# Koordinierte Sicherheits- und Datenschutz-Offenlegung, Abschlussbericht

## Mein ELBA-App (at.rsg.pfp) und Raiffeisen Kapitalmarkt (at.raiffeisen.kapitalmarkt) für Android

Neun schriftliche Benachrichtigungen, sechs erfolgreiche Zustellungen nach anfänglichen Bounces an vier verschiedene Adressen, null Antworten

**ÖFFENTLICHE OFFENLEGUNG, 19. SEPTEMBER 2026 – ACHT BEFUNDE, KEINE EINZIGE ANTWORT**

| | |
|---|---|
| **Target** | Raiffeisen Digital GmbH / Raiffeisen Bank International AG, Wien, Österreich |
| **Geprüfte Produkte** | Mein ELBA-App (at.rsg.pfp, v1.180.0) und Raiffeisen Kapitalmarkt (at.raiffeisen.kapitalmarkt) |
| **Offenlegungsreferenz** | REF AT-RAIFFEISEN-2026-R1 |
| **R1 gesendet** | 2026-06-21 |
| **Offenlegungs-/Embargodatum** | 2026-09-19 |
| **Bericht veröffentlicht** | 2026-09-19 |
| **Schweregrad** | HIGH (E-C1, fest kodierter Firebase-Schlüssel als FCM-Phishing-Vektor auf einer Bank-App, CVSS v4.0 8.8, unbeantwortet) |

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

## Contents

## Executive Summary

Am 21. Juni 2026 führte RFI-IRFOS eine statische Analyse zweier produktiver Raiffeisen-Android-Apps durch, der Retail-Banking-App Mein ELBA-App und der Investment-App Raiffeisen Kapitalmarkt, und identifizierte drei CRITICAL-, vier HIGH- und einen MEDIUM-Befund: bei Raiffeisen Kapitalmarkt ein aktiviertes, ungeschütztes Android-Backup, über das das vollständige Investmentportfolio samt Transaktionshistorie ohne Root über ADB extrahierbar ist, einen fest kodierten Firebase-Schlüssel mit aktiviertem Crashlytics, das Handelssitzungskontext an Google-US-Infrastruktur überträgt, sowie das vollständige Fehlen von Certificate Pinning auf allen Handels-Endpunkten. Bei Mein ELBA-App einen fest kodierten Firebase-Schlüssel, der gefälschte Push-Benachrichtigungen ermöglicht, ein direkter Phishing-Vektor in eine Banking-App, sowie undeklarierte Android-Ad-Services-Attribution-Tracking-Berechtigungen auf einer Retail-Banking-App.

Die ursprüngliche R1-Zustellung scheiterte an zwei ungültigen Adressen und wurde erst nach zwei weiteren gescheiterten Zustellversuchen an zwei zusätzliche ungültige Adressen am 2. Juli 2026 erfolgreich an funktionierende Adressen der Konzernmutter zugestellt. Ab diesem Zeitpunkt wurden sechs weitere schriftliche Benachrichtigungen gesendet, cc die österreichische Datenschutzbehörde, mit expliziten Fristen und einer förmlichen Berufung auf die 72-Stunden-Meldepflicht nach Art. 33(4) DSGVO.

Auf keine einzige der insgesamt neun Benachrichtigungen kam von Raiffeisen jemals eine Antwort, weder eine Bestätigung, noch ein Dementi, noch eine automatische Empfangsbestätigung. Alle acht Befunde bleiben zum Zeitpunkt der Veröffentlichung unverändert offen.

**Scope:** Statische Analyse der öffentlich über den Google Play Store bezogenen produktiven APKs beider Apps, auf einem autorisierten Testgerät, ausschließlich. Es wurden keine Raiffeisen-Konten, Backend-Systeme oder Infrastruktur zugegriffen oder getestet.

### Disposition

R1 wurde am 21. Juni 2026 an datenschutz@raiffeisen.at gesendet; diese und drei weitere Adressen erwiesen sich als ungültig und wurden erst am 2. Juli 2026 durch funktionierende Adressen (datenschutz@rbinternational.com, datenschutzbeauftragter@rbinternational.com) ersetzt. Ab der ersten erfolgreichen Zustellung wurden sechs weitere schriftliche Benachrichtigungen gesendet, cc die österreichische Datenschutzbehörde. Auf keine einzige davon kam eine Antwort, weder eine Bestätigung, noch ein Dementi, noch eine automatische Empfangsbestätigung.

| ID | Severity | Title |
|---|---|---|
| K-C1 | CRITICAL | Raiffeisen Kapitalmarkt: aktiviertes, ungeschütztes Android-Backup, vollständiges Investmentportfolio per ADB extrahierbar |
| K-C2 | CRITICAL | Raiffeisen Kapitalmarkt: fest kodierter Firebase-Schlüssel, Crashlytics aktiviert, Handelssitzungskontext an Google US |

| ID | Severity | Title |
|---|---|---|
| E-C1 | CRITICAL | Mein ELBA-App: fest kodierter Firebase-Schlüssel, FCM-Phishing-Vektor |
| K-H1 | HIGH | Raiffeisen Kapitalmarkt: kein Certificate Pinning auf Handels-Endpunkten |
| K-H2 | HIGH | Raiffeisen Kapitalmarkt: Crashlytics-Handelssitzungskontext, gesondert von K-C2 gelistet |
| E-H1 | HIGH | Mein ELBA-App: undeklariertes Android-Ad-Services-Attribution-Tracking auf einer Bank-App |
| E-H2 | HIGH | Mein ELBA-App: Firebase Cloud Messaging leitet Banking-Push-Benachrichtigungen über Google-US-Infrastruktur |
| E-M1 | MEDIUM | Mein ELBA-App: WebView setAllowFileAccess(true) explizit gesetzt |

## Betreiberanalyse

Raiffeisen Digital GmbH entwickelt beide geprüften Apps im Auftrag der Raiffeisen Bank International AG / Raiffeisen Zentralbank Österreich AG, unter Aufsicht der österreichischen Datenschutzbehörde.

## Findings

### K-C1: Raiffeisen Kapitalmarkt: aktiviertes, ungeschütztes Android-Backup, vollständiges Investmentportfolio per ADB extrahierbar

**MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 6.8**

android:allowBackup="true" mit einer leeren backup_rules.xml (vollständiges <full-backup-content />) und einer leeren data_extraction_rules.xml (uneingeschränktes <cloud-backup />). Extraktion erfordert lediglich ein entsperrtes Gerät, kein Root: adb backup -f portfolio.ab at.raiffeisen.kapitalmarkt.

Extrahierte Daten umfassen Portfoliobestände, Stückzahlen, Einstandspreise, Orderhistorie, Session-Tokens und sämtliche lokal zwischengespeicherten Finanzdaten. Dies steht im Widerspruch zu den Vertraulichkeitspflichten der MiFID II für Wertpapierdienstleistungen. Keine Reaktion von Raiffeisen zu diesem oder irgendeinem anderen Befund.

**Impact:** Physischer Zugriff auf ein entsperrtes Gerät genügt, um das vollständige Investmentportfolio eines Nutzers zu extrahieren.

**Fix:** allowBackup auf false setzen oder eine tatsächlich restriktive Backup-Konfiguration implementieren, die Finanzdaten explizit ausschließt.

### K-C2: Raiffeisen Kapitalmarkt: fest kodierter Firebase-Schlüssel, Crashlytics aktiviert, Handelssitzungskontext an Google US

**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**

Firebase-Schlüssel AIzaSyCbeU5fZrb4G4JV6uhbAwcW4ZgKqhkvX10, mit firebase_crashlytics_collection_enabled=true. Zum Vergleich: dieselbe Entwicklerorganisation setzt dies bei Mein ELBA-App explizit auf false.

Java-Stacktraces zum Absturzzeitpunkt können Portfoliozustandsobjekte, Ordermengen und -preise sowie Kontostände enthalten und werden an Google-Crashlytics-Infrastruktur in den USA übertragen, ein MiFID-II-Vertraulichkeitskonflikt. Keine Reaktion von Raiffeisen.

**Impact:** Vertrauliche Handelsdaten können bei einem App-Absturz unkontrolliert an einen US-Drittanbieter gelangen.

**Fix:** Crashlytics für diese App deaktivieren, wie es bei Mein ELBA-App bereits der Fall ist, oder Stacktraces vor Übertragung bereinigen.

### E-C1: Mein ELBA-App: fest kodierter Firebase-Schlüssel, FCM-Phishing-Vektor

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

Firebase-Schlüssel AIzaSyBLZsVWMnRvvVIpSId59DD7wxFFrVuzmT4, offengelegt in der verteilten APK.

Ermöglicht einem Angreifer, ohne jede Backend-Kompromittierung gefälschte FCM-Push-Benachrichtigungen an ELBA-Nutzer zu senden, etwa gefälschte Transaktionsbestätigungen, gefälschte 'Zugangsdaten bestätigen'-Overlays oder gefälschte Sicherheitswarnungen, ein direkter Phishing-Vektor in eine Banking-App. Keine Reaktion von Raiffeisen.

**Impact:** Ein einziger fest kodierter Schlüssel genügt, um Bank-Kund*innen gezielt und glaubwürdig zu phishen.

**Fix:** Schlüssel rotieren und auf Paketnamen und Signaturzertifikat beschränken.

### K-H1: Raiffeisen Kapitalmarkt: kein Certificate Pinning auf Handels-Endpunkten

**HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1**

Keine Network Security Config in der Kapitalmarkt-App vorhanden, kein Certificate Pinning für irgendeinen Handels-Endpunkt.

Im direkten Vergleich verfügt Mein ELBA-App derselben Entwicklerorganisation über eine der striktesten Network-Security-Konfigurationen dieser gesamten Prüfserie, mit Custom-CA-Pinning ohne Ablaufdatum auf allen Raiffeisen-Endpunkten. Keine Reaktion von Raiffeisen.

**Impact:** Ein Angreifer mit einem systemvertrauten Zertifikat kann Handelsverkehr auf kompromittierten Netzwerken abfangen.

**Fix:** Certificate Pinning auf demselben Niveau wie Mein ELBA-App implementieren.

### K-H2: Raiffeisen Kapitalmarkt: Crashlytics-Handelssitzungskontext, gesondert von K-C2 gelistet

**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**

In der ursprünglichen Befundtabelle gesondert als eigener HIGH-Punkt geführt: Crashlytics-Erfassung von Handelssitzungskontext (Portfoliozustand, Orderdaten), übertragen an Google-US-Infrastruktur.

Technisch derselbe Mechanismus wie K-C2, ursprünglich separat kategorisiert; keine Reaktion von Raiffeisen zu keinem der beiden.

**Impact:** Siehe K-C2.

**Fix:** Siehe K-C2.

### E-H1: Mein ELBA-App: undeklariertes Android-Ad-Services-Attribution-Tracking auf einer Bank-App

**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**

ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID und der Install-Referrer-Dienst sind deklariert, die Android-Privacy-Sandbox-Ad-Services-API für Kampagnen-Attribution auf einer Retail-Banking-App.

Dieser Zweck ist in der Datenschutzerklärung von Mein ELBA-App nicht offengelegt und für eine Banking-App unverhältnismäßig. Keine Reaktion von Raiffeisen.

**Impact:** Eine Werbe-Kennung wird mit der Installation einer Banking-App verknüpft, ohne entsprechende Offenlegung.

**Fix:** Die Ad-Services-Berechtigungen entfernen oder ihren Zweck explizit in der Datenschutzerklärung benennen.

### E-H2: Mein ELBA-App: Firebase Cloud Messaging leitet Banking-Push-Benachrichtigungen über Google-US-Infrastruktur

**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**

FCM aktiv und für Banking-Push-Benachrichtigungen (Transaktionswarnungen, Login-Bestätigungen) genutzt, geleitet über Google-US-Infrastruktur.

Keine Reaktion von Raiffeisen.

**Impact:** Metadaten zu Banking-Benachrichtigungen durchlaufen US-Infrastruktur ohne gesonderte Offenlegung.

**Fix:** Die Nutzung von FCM für Banking-Benachrichtigungen explizit in der Datenschutzerklärung benennen.

### E-M1: Mein ELBA-App: WebView setAllowFileAccess(true) explizit gesetzt

**LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0**

setAllowFileAccess(true) explizit konfiguriert, kein Android-10+-Standardverhalten.

Deaktiviertes JavaScript mindert das praktische Risiko erheblich. Keine Reaktion von Raiffeisen.

**Impact:** Geringes Restrisiko, durch deaktiviertes JavaScript stark eingeschränkt.

**Fix:** setAllowFileAccess auf false setzen, sofern keine Funktion dies tatsächlich benötigt.

## Null Antworten auf Neun Benachrichtigungen

Die ursprüngliche Zustellung scheiterte an vier ungültigen Adressen, bevor am 2. Juli 2026 funktionierende Adressen der Konzernmutter gefunden wurden. Ab diesem Zeitpunkt wurden sechs weitere Benachrichtigungen gesendet, cc die österreichische Datenschutzbehörde, mit expliziten Fristen und einer förmlichen Berufung auf Art. 33(4) DSGVO. Auf keine einzige kam eine Antwort, weder eine Bestätigung, noch ein Dementi, noch eine automatische Empfangsbestätigung.

## Datenschutz, Artikel für Artikel

| Befund | Bestimmung | Anliegen |
|---|---|---|
| K-C1 | DSGVO Art. 25, Art. 32(1)(a); MiFID II | Ungeschütztes Backup, vollständiges Portfolio extrahierbar |
| K-C2 / K-H2 | DSGVO Art. 28, Art. 32, Art. 46; MiFID II | Handelssitzungskontext an US-Drittanbieter |
| E-C1 | DSGVO Art. 32(2) | Fest kodiertes Credential als Phishing-Vektor |
| K-H1 | DSGVO Art. 32(1)(a) | Kein Certificate Pinning auf Handels-Endpunkten |
| E-H1 | DSGVO Art. 5(1)(c), Art. 13 | Undeklariertes Attribution-Tracking |
| E-H2 | DSGVO Art. 13 | US-geleitete Banking-Benachrichtigungen, nicht offengelegt |

## Offenlegungsverlauf & Ergebnis

| Datum | Ereignis |
|---|---|
| 2026-06-21 | R1 gesendet, scheitert an zwei ungültigen Adressen |
| 2026-06-28 | Erneuter Versand an dieselben (weiterhin ungültigen) Adressen, scheitert erneut |
| 2026-07-02 | Erfolgreiche Zustellung an datenschutz@rbinternational.com und datenschutzbeauftragter@rbinternational.com |
| 2026-07-23 / 08-12 | Follow-ups, österreichische DSB in sichtbares CC aufgenommen |
| 2026-09-04 | Follow-up beruft sich förmlich auf Art. 33(4) DSGVO |
| 2026-09-12 / 09-16 | Letzte Follow-ups bestätigen sechs Zustellungen, null Antworten |
| 2026-09-19 | Embargo, wie in den letzten vier Benachrichtigungen durchgehend angegeben, endet und dieser Bericht wird veröffentlicht |

## Restrisiko & Empfehlungen

- allowBackup bei Raiffeisen Kapitalmarkt deaktivieren oder eine restriktive Backup-Konfiguration implementieren.
- Beide Firebase-Schlüssel rotieren und auf Paketnamen und Signaturzertifikat beschränken.
- Certificate Pinning bei Raiffeisen Kapitalmarkt auf das Niveau von Mein ELBA-App bringen.

**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 Koordinierte Offenlegung gemäß ISO/IEC 29147. Die Forschungstätigkeit ist durch das österreichische Forschungsfreiheitsgesetz (Art. 17 StGG) geschützt. DSGVO Art. 5, 13, 25, 28, 32, 46; MiFID II. REF AT-RAIFFEISEN-2026-R1.