Koordinierte Sicherheits- und Datenschutz-Offenlegung, Abschlussbericht

Jö Bonus Club für Android (at.joeclub.app.joecard)

Eine pauschale Ablehnung durch den Datenschutzbeauftragten, widerlegt durch einen unabhängigen Re-Test desselben Produktions-Builds zweiundfünfzig Tage später

ÖFFENTLICHE OFFENLEGUNG, 19. SEPTEMBER 2026 – ALLE SIEBEN BEFUNDE BEIM RE-TEST UNVERÄNDERT BESTÄTIGT

Target	Unser Ö-Bonus Club GmbH, Wien, Österreich
Geprüftes Produkt	Jö Bonus Club für Android, at.joeclub.app.joecard, v5.0.1 / v5.2.1
Offenlegungsreferenz	REF JOE-2026-R1
R1 gesendet	2026-06-20
Offenlegungs-/Embargodatum	2026-09-19
Bericht veröffentlicht	2026-09-19
Schweregrad	HIGH (H1 Emarsys Warenkorbdaten an die USA, CVSS v4.0 8.7, beim Re-Test aktiv bestätigt, entgegen der Darstellung des Dat enschutzbeauftragten)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Betreiberanalyse 4

3 Findings 4

3.1 C1: Fest kodierte Firebase-Produktionscredentials, seit Offenlegung unrotiert . 5

3.2 C2: Chucker-HTTP-Debug-Interceptor aktiv im Produktions-Build, Widerspruch zur 'No-Op-Stub'-Behauptung beim Re-Test bestätigt 5

3.3 C3: Kein Certificate Pinning auf einer zahlungsfähigen Loyalty-Plattform 6

3.4 H1: SAP Emarsys Predict überträgt Warenkorbinhalte an eine US-Marketing-Cloud, aktive Konfiguration entgegen der Darstellung bestätigt 6

3.5 H2: Mixpanel-Verhaltensanalyse an die USA, unkommentiert bis zum Re-Test 7

3.6 H3: Vollständig itemisierte digitale Kassenbons ermöglichen Art.-9-Rückschlüsse 7

3.7 H4: Präzise GPS- und Bluetooth-Ortung ohne erkennbaren funktionalen Bedarf 8

4 Eine Ablehnung, ein Re-Test, ein Widerspruch 8

5 Ein separater, nicht in diesem Bericht enthaltener Fall 8

6 Datenschutz, Artikel für Artikel 9

7 Offenlegungsverlauf & Ergebnis 10

8 Restrisiko & Empfehlungen 11

Executive Summary

Am 20. Juni 2026 führte RFI-IRFOS eine statische Analyse der produktiven Jö-Bonus-Club-Android-App durch und identifizierte drei CRITICAL- und vier HIGH-Befunde: einen fest kodierten Firebase-Produktionsschlüssel, einen vollständig funktionsfähigen Chucker-HTTP-Debug-Interceptor im Produktions-Build, der Punktestände, Kaufhistorie und Zahlungsdaten lokal im Klartext speichert, das vollständige Fehlen von Certificate Pinning auf einer zahlungsfähigen Loyalty-Plattform, ein SAP-Emarsys-Predict-Modul, das Warenkorbinhalte an eine US-Marketing-Cloud überträgt, Mixpanel-Verhaltensanalyse ohne gültigen EU-Angemessenheitsbeschluss, vollständig aufgeschlüsselte digitale Kassenbons mit Rückschlussmöglichkeit auf Art.-9-Daten, sowie präzise GPS- und Bluetooth-Ortung ohne erkennbaren funktionalen Bedarf.

Christoph Wenin, Datenschutzbeauftragter, antwortete am 7. Juli 2026 substanziell: sämtliche Befunde seien unzutreffend, beruhten auf Fehlinterpretationen. Konkret kommentiert wurden nur drei der sieben Befunde: der Firebase-Schlüssel sei 'gängiger Industriestandard', Chucker sei eine 'nicht-funktionale Stub-Implementierung No-Op, die nur die Build-Kompatibilität sicherstellt', und das Emarsys-Predict-Modul sei 'weder konfiguriert noch aktiv'. Vier Befunde (C3, H2, H3, H4) blieben vollständig unkommentiert. Herr Wenin erklärte den Fall für geschlossen und untersagte weitere Untersuchungen unter Verweis auf rechtliche Konsequenzen.

Ein unabhängiger Re-Test desselben Produktions-Builds (nun v5.2.1) am 2. September 2026 widerlegte die konkret kommentierten Punkte direkt anhand des Binärcodes: die vollständige ChuckerInterceptor-Klassenstruktur samt BodyDecoder, ExportFormat und RetentionManager ist weiterhin vorhanden, mit einer 'No-Op-Stub'-Behauptung nicht vereinbar; die vollständige Emarsys-Kernklassenstruktur samt Activity-Lifecycle-Tracking ist aktiv konfiguriert, nicht inaktiv; und eine zur Laufzeit ausgelesene Konfigurationszeichenkette bestätigte eine aktiv konfigurierte Mixpanel-Instanz, obwohl dieser Befund zuvor unkommentiert geblieben war. Der Firebase-Schlüssel ist seit dem 20. Juni byte-identisch, also nicht rotiert.

Scope: Statische Analyse der öffentlich über den Google Play Store bezogenen produktiven Jö-Bonus-Club-Android-APK, auf einem autorisierten Testgerät, ausschließlich. Es wurden keine Jö-Konten, Backend-Systeme oder Infrastruktur zugegriffen oder getestet.

Disposition

R1 wurde am 20. Juni 2026 an datenschutz@joe-club.at gesendet, BCC an die österreichische Datenschutzbehörde und CERT.at. Der Datenschutzbeauftragte, Christoph Wenin, antwortete mehrfach substanziell, erklärte am 7. Juli 2026 alle sieben Befunde für unzutreffend und erklärte den Fall für geschlossen. Ein unabhängiger Re-Test desselben Produktions-Builds am 2. September 2026 bestätigte alle sieben Befunde unverändert, einschließlich zweier konkreter Punkte, die Wenins eigener Darstellung widersprechen.

ID	Severity	Title
C1	CRITICAL	Fest kodierte Firebase-Produktionscredentials, seit Offenlegung unrotiert
C2	CRITICAL	Chucker-HTTP-Debug-Interceptor aktiv im Produktions-Build, Widerspruch zur 'No-Op-Stub'-Behauptung beim Re-Test bestätigt
C3	CRITICAL	Kein Certificate Pinning auf einer zahlungsfähigen Loyalty-Plattform
H1	HIGH	SAP Emarsys Predict überträgt Warenkorbinhalte an eine US-Marketing-Cloud, aktive Konfiguration entgegen der Darstellung bestätigt
H2	HIGH	Mixpanel-Verhaltensanalyse an die USA, unkommentiert bis zum Re-Test
H3	HIGH	Vollständig itemisierte digitale Kassenbons ermöglichen Art.-9-Rückschlüsse
H4	HIGH	Präzise GPS- und Bluetooth-Ortung ohne erkennbaren funktionalen Bedarf

Betreiberanalyse

Unser Ö-Bonus Club GmbH betreibt das Jö-Bonus-Club-Programm gemeinsam mit mehreren Partnerhändlern der REWE Group, unter Aufsicht der österreichischen Datenschutzbehörde.

Findings

C1: Fest kodierte Firebase-Produktionscredentials, seit Offenlegung unrotiert

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

Google API Key AIzaSyAWutsMfdIeUrk--5wUct8e3c7AnLEFT0E, interner Systemcodename 'mpcard', permanent in jeder installierten App-Version eingebettet und ohne neues APK-Release nicht rotierbar.

Am 7. Juli 2026 listete RFI-IRFOS fünfzehn konkrete Missbrauchsvektoren allein mit diesem Schlüssel auf (Quota-/Billing-DoS, Nutzer-Enumeration, Passwort-Reset-Flut, Fake-Account-Flut, RTDB-Zugriff bei künftiger Regelfehlkonfiguration, Storage-Bucket-Zugriff, Cloud-Functions-Missbrauch und weitere). Herr Wenins Antwort: 'gängiger Industriestandard'. Der Re-Test vom 2. September 2026 bestätigte den Schlüssel als byte-identisch und damit unrotiert seit dem 20. Juni 2026.

Impact: Ein permanent eingebetteter, nicht rotierbarer Produktionsschlüssel bleibt über die gesamte App-Lebensdauer angreifbar, sobald sich Sicherheitsregeln ändern.

Fix: Schlüssel rotieren, auf Paketnamen und Signaturzertifikat beschränken, Firebase-Sicherheitsregeln als deny-by-default bestätigen.

C2: Chucker-HTTP-Debug-Interceptor aktiv im Produktions-Build, Widerspruch zur 'No-Op-Stub'-Behauptung beim Re-Test bestätigt

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1

Vollständig funktionsfähige Klassen ChuckerInterceptor$Builder, ChuckerCollector, BodyDecoder und ExportFormat speichern sämtlichen HTTP/HTTPS-Verkehr lokal im Klartext, einsehbar über eine Benachrichtigungs-UI: Ö-Punkte-Stände, Kaufhistorie, itemisierte digitale Kassenbons und Bluecode-Zahlungsdaten.

Herr Wenins Antwort: 'nicht-funktionale Stub-Implementierungen No-Op, die nur die Build-Kompatibilität sicherstellen.' Der Re-Test vom 2. September 2026 fand dieselben Klassen zusätzlich zu RetentionManager weiterhin vollständig vorhanden, eine Struktur, die mit einer No-Op-Stub-Behauptung nicht vereinbar ist.

Impact: Jeder physische Zugriff auf ein entsperrtes Gerät legt Zahlungs- und Kaufdaten im Klartext offen, ohne dass eine Netzwerkkompromittierung nötig wäre.

Fix: Chucker vollständig aus dem Produktions-Build-Flavor entfernen, mit einer verifizierbaren Gradle-Konfiguration.

C3: Kein Certificate Pinning auf einer zahlungsfähigen Loyalty-Plattform

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.xml in der APK vorhanden. Die App verarbeitet Bluecode-Zahlungen, biometrische Authentifizierung und Ö-Punkte-Transaktionen ohne TLS-Pinning.

Dieser Befund blieb über die gesamte Korrespondenz hinweg vollständig unkommentiert, auch beim Re-Test vom 2. September 2026 unverändert bestätigt.

Impact: Ein Angreifer mit einem systemvertrauten Zertifikat kann Zahlungs- und Transaktionsverkehr auf kompromittierten Netzwerken abfangen.

Fix: Certificate Pinning für alle Zahlungs- und Transaktionsendpunkte implementieren.

H1: SAP Emarsys Predict überträgt Warenkorbinhalte an eine US-Marketing-Cloud, aktive Konfiguration entgegen der Darstellung bestätigt

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

685 Klassen des größten Drittanbieter-SDK der App übertragen Warenkorbinhalte, Kategorien, verknüpfte Nutzeridentität und Push-Token an SAP-Server, mit einer eigens gebauten Produktadapter-Klasse für das Jö-Produktmodell.

Herr Wenins Antwort: 'weder konfiguriert noch aktiv.' Der Re-Test vom 2. September 2026 bestätigte die vollständige Emarsys-Kernklassenstruktur samt Activity-Lifecycle-Tracking und Geräteerkennung als aktiv, nicht als tote Abhängigkeit.

Impact: Detaillierte Warenkorbinhalte werden zu einem kommerziellen Zweck übertragen, der von der ursprünglichen Erhebungsgrundlage (Punktevergabe) abweicht.

Fix: Emarsys Predict entweder tatsächlich deaktivieren oder die Zweckänderung explizit und separat einwilligungspflichtig machen.

H2: Mixpanel-Verhaltensanalyse an die USA, unkommentiert bis zum Re-Test

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

50 Klassen von Mixpanel (San Francisco) erfassen In-App-Verhalten ohne gültigen EU-Angemessenheitsbeschluss nach Schrems II.

Dieser Befund blieb in der Antwort vom 7. Juli vollständig unerwähnt. Der Re-Test vom 2. September 2026 fand eine zur Laufzeit ausgelesene Konfigurationszeichenkette, die eine aktiv konfigurierte Mixpanel-Instanz bestätigt.

Impact: Verhaltensdaten, die mit Kaufaktionen überlappen, werden ohne belastbare Transfergrundlage in die USA übertragen.

Fix: Mixpanel explizit im Datenschutzhinweis benennen und eine Art.-46-Transfergrundlage dokumentieren.

H3: Vollständig itemisierte digitale Kassenbons ermöglichen Art.-9-Rückschlüsse

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

Vollständig itemisierte digitale Kassenbons (Produktname, Menge, Preis) über alle Partnerhändler hinweg können Rückschlüsse auf Gesundheitszustand, Religion und politische Überzeugung ermöglichen.

Dieser Befund blieb über die gesamte Korrespondenz vollständig unkommentiert, auch nach expliziter Nachfrage am 2. September 2026.

Impact: Für ein reines Punktesystem ist die vollständige Item-Ebene nicht erforderlich und schafft ein unnötiges Rückschlussrisiko auf besondere Kategorien personenbezogener Daten.

Fix: Nur aggregierte Kaufdaten für die Punktevergabe verarbeiten, itemisierte Daten nicht dauerhaft speichern.

H4: Präzise GPS- und Bluetooth-Ortung ohne erkennbaren funktionalen Bedarf

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_FINE_LOCATION, BLUETOOTH_SCAN und BLUETOOTH_CONNECT gemeinsam deklariert, ermöglichen eine auf Gangebene genaue In-Store-Ortung.

Der Re-Test vom 2. September 2026 bestätigte, dass BLUETOOTH_SCAN nun das neverForLocation-Flag trägt, eine anerkannte teilweise Härtung, während die eigentliche Notwendigkeit der verbleibenden Ortungsberechtigung weiterhin nicht begründet wurde.

Impact: GPS-Präzision ist für keine genannte Funktion einer Bonuspunkte-App erforderlich.

Fix: Auf grobe Standortdaten umstellen und die verbleibende Notwendigkeit dokumentieren.

Eine Ablehnung, ein Re-Test, ein Widerspruch

Herr Wenins Antwort vom 7. Juli 2026, wörtlich: ”Nach interner technischer und rechtlicher Prüfung halte ich fest, dass sämtliche von Ihnen als kritisch oder hoch klassifizierten Befunde unzutreffend sind.” Drei der sieben Befunde wurden konkret kommentiert, vier blieben vollständig unerwähnt. Der unabhängige Re-Test vom 2. September 2026 widerlegte alle drei konkret kommentierten Punkte direkt anhand des Binärcodes desselben Produktions-Builds, und bestätigte zusätzlich einen der vier unkommentierten Befunde (Mixpanel) als aktiv konfiguriert.

Ein separater, nicht in diesem Bericht enthaltener Fall

Herr Wenin ist zugleich Datenschutzbeauftragter für einen separaten, parallelen RFI-IRFOS-Fall bei BILLA (REWE Group), der aus Effizienzgründen zeitweise im selben E-Mail-Thread geführt wurde. Dieser Bericht behandelt ausschließlich den Jö-Bonus-Club-Fall; der BILLA-Fall wird gesondert und zu seinem eigenen Embargo-Datum behandelt.

Datenschutz, Artikel für Artikel

Befund	Bestimmung	Anliegen
C1	DSGVO Art. 32(1)(b)	Nicht rotierbares, permanent eingebettetes Credential
C2	DSGVO Art. 5(1)(f), Art. 32	Klartext-Zahlungs- und Kaufdaten lokal auf dem Gerät
H1	DSGVO Art. 5(1)(b)	Zweckänderung: Warenkorbdaten für kommerzielle Optimierung
H2	DSGVO Art. 44, Art. 13(1)(f)	US-Datentransfer ohne Angemessenheitsbeschluss
H3	DSGVO Art. 5(1)(c), Art. 9	Übermäßige Itemisierung mit Rückschlussrisiko
H4	DSGVO Art. 5(1)(c)	Übermäßig präzise Standortdaten

Datum	Ereignis

Offenlegungsverlauf & Ergebnis

Datum	Ereignis
2026-06-20	R1 an datenschutz@joe-club.at gesendet, BCC österreichische DSB/CERT.at, 3 CRITICAL + 4 HIGH Befunde
2026-06-24	Herr Wenin antwortet mehrfach substanziell, bittet um persönliches Treffen, RFI-IRFOS besteht auf schriftlicher Kommunikation
2026-07-07	Herr Wenin erklärt alle sieben Befunde für unzutreffend, kommentiert konkret nur drei, erklärt den Fall für geschlossen
2026-08-05	Follow-up: 29 Tage seit Fallschließung, kein konkreter Gegenbeweis je erhalten
2026-09-02	Unabhängiger Re-Test des Produktions-Builds v5.2.1: alle sieben Befunde unverändert bestätigt, drei kommentierte Punkte widerlegt
2026-09-19	Embargo, wie durchgehend in der Korrespondenz angegeben, endet und dieser Bericht wird veröffentlicht

Restrisiko & Empfehlungen

- Chucker tatsächlich aus dem Produktions-Build entfernen und dies durch eine verifizierbare Build-Konfiguration nachweisen.
- Den Firebase-Schlüssel rotieren, seit Offenlegung unverändert.
- Certificate Pinning für alle Zahlungs- und Transaktionsendpunkte implementieren.

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, 9, 13, 32, 44, 46. REF JOE-2026-R1.