Koordinierte Offenlegung, Abschlussbericht

Zurich ZAPP Android (at.zurich.zapp) + Zurich ZIO Android (com.zurich.ziomob2)

Zurich Insurance Group, Österreich (SIX: ZURN)

GENERISCHE ZUSAGE OHNE FOLGE-BESTÄTIGUNG · FALL GESCHLOSSEN UND VERÖFFENTLICHT AM 26. SEPTEMBER 2026, AM ANGEGEBENEN EMBARGO-DATUM

Ziel	Zurich Insurance Group, Österreich
Package	at.zurich.zapp v5.0.0, com.zurich.ziomob2 v1.3.2 (versionCode 2026061201)
Betreiber	Zurich Insurance Group AG, Zweigniederlassung Österreich
Erstmeldung	2026-06-26
Angegebenes Embargo	2026-09-26, dem Betreiber direkt in der Erstmeldung mitgeteilt
Bericht veröffentlicht	2026-09-26, zum angegebenen Datum
Behörden	Österreichische Datenschutzbehörde (DSB), Finanzmarktaufsicht (FMA)
Ausgehende Nachrichten gesamt	6 über 72 Tage, an datenschutz@at.zurich.com und dpo@at.zurich.com.
Eingehende Antworten	Eine generische Zwischennachricht am 28. Juli 2026, ohne inhaltliche Bestätigung oder Widerlegung eines der vier Befunde, keine weitere Rückmeldung in den folgenden 60 Tagen.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Am 26. Juni 2026 meldete RFI-IRFOS vier Befunde in zwei österreichischen Zurich-Apps. Ein Firebase-API-Schlüssel ist in beiden Apps hardcodiert, und FirebaseInitProvider initialisiert vor jedem Einwilligungssignal. Dieser Befund korrigiert sich auf HIGH/8.8 unter CVSS v4.0.

Ein zweiter Befund: die Mobility-App ZIO startet per BOOT_COMPLETED-Receiver automatisch bei jedem Geräteneustart und greift dabei auf Standortdaten zu, bevor die Nutzerin oder der Nutzer die App je geöffnet hat. Rechnerisch erreicht dieser Befund unter CVSS v4.0 nur LOW/2.4, da das Modell für Einzelgeräte-Angriffsszenarien ausgelegt ist. RFI-IRFOS hebt ihn wegen des landesweiten Kundenbestands beider Apps und der systematischen, nutzerunabhängigen Auslösung auf MEDIUM an (RFI-IRFOS-Blast-Radius-Eskalation).

Ein dritter Befund, MEDIUM: das Firebase-Projekt corp-airship—prod verweist auf Urban Airship (Airship, USA), eine Marketing-Automation-Plattform, die in der Datenschutzerklärung keiner der beiden Apps als Auftragsverarbeiter genannt ist. Ein vierter Befund, ebenfalls MEDIUM: ZAPP besitzt kein Network-Security-Config-File, das Standardverhalten für Netzwerkverkehr bleibt damit undokumentiert.

Sechs Nachrichten wurden über 72 Tage gesendet. Am 28. Juli 2026 bestätigte dpo@at.zurich.com den Eingang der Meldung mit einer generischen Zusage, die Befunde zu prüfen und, sofern zutreffend, zu beheben, ohne einen der vier Befunde inhaltlich zu bestätigen oder zu widerlegen. Auf drei weitere Nachrichten über die folgenden 60 Tage erfolgte keine Rückmeldung mehr. Die österreichische Finanzmarktaufsicht antwortete zweimal mit einem automatisierten Verweis auf ihren Verbraucherkanal, keine dieser Antworten stammt von Zurich selbst. Das 90-Tage-Embargo, dem Betreiber direkt mitgeteilt, läuft heute ab. Dieser Bericht und die begleitende Abschlussmitteilung veröffentlichen zum angegebenen Datum.

Scope: Root-Level-Code-Analyse der produktiven Zurich-ZAPP-App (at.zurich.zapp, Version 5.0.0) und der Zurich-ZIO-App (com.zurich.ziomob2, Version 1.3.2), direkt von einem Produktivgerät mit Android 15 extrahiert und am 26. Juni 2026 untersucht. Es wurde kein Konto angelegt, und es fand keine Interaktion mit der Backend-Infrastruktur von Zurich, Firebase oder Urban Airship statt.

Disposition

Vier Befunde wurden am 26. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Der hardcodierte Firebase-Schlüssel mit Pre-Consent-Initialisierung korrigiert sich auf HIGH. Die undokumentierte Urban-Airship-Anbindung und das fehlende Network-Security-Config-File korrigieren sich auf MEDIUM. Der Autostart-Befund korrigiert sich rechnerisch auf LOW, RFI-IRFOS hebt ihn wegen des landesweiten Kundenbestands beider Apps auf MEDIUM an. Zurich bestätigte am 28. Juli 2026 lediglich den Eingang und kündigte eine Prüfung an, ohne einen der vier Befunde inhaltlich zu bestätigen oder zu widerlegen; auf drei weitere Nachrichten über 60 Tage folgte keine Rückmeldung mehr.

ID	Severity	Title
B1	HIGH	Firebase-API-Schlüssel hardcodiert in beiden Apps, Pre-Consent-Initialisierung
B2	MEDIUM	BOOT_COMPLETED-Autostart mit Standortzugriff nach jedem Geräteneustart
B3	MEDIUM	Urban Airship als undisclosed Marketing-Backend
B4	MEDIUM	Kein Network Security Configuration File in ZAPP

Die Antwort vom 28. Juli 2026

dpo@at.zurich.com bestätigte am 28. Juli 2026 den Eingang der Meldung mit dem Satz, man analysiere die Befunde bereits und werde sie, sofern evident, ehestmöglich beheben. Keiner der vier Befunde wurde darin inhaltlich bestätigt oder widerlegt. Auf drei weitere Nachrichten am 12. August, 24. August und 6. September 2026 erfolgte keine weitere Rückmeldung von Zurich. Die österreichische Finanzmarktaufsicht antwortete zweimal automatisiert mit einem Verweis auf ihren Verbraucherkanal, diese Antworten stammen nicht von Zurich.

Findings

B1: Firebase-API-Schlüssel hardcodiert in beiden Apps, Pre-Consent-Initialisierung

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8.

Ein Firebase-API-Schlüssel ist im Play-Store-Binary beider Apps (ZAPP und ZIO) hardcodiert. FirebaseInitProvider initialisiert automatisch beim App-Start, bevor irgendein Einwilligungssignal vorliegt.

```
google_api_key (Firebase, in beiden Binaries at.zurich.zapp und com.zurich.ziomob2
    identisch extrahierbar)
FirebaseInitProvider (initOrder=100, vor Consent-Screen)
```

Impact: Jeder, der eine der beiden APKs herunterlädt, kann den Schlüssel extrahieren. Nutzungsdaten werden zudem bereits beim App-Start erfasst, unabhängig von jeder Einwilligung. Art. 7, Art. 32 DSGVO.

Fix: Schlüssel nach Package-Name und Zertifikat einschränken, Firebase-Initialisierung hinter einen Consent-Mechanismus stellen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B2: BOOT_COMPLETED-Autostart mit Standortzugriff nach jedem Geräteneustart

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

Die Mobility-App ZIO registriert einen BOOT_COMPLETED-Receiver, der die App bei jedem Geräteneustart automatisch im Hintergrund startet und dabei auf Standortdaten zugreift, bevor die Nutzerin oder der Nutzer die App je geöffnet hat. RFI-IRFOS blast-radius escalation: raised from LOW/2.4 to MEDIUM because CVSS models single-device adversarial scenarios and does not capture the systematic, user-independent trigger across the entire Austrian customer base of both apps.

```
AndroidManifest.xml: <receiver ...>
  <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></intent
    -filter>
</receiver>
ACCESS_FINE_LOCATION im Autostart-Pfad
```

Impact: Standorterfassung beginnt vor jeder bewussten Nutzungsentscheidung, systematisch bei jedem Neustart, über den gesamten Kundenbestand der Mobility/Telematik-App. Art. 5(1)(c), Art. 7 DSGVO.

Fix: BOOT_COMPLETED-Autostart entfernen oder an eine vorherige aktive Nutzerinteraktion binden. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B3: Urban Airship als undisclosed Marketing-Backend

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.

Das Firebase-Projekt corp-airship—prod verweist auf Urban Airship (Airship, USA) als Marketing-Backend für ZIO. Airship ist in der Datenschutzerklärung keiner der beiden Apps als Auftragsverarbeiter genannt.

```
Firebase-Projekt: corp-airship---prod
Urban Airship SDK (Airship, USA)
```

Impact: Versicherungskundendaten fließen an einen namentlich nicht genannten US-Auftragsverarbeiter. Art. 13, Art. 44 DSGVO.

Fix: Urban Airship namentlich als Auftragsverarbeiter offenlegen oder Integration entfernen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B4: Kein Network Security Configuration File in ZAPP

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3.

ZAPP enthält keine res/xml/network_security_config.xml, das Standardverhalten für Netzwerkverkehr bleibt damit undokumentiert und ungehärtet.

Impact: Ohne dokumentierte Network Security Configuration ist unklar, welche Verschlüsselungsgarantien für den Netzwerkverkehr der Versicherungs-App tatsächlich gelten. Art. 25, Art. 32 DSGVO.

Fix: Network Security Configuration mit expliziter TLS-Pinning-Konfiguration ergänzen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

Datenschutz, Artikel für Artikel

Die Befunde ordnen sich einer kleinen, spezifischen Gruppe von DSGVO-Bestimmungen zu, hier gesammelt statt über die Befunde verstreut.

Artikel	Befund	Grundlage
Art. 7, Art. 32 DSGVO	B1	Firebase-API-Schlüssel hardcodiert, Pre-Consent-Initialisierung.
Art. 5(1)(c), Art. 7 DSGVO	B2	BOOT_COMPLETED-Autostart mit Standortzugriff.
Art. 13, Art. 44 DSGVO	B3	Urban Airship als undisclosed Marketing-Backend.
Art. 25, Art. 32 DSGVO	B4	Kein Network Security Configuration File.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 ist die Scoring-Richtlinie von RFI-IRFOS, keine Ober- oder Untergrenze. Sie liefert einen reproduzierbaren, für Dritte nachvollziehbaren Ausgangspunkt für den Schweregrad und erfasst reale Blast-Radius-Effekte nicht von sich aus. In diesem Bericht korrigiert sich B1 auf HIGH, B3 und B4 korrigieren sich auf MEDIUM auf ihrer eigenen berechneten Stufe, B2 wird von CVSS-LOW auf MEDIUM als RFI-IRFOS-Blast-Radius-Eskalation angehoben. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: ZURICH-AT-2026.