Koordinierte Offenlegung, Abschlussbericht

myUNIQA Android (at.uniqa.myuniqa.ionic)

UNIQA Insurance Group AG, Wien, Österreich (ATX: UNQS)

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

Ziel	UNIQA Insurance Group AG, Wien, Österreich
Package	at.uniqa.myuniqa.ionic, Version 2.619.0 (versionCode 215182)
Betreiber	UNIQA Insurance Group AG
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 78 Tage, an datenschutz@uniqa.at, security@uniqa.at (dauerhaft unzustellbar) und presse@uniqa.at.
Eingehende Antworten	Eine generische Zwischennachricht am 31. Juli 2026, ohne inhaltliche Bestätigung oder Widerlegung eines der vier Befunde, danach nur noch automatisierte Eingangsbestätigungen.

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 der myUNIQA-App. Ein Firebase-API-Schlüssel ist im Play-Store-Binary hardcodiert, und FirebaseInitProvider initialisiert vor jedem Einwilligungssignal. Dieser Befund korrigiert sich auf HIGH/8.8 unter CVSS v4.0.

Ein zweiter Befund: der Dynatrace OneAgent erfasst Nutzerinteraktionen auf Bildschirmebene, welche Felder ausgefüllt werden, wie lange auf welchem Formular verweilt wird, welche Aktionen ausgeführt werden, auf einer Kranken- und Lebensversicherungs-App. Formulareingaben bei Schadenmeldung, Vertragsabschluss und Leistungsabrechnung fließen als Verhaltensdaten in Echtzeit zu Dynatrace-Servern in den USA, Dynatrace erscheint in der Datenschutzerklärung nicht als Auftragsverarbeiter. Dieser Befund korrigiert sich auf HIGH/8.7.

Ein dritter Befund, ebenfalls HIGH/8.7: das Kofax-SDK (2.395 Klassen) verarbeitet Dokumentenaufnahmen wie Arztbriefe, Krankenhausentlassungsberichte, Laborergebnisse und Schadenmeldungen mit medizinischen Angaben. Ob und in welchem Umfang OCR-Ergebnisse oder Rohdokumente an Kofax-Server in den USA übermittelt werden, ist aus der Datenschutzerklärung nicht ersichtlich. Ein vierter Befund, MEDIUM/6.9: das Unblu-SDK kann während aktiver Beratungsgespräche im Hintergrund auf das Mikrofon zugreifen, ohne dass erkennbar ist, ob Gesprächsinhalte bei Unblu in der Schweiz oder den USA gespeichert werden.

Positiv vermerkt: myUNIQA verfügt über eine korrekt konfigurierte Network Security Configuration ohne Klartext-HTTP als Standard, und es gibt keinen BOOT_COMPLETED-Autostart. Sechs Nachrichten wurden über 78 Tage gesendet. UNIQA bestätigte am 31. Juli 2026 den Eingang mit einer generischen Zusage, die Punkte sorgfältig zu prüfen, ohne einen der vier Befunde inhaltlich zu bestätigen oder zu widerlegen. Auf drei weitere Nachrichten über die folgenden 43 Tage antwortete ausschließlich der automatisierte UNIQA-Automailer, keine weitere menschliche Rückmeldung. 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 myUNIQA-App (at.uniqa.myuniqa.ionic, Version 2.619.0), 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 UNIQA, Dynatrace, Kofax oder Unblu statt.

Disposition

Vier Befunde wurden am 26. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Der hardcodierte Firebase-Schlüssel, das Dynatrace-Real-User-Monitoring auf Versicherungsformularen und das Kofax-Dokumenten-OCR korrigieren sich jeweils auf HIGH. Das Unblu-Live-Audio-SDK korrigiert sich auf MEDIUM. UNIQA bestätigte am 31. Juli 2026 lediglich den Eingang mit einer generischen Zusage, die Punkte sorgfältig zu prüfen, ohne einen der vier Befunde inhaltlich zu bestätigen oder zu widerlegen; auf drei weitere Nachrichten über 43 Tage folgten nur automatisierte Eingangsbestätigungen des UNIQA-Automailers, keine weitere menschliche Antwort.

ID	Severity	Title
B1	HIGH	Firebase-API-Schlüssel hardcodiert, Pre-Consent-Initialisierung
B2	HIGH	Dynatrace Real-User-Monitoring auf Versicherungs-formularen
B3	HIGH	Kofax-Dokumenten-OCR für Arztbriefe und Ver-sicherungsrechnungen
B4	MEDIUM	Unblu-Live-Audio-Stream von Versicherungsberatun-gen

Was myUNIQA richtig macht

myUNIQA verfügt über eine korrekt konfigurierte Network Security Configuration mit clearte xtTrafficPermitted="false" als globalem Standard, kein unverschlüsselter HTTP-Verkehr ist damit vorgesehen. Die App registriert außerdem keinen BOOT_COMPLETED-Receiver und startet nicht automatisch nach Geräteneustarts. Beides ist ein messbarer Qualitätsunterschi ed zu anderen geprüften Apps dieser Serie und wird ausdrücklich anerkannt.

Die Antwort vom 31. Juli 2026

presse@uniqa.at bestätigte am 31. Juli 2026 den Eingang der Meldung mit dem Satz, die Sicherheit der Systeme habe höchste Priorität und man prüfe die angesprochenen Punkte sorgfältig. Keiner der vier Befunde wurde darin inhaltlich bestätigt oder widerlegt, keine der drei gestellten Ja/Nein-Fragen wurde beantwortet. Auf drei weitere Nachrichten am 15. August, 3. September und 12. September 2026 antwortete ausschließlich der automatisierte UNIQA-Automailer mit einer generischen Eingangsbestätigung, keine weitere menschliche Rückmeldung erfolgte.

Findings

B1: Firebase-API-Schlüssel hardcodiert, 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 und die zugehörige App-ID sind im Play-Store-Binary hardcodiert. FirebaseInitProvider initialisiert automatisch vor dem ersten App-Bildschirm, vor jeder Einwilligungsmöglichkeit.

```
res/values/strings.xml
google_api_key = AIzaSyDn2OABRsj1mF_O8NBw5E2LNhLnD5kB6jg
google_app_id = 1:238222096769:android:58a0048d1a0dbc62e21080
FirebaseInitProvider (initOrder=100, directBootAware=true)
```

Impact: Missbrauchsvektoren: Quota-Erschöpfung, FCM-Push-Spoofing, Storage-Bucket-Zugriff bei fehlkonfigurierten Firebase-Regeln. Nutzungsdaten werden zudem bereits vor jeder Einwilligung erfasst. 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: Dynatrace Real-User-Monitoring auf Versicherungsformularen

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

Der Dynatrace OneAgent erfasst Nutzerinteraktionen auf Bildschirmebene: welche Felder ausgefüllt werden, wie lange auf welchem Formular verweilt wird, welche Aktionen ausgeführt werden. Auf einer Kranken- und Lebensversicherungs-App fließen damit Formulareingaben bei Schadenmeldung, Vertragsabschluss und Leistungsabrechnung als Verhaltensdaten in Echtzeit zu Dynatrace-Servern in den USA.

```
smali/com/dynatrace/cordova/plugin/DynatraceCordovaPlugin.smali
const-string v3, "dataCollectionLevel" (OFF / PERFORMANCE / USER_BEHAVIOR)
smali/com/dynatrace/agent/storage/db/OneAgentDatabase_Impl.smali
CREATE TABLE events (id, event, timestamp, isPriorityData, eventSizeBytes)
```

Impact: Gesundheitsdaten (Art. 9 DSGVO) aus Schadenmeldungen und Vertragsabschluss fließen an einen in der Datenschutzerklärung nicht als Auftragsverarbeiter genannten US-Anbieter. Art. 9, Art. 13, Art. 44 DSGVO.

Fix: Dynatrace namentlich als Auftragsverarbeiter offenlegen und Rechtsgrundlage nach Art. 9(2) DSGVO dokumentieren, oder Real-User-Monitoring auf Formularen mit Gesundheitsbezug deaktivieren. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B3: Kofax-Dokumenten-OCR für Arztbriefe und Versicherungsrechnungen

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

Das Kofax-SDK (2.395 smali-Klassen, Kofax Inc., Irvine, Kalifornien) verarbeitet Dokumentenaufnahmen. Im Kontext einer Kranken- und Lebensversicherungs-App sind das typischerweise Arztbriefe, Krankenhausentlassungsberichte, Laborergebnisse und Schadenmeldungen mit medizinischen Angaben. Ob und in welchem Umfang OCR-Ergebnisse oder Rohdokumente an Kofax-Server übermittelt werden, ist aus der Datenschutzerklärung nicht ersichtlich.

```
com/kofax/android/abc/ (Agility Barcode Capture)
com/kofax/android/isg/ (Image Services Gateway, Bildverarbeitung)
2.395 smali-Klassen aus com/kofax/android/
```

Impact: Dokumente mit Art. 9 Gesundheitsdaten verlassen möglicherweise die EU an einen namentlich nicht genannten US-Auftragsverarbeiter. Art. 9, Art. 13, Art. 44 DSGVO.

Fix: Kofax namentlich als Auftragsverarbeiter offenlegen und Datenschutz-Folgenabschätzung um die Dokumentenübermittlung ergänzen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B4: Unblu-Live-Audio-Stream von Versicherungsberatungen

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 Unblu-SDK (409 smali-Klassen, Unblu AG, Basel) registriert einen Hintergrunddienst mit foregroundServiceType=”microphone”, der während eines aktiven Beratungsgesprächs im Hintergrund auf das Mikrofon zugreifen kann. Ob Gesprächsinhalte bei Unblu gespeichert oder verarbeitet werden, ist aus der Datenschutzerklärung nicht erkennbar.

```
AndroidManifest.xml: <service android:name="com.unblu.sdk.core.module.call.
    UnbluBackgroundCallService" android:foregroundServiceType="microphone"/>
smali_classes2/L7/b$c.smali: AudioRecord.startRecording()
```

Impact: Beratungsgespräche zu Kranken-, Lebensversicherung oder Schadenabwicklung sind naturgemäß sensibel, ihre Speicherbedingungen bei einem Anbieter mit Schweizer und US-Infrastruktur bleiben undokumentiert. Art. 13, Art. 44 DSGVO.

Fix: Speicherort und -dauer der Gesprächsinhalte in der Datenschutzerklärung offenlegen. 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. 9, Art. 13, Art. 44 DSGVO	B2	Dynatrace Real-User-Monitoring auf Versicherungsformularen.
Art. 9, Art. 13, Art. 44 DSGVO	B3	Kofax-Dokumenten-OCR für Arztbriefe und Versicherungsrechnungen.
Art. 13, Art. 44 DSGVO	B4	Unblu-Live-Audio-Stream von Versicherungsberatungen.

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 korrigieren sich B1, B2 und B3 auf HIGH, B4 korrigiert sich auf MEDIUM, jeweils auf ihrer eigenen berechneten Stufe. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: UNIQA-MYUNIQA-2026.