no Bluetooth permission. The policy says data is stored in the People's Republic of China. The hosting location of the hosts above was not examined in this review.

Engagement Summary

The first notice went out on 21 August 2026 to privacy@service.ottai.com, service@ottai.com and ottai-dev@ottai.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It asked for answers to three questions within 14 days. No delivery failure notice and no automatic reply was received for any of the three addresses.

RFI-IRFOS followed up on 12 September 2026, 22 days after delivery, with the three questions repeated and a deadline of 26 September 2026. A reminder went to the same three addresses on 17 October 2026. No reply of any kind has arrived as of 14 November 2026.

Findings

C1: Glucose data received over three hardcoded channels, Play label says no data collected

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

Ottai Share exists to receive another person's real-time blood glucose values and glucose alerts. The compiled Dart binary contains the alert terminology (high, low and urgent low glucose, in seven languages) and three hardcoded channels for it: a Firebase Realtime Database, a REST backend under two hostnames and an MQTT client with a stored credential key. Google Play's Data Safety section for the listing, read on 21 August 2026, states that no data is collected and none is shared with third parties.

```
AlertsHighGlucose  AlertsLowGlucose  AlertsUrgentGlucose
AlertGlucoseCloseNotice  alert_glucose_low_night  AlertSettingGlucoseEnum
"Urgent Low Alert"
"Your blood glucose level is critically low. Please take immediate action to
address this situation and seek timely assistance from your HCP."
"Ask the person who's wearing the Ottai CGM to open Ottai App, tap 'Profile'
- 'Family Care', then enter your email address to invite you to follow."
```

```
https://ottaishare-default-rtdb.firebaseio.com     Firebase Realtime Database
https://ottai.seas.synapsor.com/ai-api/             REST backend
https://seas.ottai.com/ai-api/                      REST backend, branded host
mqtt_client Dart package (assets/flutter_assets/NOTICES.Z), stored key
    key_user_mqtt_info
```

```
Google Play, Data Safety, fetched 2026-08-21:
"No data shared with third parties... No data collected."
```

Limits of this finding. The analysis is static. RFI-IRFOS captured no traffic and read no payload, so what a glucose message looks like on each channel was not observed. The stored MQTT credential key is the reason the report treats the MQTT client as in use and not merely

linked, which is an inference from the string. The Apple App Store label cited in the notice was not re-read when this report was drafted and is marked UNVERIFIED here. The finding stands on the Google Play label alone.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to CRITICAL because the data is blood glucose, health data under Art. 9, of people who depend on it for alerts, and the store label is the disclosure a family reads before installing. CVSS gives a pure disclosure failure 0.0.

Impact: A relative who installs the app to watch a family member's glucose receives readings and urgent-low alerts that the app's own store label describes as no data at all. Neither the relative nor the person wearing the sensor can see from the label that a health value is moving through three channels.

Fix: Correct the Data Safety declaration so that health data and the other categories the app handles are listed with purposes and recipients, and align the Apple label with it.

C2: Policy stores data in China under PRC law and never mentions the GDPR

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The privacy policy at seas.ottai.com/seas-privacy-policy/ (Edition 5, effective 2025-08-15) says private and important data collected and generated in the operator's operations is stored in the People's Republic of China and is currently not transmitted outside China. It subjects the policy to PRC law and to the courts at the operator's place of residence, frames data-subject rights under Chinese law and common practice in other countries, and gives a mainland Chinese customer-service number as its only contact. A search of the full text for GDPR, European Union, Art. 27, data protection officer and DPO returned zero matches.

```
Section 3, Privacy storage site:
"We store private and important data collected and generated in our operations in the
People's Republic of China in accordance with relevant laws and regulations. Currently
    ,
we will not transmit the above information outside of China. If we do need to provide
such information outside of China due to business needs, we will follow the
    regulations
of the relevant countries or ask for your consent."

Section 8, Contact us, subsection 3:
"The validity, interpretation, and dispute resolution of this policy shall be governed
     by
the laws of the People's Republic of China... we agree to submit the dispute or
controversy to the jurisdiction of the people's court with jurisdiction over the place
     of
residence of Ottai Technology (Wuxi) Co., Ltd."

Section 5, Your rights, preamble:
"Under relevant Chinese laws, regulations, standards, and common practices in other
countries and regions, we guarantee that you can exercise the following rights..."

Contact channel given: +86 400-9039-130
```

Limits of this finding. The finding rests on the operator's own statement. RFI-IRFOS did not examine where the hosts in finding C1 are served from, and did not observe an EU user's data reach a server in China. The notice described this as a Chapter V transfer. The policy itself says the data is stored in China, and no Art. 46 safeguard and no Art. 27 representative is named anywhere.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to CRITICAL because the policy places Art. 9 health data in a third country with no adequacy decision and no named safeguard, and leaves EU users without any EU point of accountability. CVSS gives a legal-framework gap 0.0.

Impact: An EU user of an app that carries health data finds a policy that sends the data to China, applies Chinese law and Chinese courts, and offers no EU contact, no supervisory-authority route and no safeguard for the transfer.

Fix: State the actual storage location for EU users. If data leaves the EEA, name the Art. 46 mechanism, appoint an Art. 27 representative, name a data protection contact in the Union and describe the rights under the GDPR.

C3: Firebase starts before any consent, no consent platform present

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

FirebaseInitProvider is declared with initOrder 100 and directBootAware true. Android initialises ContentProviders during Application creation, before any Activity and before the device is unlocked. No OneTrust, Didomi, Usercentrics or Google User Messaging Platform code exists in the three dex files or in the 330-package dependency manifest. No Consent Mode default-state flag is set in the resources, so Firebase Analytics and the Measurement SDK run with collection enabled from the first launch. The ad-services configuration grants attribution access to all callers.

```
<service android:directBootAware="true" android:exported="false"
    android:name="com.google.firebase.components.ComponentDiscoveryService"/>
   registers FlutterFirebaseAppRegistrar, FirebaseMessagingRegistrar,
   FirebaseCrashlyticsRegistrar, AnalyticsConnectorRegistrar,
    FirebaseSessionsRegistrar
   and 8 more Firebase registrars
<provider android:authorities="com.ottai.share.firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<receiver android:name="com.google.android.gms.measurement.AppMeasurementReceiver"/>
<service android:name="com.google.android.gms.measurement.AppMeasurementService"/>

res/xml/ga_ad_services_config.xml:
<ad-services-config><attribution allowAllToAccess="true" /></ad-services-config>
```

classes3.dex contains only the generic IAB TCF reader strings (IABTCF_CmpSdkID, IABTCF_TCString, IABTCF_gdprApplies) that ship inside Google's own SDK. Because no consent platform in the app writes those keys, they stay unset.

Limits of this finding. The analysis is static. RFI-IRFOS captured no traffic and measured no analytics payload.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the whole application processes Art. 9 data and the build has no mechanism to ask for a choice before analytics start. The same missing mechanism applies on every launch.

Impact: On the first launch of an app built to deliver glucose alerts, Firebase Analytics, Crashlytics, Messaging and the Measurement SDK are already running, and nothing in the build lets the user decline them first.

Fix: Disable automatic Firebase Analytics collection in the manifest, set the Consent Mode defaults to denied, add a consent platform and start the SDKs from code only after a recorded choice.

H1: Firebase API key hardcoded for the glucose database project

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

res/values/strings.xml contains the Firebase API key for project ottaishare, which is also the project behind ottaishare-default-rtdb.firebaseio.com, the Realtime Database named in C1. Google documents that Firebase API keys are not secrets by design. The exposure is one of availability and configuration: an extracted key can be used against the project's quotas, and whether the database and storage rules restrict access depends on server-side settings the binary does not show.

```
google_api_key                AIzaSyCIqJvhSo90IewdIAKikXCfm0Bib-olXTM
google_crash_reporting_api_key [same value as google_api_key]
google_app_id                 1:656539889660:android:a94aafc689ec85d8d44c79
project_id                    ottaishare
google_storage_bucket         ottaishare.appspot.com
gcm_defaultSenderId           656539889660
default_web_client_id         656539889660-t5oflqb316voqbsbt1229af77l4c9ocq.apps.
    googleusercontent.com
```

What is not established. RFI-IRFOS sent no request with the key, tested no Realtime Database or Storage rules and made no statement about their configuration. No App Check client component is registered in the manifest. Whether enforcement is switched on for the project is a server-side setting. The notice described read, write and quota paths as consequences if the rules are not locked down, and asked the operator to show that they are.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the project carries a safety-alert channel for people with diabetes, so exhausting its quota is an availability failure of a health service and not a billing inconvenience.

Impact: The Firebase project that carries glucose alerts can be reached with a key every installed copy holds. If the quota is exhausted, delivery of urgent-low warnings through that channel is disrupted, and what more a third party can do depends on rules the operator has not shown.

Fix: Restrict the key by application signature and API, enforce App Check, keep Realtime Database and Storage rules at deny-by-default with per-user scoping, and rate-limit Auth.

H2: Cleartext traffic permitted app-wide, no network security configuration

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B)

AndroidManifest.xml sets android:usesCleartextTraffic to true at application level. targetSdkVersion is 35, where the platform default would deny cleartext, so the app overrides a safe default. No networkSecurityConfig attribute is present and no network_security_config.xml exists anywhere in the package, so there is no per-domain restriction and no certificate pinning for any of the three channels in C1.

```
<application android:allowBackup="false" ... android:usesCleartextTraffic="true">
res/xml/network_security_config.xml: does not exist
```

Limits of this finding. This is a permission and not an observation. RFI-IRFOS did not measure whether any channel actually uses plain HTTP or unencrypted MQTT. The finding is that nothing in the configuration forces TLS.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the data in transit is health data of people who rely on timely alerts, and the platform default that would have protected it was overridden on purpose.

Impact: On a shared or hostile network, nothing in the app's configuration prevents glucose readings and alerts from travelling unencrypted if any channel falls back to plain transport.

Fix: Set cleartext to false, add a network security configuration with pinned trust anchors for the operator's domains and verify that each channel uses TLS.

H3: Advertising ID and attribution permissions against a no-data label

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

The manifest declares AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID, and the ad-services configuration sets allowAllToAccess true. A search of the 330 dependencies and all dex files found no dedicated ad-mediation SDK, so these permissions most plausibly come from Google's own Firebase Analytics and Play Services measurement stack. Whatever consumes them, the identifier and the attribution API are enabled in a binary whose Play label declares that no data is collected.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
```

Limits of this finding. RFI-IRFOS did not observe the identifier leaving the device. The finding concerns the contradiction with the label and the absence of any consent step.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app is a health companion and the label users rely on is wrong about it. The platform policy on Data Safety accuracy is a separate issue from the GDPR.

Impact: A family carer's advertising identifier is available to Google's measurement stack in an app whose store label says it collects nothing.

Fix: Remove the permissions the app does not need, set the ad-services configuration to deny, and correct the Data Safety declaration.

H4: SMS and call alert for extreme glucose values with no named processor

---

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

Section 2.4 of the privacy policy says that, if the user activates the service, the operator and/or a third party commissioned by it will alert the user by text message and/or phone call if an extreme abnormality in glucose levels is detected. The manifest declares no SEND_SMS, READ_SMS or CALL_PHONE permission, confirmed by the decoded manifest and by aapt dump permissions, so any such alert runs on the server side. Section 8 names AliCloud SMS Service (Alibaba Group Holding Ltd.) as an SDK but limits its stated purpose to login and other important operations. No processor is named for the glucose-alert flow.

```
Section 2.4:
"If you activate this service, we and/or a third party commissioned by us will alert
    you
via text message and/or phone call if we detect an extreme abnormality in your glucose
     levels."

Section 8, first listed SDK:
Product Name: AliCloud SMS Service
Company: Alibaba Group Holding Ltd.
Purpose: To send SMS messages to users through the SMS service when users log in and
during other important operations.
Type of privacy collected: User's cell phone number
```

UNVERIFIED. Whether the SMS and call mechanism is active for this build, whether the push-notification channel from C1 has replaced it, and what the messages contain are server-side questions. RFI-IRFOS did not examine them. The libapp.so string get sms code success: shows that an SMS flow exists for login.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to HIGH because a message that says an extreme glucose value was detected is itself health data, it reaches the user through a processor the policy does not name for this purpose, and the flow is described as safety-critical. CVSS gives a disclosure gap 0.0.

Impact: A person who switches on the safety alert is told that a health-derived signal reaches them by SMS or call and is not told which company handles that message.

Fix: Name the processor for the glucose-alert SMS and call flow in the policy, state where it operates, and document the DPIA that covers this automated processing.

M1: No Bluetooth permission although the policy calls it mandatory

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The privacy policy's device-permission table says the Bluetooth permission is used to connect Ottai products and is mandatory, and that the CGM sensor cannot be connected without it. The binary contains Bluetooth state and pairing text in several languages. The manifest declares no BLUETOOTH, BLUETOOTH_ADMIN, BLUETOOTH_SCAN or BLUETOOTH_CONNECT permission, confirmed by the decoded manifest and by aapt dump permissions. This build cannot pair a sensor.

```
Policy Section 2.5: "Permission name: Bluetooth / Purpose of permission: used to
    connect
Bluetooth devices of Ottai products / ... it is mandatory; if refused, the CGM Sensor
cannot be connected."

libapp.so: bluetoothScan, bluetoothConnect, bluetoothAdvertise, "Bluetooth is Off",
"Active Bluetooth para obtener lecturas y alertas"
AndroidManifest.xml: no BLUETOOTH* permission
```

The most consistent reading is that Ottai Share, the follower app, shares a localisation bundle with the wearer app and does not itself pair sensors. That reading is non-alarming. The point is a documentation gap: the policy does not distinguish between the two apps.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the policy is the only description of the app's data handling that a carer receives and it describes a capability this app lacks. CVSS gives a documentation gap 0.0.

Impact: A carer reading the policy is told a permission is mandatory for a function this app does not perform, so the policy does not describe what this app actually does.

Fix: Split the permission table by app or mark which permissions apply to Ottai Share.

M2: PEGI 3 rating against an adults-only policy, no age gate found

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The privacy policy states that the products and services are intended only for adults aged 18 and over and that minors should not create accounts, with or without parental consent. Google Play rates the listing PEGI 3. Date-of-birth entry is optional according to the policy (Section 1.3). No date-of-birth gate, blocking string or eligibility logic was found in libapp.so, which contains only the bare label Date of Birth.

```
Policy Section 6: "Our products and services are intended only for adults who have
    reached the
age of 18. Minors should not create their private subject accounts, with or without
parental or guardian consent."
Google Play content rating: PEGI 3
```

Limits of this finding. No account was created, so whether a minor can register was not tested. Special-category processing of minors is therefore not established.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the follower role is a family role, so adults and children share the same households. CVSS gives a design gap 0.0.

Impact: The store tells parents the app suits all ages while the operator's policy excludes minors, and the app contains no check that would enforce the policy.

Fix: Align the store rating and the policy, and add an age check or a documented guardian route.

M3: Medical-device panel names a Singapore entity, no EU representative

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The Play listing's developer panel carries EU medical device information for a Continuous Glucose Monitoring System. The only responsible party named is Syai Health Technology PTE. LTD. in Singapore. MDR Article 11 requires an authorised representative established in the Union where the manufacturer is not. No such representative appears on the panel, in the privacy policy or in any source RFI-IRFOS read.

```
EU medical device information
Continuous Glucose Monitoring System (SRN: SG-MF-000041645)
Syai Health Technology PTE. LTD
112 Robinson Road #03-01, Robinson 112, Singapore, 068902
eIFU
UDI-DI: 08885021260204
```

Limits of this finding. RFI-IRFOS did not check EUDAMED or the device labelling, where an authorised representative may be recorded. The finding concerns the listing and the policy. Enforcement of the MDR sits with a different authority than data protection.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the companion app belongs to a medical device and the gap mirrors the missing EU accountability in C2. The regime is different and the matter is outside the scope of data protection law.

Impact: For a glucose-monitoring system sold to people in the Union, the listing shows no accountable party inside the Union, the same pattern as the missing GDPR representative in C2.

Fix: Name the EU authorised representative on the listing and in the policy, or document where it is recorded.

Impact Analysis

The people affected are, first, the wearers of the Ottai sensor, people who monitor their blood glucose, and second, the relatives and carers who follow them through Ottai Share. The wearer's glucose history and urgent-low events are health data about a person with a chronic condition. The follower's email address and phone number are personal data as well.

What the evidence shows is a mismatch of disclosure and design. The store label tells families that no data is collected (C1). The policy places the data in China under Chinese law and offers the EU user no representative and no GDPR route (C2). Analytics start before any choice (C3). The channel that carries alerts depends on a project key every install carries (H1) and on a configuration that does not force TLS (H2).

The analysis found no evidence of a breach or misuse and did not examine the server side, so it does not say who has accessed glucose data. The policy restricts the service to adults. The follower role is a family role, and whether minors are wearers or followers was not established.

The Complete Chain

Step 1, discovery: a relative finds Ottai Share on Google Play. The Data Safety label says no data is collected, and the listing carries an EU medical device panel that names a Singapore entity (C1, M3).

Step 2, first launch: Firebase starts before any screen and the advertising and attribution permissions are in place (C3, H3).

Step 3, invitation: the wearer enters the relative's email address in the Ottai app. The follower account is created and linked to the wearer's data. No consent choice and no age check appears in the build (C3, M2).

Step 4, transmission: glucose values and alerts reach the follower through the Firebase Realtime Database, the REST backend and the MQTT connection. The configuration does not force TLS (C1, H2).

Step 5, storage: the policy says data is stored in the People's Republic of China under PRC law. No safeguard, representative or GDPR route is named (C2).

Step 6, an emergency: the policy says an SMS or a call may follow an extreme glucose value, through a processor it does not name for this purpose (H4).

Step 7, the user tries to act: the only contact is a mainland Chinese phone number. No EU representative and no data protection contact exists (C2).

Health Data & Medical Device Context

Blood glucose values are health data within Art. 4(15) and Art. 9(1) GDPR and Recital 35. Processing needs an Art. 6(1) basis and an Art. 9(2) condition. The build shows no mechanism that obtains either before processing starts, and the policy does not describe the GDPR framework at all.

The measuring system the app belongs to is listed as a medical device with an SRN and a UDI-DI. MDR Article 11 requires an authorised representative in the Union where the manufacturer is established outside it. The listing names Syai Health Technology PTE. LTD in Singapore and no EU-established representative (M3). RFI-IRFOS did not check EUDAMED or device labelling. The MDR is enforced by authorities other than data protection supervisors. It is mentioned because the same pattern, no accountable party inside the Union, appears in both registers.

Child Protection & Age Rating

The policy says the service is for adults aged 18 and over and that minors should not create accounts. Google Play rates the listing PEGI 3. The build contains no age gate and treats date of birth as an optional profile field (M2). The follower role exists to connect family members, and a family can include children. RFI-IRFOS did not test registration and does not claim that a minor's data is processed. It reports that the store rating and the operator's own policy disagree and that nothing in the build enforces the policy.

Data Protection: Article by Article

Article 4(15) and Article 9(1) and (2): engaged by C1, C3 and H4. Blood glucose values and a message about an extreme glucose value are health data and need an Art. 9(2) condition.

Article 5(1)(a), Article 12 and Article 13(1)(c) and (e): engaged by C1, H3, H4 and M1. The store label, the policy and the binary describe the processing in different ways and the processor for the alert flow is not named.

Article 5(2): engaged by C2, C3 and H1. The operator carries the burden of showing safeguards and server-side rules.

Article 6(1), Article 7(1) and ePrivacy Directive Article 5(3): engaged by C3. Processing and access to terminal equipment begin before any consent mechanism exists.

Article 8: engaged conditionally by M2.

Article 13(1)(f), Article 27, Article 44 and Article 46: engaged by C2. The policy places data in China, no adequacy decision exists for China and no safeguard or representative is named.

Article 25 and Article 32(1)(a) and (b): engaged by H1 and H2. A project key ships in every install and the configuration does not force TLS.

Article 35: engaged by H4 and the processing as a whole. A DPIA is expected for large-scale processing of health data and for the automated alerting. The notice asked whether one exists.

Consumer Protection & Platform Disclosures

Google Play's Data Safety section is the disclosure families read before installing. For this listing it says no data is collected and none is shared, while the app's only function is to receive another person's glucose values (C1). The advertising-identifier permissions and the attribution configuration sit in the same binary (H3). The Apple App Store label is cited in the notice and was not re-read for this report, so it is marked UNVERIFIED here. Google Play publishes the label as the developer declares it. This report makes no statement about Google's own obligations.

Regulatory & Legal Landscape

No EU establishment of the controller was identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected can act under Article 55. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the first notice in copy. The medical-device aspects (M3) sit with the competent authorities under the MDR.

The operator's policy rests on Chinese law. RFI-IRFOS does not assess Chinese law. For EU users the relevant question is what the GDPR requires of a controller that offers a health app in the Union, and the policy answers none of it. The pre-consent initialisation pattern in C3 recurs across health and consumer apps in the RFI-IRFOS programme, which treats every operator under the same rules regardless of size.

Indicators of Compromise & Reproducible Evidence

Every point below can be checked against the public Google Play build, the mirror listing and the public web pages named.

```
Package         com.ottai.share
Version         1.17.0 / versionCode 263021
base.apk        SHA-256 87
    dd15a8f9baa94446e6bd23c699019c996f55e9888eb73672d079b417034f81
XAPK bundle     SHA-256
    ca45b7e934434867b92b61a6a5b7be69bd754fc76021b658318110d4d77e40aa
                APKPure, 65,822,741 bytes in the listing metadata, base.apk 35.6 MB
Min/target SDK  24 / 35
Code base       Flutter, lib/armeabi-v7a/libapp.so 16.9 MB, three classes*.dex
```

```
Firebase project   ottaishare
App ID             1:656539889660:android:a94aafc689ec85d8d44c79
Sender ID          656539889660
Storage bucket     ottaishare.appspot.com
Realtime Database  https://ottaishare-default-rtdb.firebaseio.com
API key: present in res/values/strings.xml, value as extracted:
    AIzaSyCIqJvhSo90IewdIAKikXCfm0Bib-olXTM
```

```
https://ottai.seas.synapsor.com/ai-api/
https://seas.ottai.com/ai-api/
mqtt_client package, key key_user_mqtt_info
Contact strings    privacy@service.ottai.com, service@ottai.com (libapp.so), ottai-
    dev@ottai.com (Play panel)
Policy             https://seas.ottai.com/seas-privacy-policy/ (Edition 5, 2025-08-15,
     read 2026-08-21)
Play listing       play.google.com/store/apps/details?id=com.ottai.share (read
    2026-08-21)
Medical device     SRN SG-MF-000041645, UDI-DI 08885021260204, Syai Health Technology
    PTE. LTD
```

```
apktool d on the base APK: AndroidManifest.xml, res/values/strings.xml, res/xml/
    ga_ad_services_config.xml
aapt dump permissions: no SEND_SMS, READ_SMS, CALL_PHONE, BLUETOOTH*
strings on libapp.so: AlertsUrgentGlucose, key_user_mqtt_info, "get sms code success:"
search for OneTrust, Didomi, Usercentrics, consentmanager, com/google/android/ump: 0
    matches
res/xml/network_security_config.xml: not present
```

Disclosure Timeline & Outcome

2026-08-21 First notice (REF OTTAI-2026-R1) to privacy@service.ottai.com, service@ottai.com and ottai-dev@ottai.com, CC dsb@dsb.gv.at and edps@edps.europa.eu, with three questions and a 14-day reply request.

2026-09-04 The 14-day reply window closed with no answer.

2026-09-12 Follow-up to the same three addresses restating the three questions, deadline 26 September 2026.

2026-10-17 Reminder to the same three addresses, 33 days before publication.

2026-11-14 No reply of any kind on the thread.

2026-11-19 Publication date, unchanged since the first notice.

What Ottai Got Right

Android backup is disabled. The policy points to a working in-app path for access and correction (Home page, Profile, Edit Information) and describes deletion, retention limits and breach notification in more operational detail than most policies in the programme. The policy states that declining marketing notifications does not affect safety-critical glucose alerts, which keeps marketing consent apart from the safety feature. Section 8 lists third-party SDKs with product, company, purpose, data type, contact and policy link, a level of detail few policies reach. Glucose and alert terminology is localised in seven languages, which serves the actual audience of non-English-speaking carers. The company has pursued EU medical-device registration for the underlying system, and M3 concerns who is named as accountable within it.

Residual Risk & Recommendations

Everything in the findings table is open at the date of publication. A final APK diff before 19 November 2026 determines the state the published report records.

What remains unknown and matters most: where the hosts in C1 are served from and what an EU user's data path actually is, whether the SMS and call alert is active and which processor sends it, and whether the Firebase project's rules and App Check enforcement protect the glucose data.

Recommendations: correct the Data Safety and App Store labels so that health data and its recipients are named. Publish a policy that applies to EU users, states the storage location, names the Art. 46 mechanism and the Art. 27 representative and gives an EU data protection contact. Disable automatic Firebase Analytics, set Consent Mode defaults to denied and add a consent platform. Restrict the Firebase key, enforce App Check and keep database and storage rules at deny-by-default. Set cleartext to false and add a network security configuration. Remove unused advertising permissions. Name the processor for the glucose-alert SMS and call flow and document the DPIA. Align the PEGI rating with the adults-only policy and name the EU authorised representative for the device.

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

plus public web pages read by plain HTTP GET. No Ottai server, key or account was used. Final report, published 21 November 2026. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG and GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF OTTAI-2026-R1.