



Security & Privacy Disclosure, Final Report

Meine ÖGK for Android (at.itsv.mobile.meineoegk)

Austria's statutory health insurer for 8.5 million people hardcodes a Firebase key, starts two Google tracking systems before any consent screen, and leaves undisclosed Art. 9 audio processing in its telemedicine feature, unresolved through 113 days and a 23-day-overdue embargo, with zero reply of any kind

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 24
SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

Target	Österreichische Gesundheitskasse (ÖGK), Austria's statutory health insurer for roughly 8.5 million insured people
Package	at.itsv.mobile.meineoegk
Platform Audited	Android · v3.2.0, static analysis of the production APK
Initial Disclosure (R1)	2026-06-26 (REF OEGK-2026)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (3 Critical, 2 High)
Correspondence	5 messages sent by RFI-IRFOS across two threads, 0 replies of any kind received, 2 of the original R1's 2 direct recipient addresses bounced
Authorities BCC'd / CC'd	Austrian Datenschutzbehörde (DSB) · Finanzmarktaufsicht (FMA) · Bundesministerium fuer Soziales (Sozialministerium) · Press contact (presse@oegk.at)

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	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	C1: Firebase API key hardcoded in the production binary, with unauthenticated query risk if security rules are misconfigured	6
4.2	C2: FirebaseInitProvider and MIKitInitProvider both auto-initialize before the first screen, before any consent opportunity	6
4.3	H1: BOOT_COMPLETED receiver restarts the app automatically after every device reboot	7
4.4	H2: Expo Contacts module holds full read and write access to the device address book with no stated purpose	7
4.5	C3: WebRTC telemedicine feature captures RECORD_AUDIO with Art. 9 obligations for medical-consultation data not clearly addressed	8
5	Impact Analysis	8
6	The Complete Chain: Two Bounced Mailboxes, One Working Address, and Ninety-Two Days of Silence	9
7	Data Protection — Article by Article	9
8	Regulatory & Legal Landscape	10
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	11
11	Residual Risk & Recommendations	11

Executive Summary

The Österreichische Gesundheitskasse (ÖGK) is Austria's statutory health insurer, covering roughly 8.5 million insured people. Its Android application, Meine ÖGK (at.itsv.mobile.meineoegk, v3.2.0), is the primary digital channel through which insured people manage claims, appointments, and telemedicine consultations.

Static analysis identified five findings. A Firebase API key is hardcoded in the production Play Store binary, with no authentication required to query the associated Firebase project if its security rules are misconfigured. FirebaseInitProvider (initOrder=100) and MIKitInitProvider (initOrder=99) both auto-initialize before the first Activity screen, before any opportunity to consent or decline, meaning two separate Google tracking systems start on every single install unconditionally. A BOOT_COMPLETED receiver, via expo.modules.notifications, restarts the app automatically after every device reboot with no user interaction. An Expo Contacts module holds full read and write access to the insured person's device address book, with no stated purpose for a health insurer to write to a user's contacts. Most seriously, the app's WebRTC telemedicine feature, used for video consultations with doctors, captures RECORD_AUDIO data with Art. 9 obligations for that health-data-adjacent processing not clearly addressed anywhere in the application's available disclosures.

RFI-IRFOS disclosed these findings on 26 June 2026 under REF OEGK-2026 to datenschutz@oegk.at and info@oegk.at, CC presse@oegk.at, BCC the Austrian DSB, the FMA, and the Bundesministerium fuer Soziales. Both direct recipient addresses bounced. RFI-IRFOS located a working address, dsb@oegk.at, and sent four follow-ups across the embargo period, on 5 August, 15 August, 24 August, and 6 September 2026, each restating the five findings and the still-open questions. At no point in 92 days of correspondence did the ÖGK send a reply of any kind, not an acknowledgment, not a rejection, not even an automated response, to any of the five messages sent across either address. The stated embargo of 26 September 2026 passed 21 days ago with the case in exactly this state.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the production binary, with unauthenticated query risk if security rules are misconfigured
C2	CRITICAL	FirebaseInitProvider and MIKitInitProvider both auto-initialize before the first screen, before any consent opportunity
H1	HIGH	BOOT_COMPLETED receiver restarts the app automatically after every device reboot
H2	HIGH	Expo Contacts module holds full read and write access to the device address book with no stated purpose
C3	CRITICAL	WebRTC telemedicine feature captures RECORD_AUDIO with Art. 9 obligations for medical-consultation data not clearly addressed

Subject & Operator Context

The Österreichische Gesundheitskasse (ÖGK) is Austria's statutory social health insurance provider, created in 2020 from the merger of the country's regional health insurance funds. It covers roughly 8.5 million insured people, the large majority of Austria's population, making it one of the highest-reach applications in this entire disclosure series by user count.

A statutory health insurer's app sits in a different risk category than a consumer product: the people using it have no real alternative provider to switch to, the data it touches (claims, appointments, telemedicine consultations) is inherently health-adjacent under GDPR Art. 9, and the institution itself is a public body answerable to the same regulators RFI-IRFOS BCC'd on the original disclosure. The findings in this report concern an app that starts tracking before consent, holds an unexplained write capability over a user's address book, and leaves its own telemedicine audio processing undocumented, all inside that context.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 26 June 2026 under REF OEGK-2026 to datenschutz@oegk.at and info@oegk.at, CC presse@oegk.at, BCC the Austrian DSB, the FMA, and the Bundesministerium fuer Soziales. Both direct recipient addresses, datenschutz@oegk.at and info@oegk.at, returned delivery failures from postmaster@sv-services.at.

RFI-IRFOS located dsb@oegk.at as a working address and sent four follow-ups across the embargo period: 5 August 2026, 15 August 2026, 24 August 2026 (CC the Austrian DSB), and 6 September 2026 (CC presse@oegk.at), each restating all five findings and a set of still-open questions. No message from any of these five sends, across either address, ever received a reply of any kind, not an acknowledgment, not a rejection, not an automated response, not a bounce beyond the original two. The stated embargo of 26 September 2026 passed 21 days before this report's publication date, with the ÖGK having said nothing at all in 92 days of correspondence.

Findings

C1: Firebase API key hardcoded in the production binary, with unauthenticated query risk if security rules are misconfigured

CRITICAL (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, 5.4) — hardcoded credential on a statutory health insurer's backend, blast-radius escalated from MEDIUM

```
Firestore project ID: meineoegk
Hardcoded API key present in production binary, no runtime
authentication required to query the project if security
rules permit unauthenticated access
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.4 to CRITICAL because the hardcoded key sits in the production binary of Austria's statutory health insurer, used by roughly 8.5 million insured people, and if the associated Firebase project's security rules are misconfigured, the key alone is sufficient to query that project with no further authentication. The scale of the affected population and the health-adjacent nature of the data a statutory insurer's backend holds place this well beyond a generic hardcoded-credential finding.

C2: FirebaseInitProvider and MLKitInitProvider both auto-initialize before the first screen, before any consent opportunity

CRITICAL (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, 5.4) — two Google tracking systems start pre-consent on every install, blast-radius escalated from MEDIUM

```
FirebaseInitProvider    initOrder=100
MLKitInitProvider       initOrder=99

Both execute before the first Activity.onCreate(), ahead of
any consent screen or SDK gating logic
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.4 to CRITICAL because FirebaseInitProvider (initOrder=100) and MLKitInitProvider (initOrder=99) both start before the first Activity screen is rendered, meaning this pre-consent initialization applies to every single install of a statutory health insurer's app, unconditionally, with no opportunity for any of the 8.5 million insured people this app serves to consent or decline before tracking begins.

H1: BOOT_COMPLETED receiver restarts the app automatically after every device reboot

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 4.6)
— unconditional boot-persistence capability, blast-radius escalated from MEDIUM

```
android.permission.RECEIVE_BOOT_COMPLETED  
Registered via expo.modules.notifications
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.6 to HIGH because the BOOT_COMPLETED receiver, registered via expo.modules.notifications, restarts the application automatically after every device reboot with no user interaction and no visible indication to the user that this occurred, a capability exceeding what Art. 5(1)(c) data minimisation permits absent a specific, disclosed purpose for unconditional background persistence on a statutory health insurer's app.

H2: Expo Contacts module holds full read and write access to the device address book with no stated purpose

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.5)
— unexplained write access to third-party contact data, blast-radius escalated from MEDIUM

```
android.permission.READ_CONTACTS  
android.permission.WRITE_CONTACTS  
Expo Contacts module: full read/write, no disclosed feature  
identified that requires write access
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.5 to HIGH because write access to a user's address book reaches beyond the user themselves to every third party in that address book, people who never installed this app and never had any opportunity to consent, with no feature identified during this audit that a statutory health insurer's app would need this capability for. Read access alone would already exceed data minimisation; write access has no documented justification at all.

C3: WebRTC telemedicine feature captures RECORD_AUDIO with Art. 9 obligations for medical-consultation data not clearly addressed

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — undisclosed audio processing during actual medical consultations, blast-radius escalated from HIGH

```
android.permission.RECORD_AUDIO
WebRTC telemedicine module: live audio capture during
video/audio consultations, Art. 9 processing basis and
recipient disclosure not identified in available documentation
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL because this is not biometric authentication or a generic sensor permission, it is live audio capture during what is, by the feature's own stated purpose, an actual medical consultation between an insured person and a doctor. Art. 9(1) health data obligations apply directly and unambiguously to this data flow, and this audit found no clear documentation of the Art. 9(2)(h) health care-processing basis, retention terms, or recipient disclosure that should accompany audio data generated inside a telemedicine appointment on a statutory health insurer's own app.

Impact Analysis

C1 and C2 describe an app that hardcodes a backend credential and starts two separate Google tracking systems before any consent mechanism can act, both on an app used by roughly 8.5 million insured people, nearly the entire population Austria's statutory health system serves. H1 and H2 each extend the app's reach beyond what a health-insurance function requires: an unconditional boot-triggered restart, and write access to a third party's address book. C3 is the most serious finding in this report on its own terms, not because of scale but because it concerns live audio captured during an actual medical consultation, the kind of data GDPR Art. 9 was written specifically to protect, with no clear documentation found anywhere in the app's available disclosures.

What distinguishes this case from most others in this disclosure series is not any single technical finding but the complete absence of any response. Two of the two addresses used in the original disclosure bounced, a working address was found and used for every subsequent message, and across 92 days and five total sends, Austria's statutory health insurer for 8.5 million people did not send a single reply, not even an acknowledgment, to a disclosure that named a live Art. 9 audio-processing gap in its own telemedicine feature.

The Complete Chain: Two Bounced Mailboxes, One Working Address, and Ninety-Two Days of Silence

Step 1 — Disclosure sent, both addresses bounce: RFI-IRFOS sends the original findings to datenschutz@oegk.at and info@oegk.at on 26 June 2026 under REF OEGK-2026. Both addresses return delivery failures from postmaster@sv-services.at.

Step 2 — A working address is located: RFI-IRFOS identifies dsb@oegk.at as a functioning contact point and re-routes all subsequent correspondence through it rather than treating the bounces as a dead end.

Step 3 — Four follow-ups, zero acknowledgment: Messages sent 5 August, 15 August, 24 August, and 6 September 2026 to dsb@oegk.at all deliver successfully. None receives any reply, of any kind, from the ÖGK.

Step 4 — Embargo reached in silence: The stated embargo of 26 September 2026 passes with no change in the correspondence record: five messages sent across two addresses and one working mailbox, zero substantive replies, zero acknowledgments, zero automated responses beyond the original two bounces.

Step 5 — Publication: This report publishes 21 days after the embargo date, on the terms stated from the first message.

This case differs from a simple non-response: RFI-IRFOS actively diagnosed a delivery failure, found a working channel, and continued the full follow-up cadence through that channel, and the ÖGK still chose not to respond at any point.

Data Protection — Article by Article

Art. 32 GDPR — Security of processing: C1's hardcoded Firebase key falls short of the technical security measures Art. 32 requires for a statutory health insurer's backend infrastructure.

Art. 7(1) GDPR — Conditions for consent: C2's `FirebaseInitProvider` and `MIKitInitProvider` both initialize before any consent mechanism can act, for every install.

Art. 5(1)(a) GDPR — Lawfulness, fairness and transparency: C2's pre-consent tracking is not disclosed to the user before it occurs.

Art. 5(1)(c) GDPR — Data minimisation: H1's unconditional boot-triggered restart and H2's unexplained Contacts write access both exceed what a health-insurance function requires.

Art. 6 GDPR — Lawfulness of processing: H2's write access to third-party contact data, affecting people who never consented to anything, lacks an identified lawful basis.

Art. 9(1)/Art. 9(2)(h) GDPR — Special categories of data, health and social-care processing: C3's telemedicine audio capture occurs during actual medical consultations with no clearly documented Art. 9(2)(h) basis.

Art. 13(1)(e) GDPR — Transparency, recipients of data: C3's telemedicine audio processing has no identified recipient disclosure in documentation reviewed for this audit.

Regulatory & Legal Landscape

The Österreichische Gesundheitskasse is an Austrian statutory body, placing it squarely within the jurisdiction of the Austrian Datenschutzbehörde (DSB), BCC'd on the original disclosure and CC'd on one follow-up. The Finanzmarktaufsicht (FMA) and the Bundesministerium fuer Soziales were also BCC'd given the ÖGK's status as a public social-insurance institution.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 9 special-category violation in C3, up to EUR 20,000,000 or 4% of total worldwide annual turnover; for a statutory public body, the relevant comparator is typically the body's own budget or an amount set under national implementing law rather than a commercial turnover figure, but the Art. 83(5) tier itself still applies to the underlying violation. Art. 83(4) applies to the Art. 5, 6, 7, and 32 issues in C1, C2, H1, and H2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. That a public statutory health insurer, answerable to the same DSB it was BCC'd on, did not respond at all across 92 days and five sends is itself a fact relevant to any regulator assessing institutional engagement with disclosed Art. 9 findings.

Indicators of Compromise

The following identifiers, permissions, and provider declarations were extracted from the production APK (v3.2.0) via static analysis only. No ÖGK servers, accounts, or infrastructure were probed.

```
C1 -- Hardcoded Firebase API key, project: meineoegk

C2 -- FirebaseInitProvider initOrder=100,
     MlKitInitProvider initOrder=99

H1 -- android.permission.RECEIVE_BOOT_COMPLETED
     (expo.modules.notifications)

H2 -- android.permission.READ_CONTACTS, WRITE_CONTACTS
     (Expo Contacts module)

C3 -- android.permission.RECORD_AUDIO (WebRTC telemedicine
     module)
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure sent under REF OEGK-2026 to datenschutz@oegk.at and info@oegk.at. CC: presse@oegk.at. BCC: Austrian DSB, FMA, Bundesministerium fuer Soziales. Both direct recipient addresses bounce via postmaster@sv-services.at.

2026-08-05 Follow-up sent to dsb@oegk.at, the working address located after the original bounces. No reply.

2026-08-15 Second follow-up to dsb@oegk.at. No reply.

2026-08-24 Third follow-up to dsb@oegk.at, CC the Austrian DSB. No reply.

2026-09-06 Fourth follow-up to dsb@oegk.at, CC presse@oegk.at, 72 days since the original disclosure. No reply.

2026-09-26 Stated embargo date reached. No message of any kind received from the ÖGK across either address or any of the five sends.

2026-10-17 This report published, 21 days after the embargo date. All five findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 — Immediate: Rotate the hardcoded Firebase key and confirm the associated project's security rules require authentication for all read/write operations.

C2 — Immediate: Reorder `FirebaseInitProvider` and `MIKitInitProvider` initialization to occur strictly after an affirmative consent signal, not before, for all 8.5 million insured people this app serves.

H1 — Governance: Scope the `BOOT_COMPLETED` receiver to a specific disclosed purpose (e.g. pending-notification delivery) or remove it; disclose the behaviour to users regardless.

H2 — Immediate: Remove `WRITE_CONTACTS` entirely unless a specific, disclosed feature requires it; scope `READ_CONTACTS` to the minimum needed for any retained feature and disclose the purpose explicitly.

C3 — Immediate: Document the Art. 9(2)(h) legal basis, retention period, and any recipients for audio data generated during telemedicine consultations, and disclose this clearly to insured people before any video/audio consultation begins.

Across all findings: establish a functioning intake channel for external security and privacy disclosures. The original disclosure addresses, datenschutz@oegk.at and info@oegk.at, both bounced, and even after a working channel was found and used for four subsequent messages over 92 days, no reply of any kind was ever sent. For a statutory body serving 8.5 million people, a non-functional disclosure intake process is itself an operational gap worth correcting independently of the findings in this report.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis of

the published application using publicly available tooling. No ÖGK servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory

