Coordinated Security & Privacy Disclosure, Final Report

ÖBB Tickets for Android (at.oebb.ts)

Seven written notices, ninety-one days, one general denial, one refusal to continue correspondence, six findings never technically addressed

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – SIX FINDINGS ON THE NATIONAL RAIL TICKETING APP, ALL UNRESOLVED

Target	ÖBB-Personenverkehr AG, Austria (national rail passenger operator)
Product audited	ÖBB Tickets for Android, at.oebb.ts, v5.2623
Disclosure reference	REF: at.oebb.ts (used throughout the live correspondence)
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1 hardcoded Firebase production key incl. App Distribution API, CVSS v4.0 8.8, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production ÖBB Tickets Android application and identified six findings: a hardcoded Firebase production key with the App Distribution beta-test API present in the shipped build, a complete absence of certificate pinning on a state-operated payment application handling ticket purchases and VorteilsCard/KlimaTicket identity data, an embedded FairTiq SDK transmitting companion and community-tracking data to Switzerland, a shared-infrastructure finding that the standalone FairTiq app routes payment data through China UnionPay with no EU adequacy decision covering that transfer, on-device TensorFlow Lite movement analysis combined with the ACTIVITY_RECOGNITION permission with no documented Art. 6(1) legal basis, and READ_PHONE_STATE/IMEI collection disproportionate to a ticketing app's stated purpose.

ÖBB Kund:innenservice, represented by Luisa Berger, replied twice. On 30 June 2026, a general reply stated the described findings 'in der vorliegenden Form nicht bestätigt' (could not be confirmed in the form presented) without addressing any specific technical claim, reproduction step, or code location, and answered RFI-IRFOS's three standing questions (legal basis, Art. 33 applicability, DPIA obligation) only in the abstract, declining to disclose whether these processes had actually been carried out. On 7 July 2026, following RFI-IRFOS's detailed technical rebuttal with apktool/grep reproduction steps, Berger replied a second time declining to continue correspondence altogether, characterizing the disclosure as an unsolicited commercial contact made in a professional capacity with no business relationship obligating a substantive response, and stated no further correspondence would be conducted on the matter.

No reply of any kind was received after 7 July 2026, across three further RFI-IRFOS notices (23 July, 15 August, 31 August 2026), all cc'd to the Austrian Datenschutzbehörde. None of the six findings received a specific technical response, confirmation, or denial grounded in the actual code or configuration RFI-IRFOS cited. The FairTiq SDK findings (H1, H2) are shared with RFI-IRFOS's parallel, separately-timed disclosure to FairTiq AG itself, covering the same embedded SDK version (com.fairtiq.android v7.5.4) from the vendor's side.

Scope: Static analysis of the publicly downloaded production ÖBB Tickets Android APK (v5.2623), on an authorized test device, only. No ÖBB account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to datenschutz.personenverkehr@pv.oebb.at, cc dsb@dsb.gv.at from 7 July 2026 onward. Two findings, six unaddressed. ÖBB Kund:innenservice (Luisa Berger) replied twice: a general, non-technical denial on 30 June 2026, and a refusal to continue correspondence on 7 July 2026 characterizing the disclosure as an unsolicited commercial offer. No reply of any kind was received after that, across three further notices through 31 August 2026.

ID	Severity	Title
C1	HIGH	Hardcoded Firebase production key, App Distribution API present in production build
C2	HIGH	No certificate pinning on a state-operated payment application
H1	HIGH	Embedded FairTiq SDK transmits companion and community data to Switzerland
H2	HIGH	Shared infrastructure: FairTiq routes payment data via China UnionPay
H3	MEDIUM	On-device movement analysis via TensorFlow Lite and ACTIVITY_RECOGNITION
H4	MEDIUM	READ_PHONE_STATE / IMEI collection disproportionate to stated purpose

Subject & Operator Analysis

ÖBB-Personenverkehr AG operates Austria's national passenger rail network as a subsidiary of Österreichische Bundesbahnen, under the direct jurisdiction of the Austrian Datenschutzbehörde.

Findings

C1: Hardcoded Firebase production key, App Distribution API present in production build

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

Google API Key AIzaSyAcIy62JNN-Ufv0zuy2DIL3YVU-paTrD2M and App ID 1:146046811297:android:605bc1869a00958aa484e0 hardcoded in the shipped production APK. com.google.firebase-firebase-appdistribution-api, a beta test-distribution component, is present in the production build rather than stripped out.

ÖBB's 30 June 2026 reply stated this finding 'in der vorliegenden Form nicht bestätigt' without addressing the specific key, App ID, or the App Distribution component's presence in a production build. No technical rebuttal, App Check status, or Security Rules confirmation was ever supplied.

Impact: Risk spans quota/billing denial-of-service against the national ticketing app's Firebase project, forged push notifications to its user base, and, given the App Distribution API's presence in production, a distinct and unusual question of whether beta-build distribution channels are reachable through the same exposed project.

Fix: Strip the App Distribution API from production builds, confirm Firebase App Check enforcement, and publish a Security Rules export proving deny-by-default configuration.

C2: No certificate pinning on a state-operated payment application

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

No network_security_config.xml found anywhere in the APK. Ticket purchases, payment data, Vorteilscard and KlimaTicket identity data, and real-time location are all transmitted without TLS certificate pinning.

ÖBB's 30 June 2026 reply did not confirm or deny this specific finding; the general 'nicht bestätigt' response did not identify any network_security_config.xml RFI-IRFOS's analysis had missed. No reply after 7 July 2026 addressed it further.

Impact: On an adjacent, attacker-controlled network, payment credentials, subsidized-fare identity documents, and location data on a state-operated national ticketing app can be intercepted and manipulated without triggering a pinning failure.

Fix: Deploy a network_security_config.xml restricting trust to a defined certificate set for all payment and identity-bearing endpoints.

H1: Embedded FairTiq SDK transmits companion and community data to Switzerland

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

The embedded FairTiq SDK (2,618 classes) transmits TrackerDataRest, CommunityIdRest, CompanionsConfigurationRest, TemporalStationRest, and JourneyCheckoutReason payloads to FairTiq servers in Switzerland.

Which passage of the app's privacy policy covers this specific third-country transfer of companion and community-tracking data was asked repeatedly and never answered. This finding is shared with RFI-IRFOS's separate, directly-addressed disclosure to FairTiq AG covering the same SDK version from the vendor's side, which received a substantive, disputed-in-part technical response, unlike this case.

Impact: Companion and community-tracking data tied to individual journeys is transferred to a third country with no confirmed disclosure or transfer mechanism named in the app's own privacy policy.

Fix: Name FairTiq AG (Switzerland) explicitly as a processor with its transfer mechanism in the privacy policy, and confirm a DPIA/TIA was completed for this data flow.

H2: Shared infrastructure: FairTiq routes payment data via China UnionPay

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

The standalone FairTiq app, sharing infrastructure with the embedded ÖBB Tickets SDK, contains a ChinaUnionPayPaymentMethodRest payment path. China has no EU adequacy decision.

Cross-app finding: whether ÖBB Tickets users' payment or journey data can reach this same shared FairTiq infrastructure was never addressed by ÖBB. RFI-IRFOS's separate FairTiq disclosure covers this payment path directly.

Impact: Shared SDK infrastructure between ÖBB Tickets and a vendor with a China-routed payment path raises an unresolved cross-border transfer question with no confirmed EU adequacy or Art. 46 safeguard.

Fix: Confirm to what extent ÖBB Tickets user data can reach FairTiq's China UnionPay payment path, and document the applicable Art. 46 safeguard if so.

H3: On-device movement analysis via TensorFlow Lite and ACTIVITY_RECOGNITION

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

TensorFlow Lite (with GPU/NNAPI hardware delegates) combined with the ACTIVITY_RECOGNITION permission, consistent with automatic trip detection or check-in/check-out inference.

RFI-IRFOS asked whether a DPIA under Art. 35 was conducted for this processing and what Art. 6(1) legal basis applies. ÖBB's 30 June 2026 reply stated that whether a DPIA was required 'betrifft interne Compliance- und Risikoabwägungsprozesse' and that there is no obligation to disclose this to an external party. No further answer followed.

Impact: On-device inference of a rider's movement pattern, tied to a real identity through Vorteilscard/KlimaTicket data, operates without a confirmed documented legal basis or impact assessment.

Fix: Document the Art. 6(1) legal basis for movement-pattern inference and confirm whether an Art. 35 DPIA was conducted.

H4: READ_PHONE_STATE / IMEI collection disproportionate to stated purpose

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

The app requests READ_PHONE_STATE, granting access to the device IMEI, on a ticketing application with no stated purpose requiring hardware-level device identification.

Never addressed specifically in either of ÖBB's two replies.

Impact: A persistent hardware identifier is collected beyond what ticket issuance and validation require, raising an Art. 5(1)(c) data-minimization question.

Fix: Remove the READ_PHONE_STATE permission unless a specific, documented purpose requiring IMEI access exists.

A General Denial, Then a Refusal to Engage

ÖBB Kund:innenservice, represented by Luisa Berger, produced two named replies rather than silence, which places this case above the campaign's median. Neither reply engaged with a specific finding on its technical merits. The first, 30 June 2026, stated the findings 'in der vorliegenden Form nicht bestätigt' without naming which specific claim was disputed or why, and answered RFI-IRFOS's questions on legal basis, Art. 33, and DPIA obligations by stating these are internal matters with no disclosure obligation to an external party. The second, 7 July 2026, declined all further correspondence, framing the disclosure itself as an unsolicited commercial contact carrying no obligation to respond. RFI-IRFOS disputed that framing the same day: a coordinated vulnerability disclosure under ISO/IEC 29147, naming six specific findings with reproduction steps, is not a commercial solicitation, and the six findings themselves are unrelated to whether any commercial terms were also offered.

Shared Infrastructure: the FairTiq Cross-Reference

The FairTiq SDK embedded in ÖBB Tickets (com.fairtiq.android v7.5.4) is the same SDK RFI-IRFOS disclosed directly to FairTiq AG under its own reference and embargo date. FairTiq's own security team engaged substantively and in good faith with two of that report's originally-CRITICAL findings, disputing them on technical grounds RFI-IRFOS could not fully refute, and confirmed four HIGH findings including the China UnionPay payment path and the Swiss-routed companion/community data at issue here. ÖBB, as the operator embedding that SDK into a state ticketing app used by a national population, never engaged with either the companion-data transfer (H1) or the shared China UnionPay payment infrastructure (H2) on their merits.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded Firebase key, App Distribution API present in production, unaddressed
C2	GDPR Art. 32(1)(a)	No certificate pinning on a payment and identity-bearing application, unaddressed
H1	GDPR Art. 13(1)(f), Art. 44	Undisclosed third-country transfer of companion/community data to Switzerland
H2	GDPR Art. 44, Art. 46	Shared infrastructure with a China-routed payment path, no confirmed adequacy
H3	GDPR Art. 6(1), Art. 35	On-device movement inference, no confirmed legal basis or DPIA
H4	GDPR Art. 5(1)(c)	IMEI collection disproportionate to stated purpose

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to datenschutz.personenverkehr@pv.oebb.at, 2 CRITICAL + 4 HIGH findings disclosed, embargo stated as 2026-09-19; a paid remediation-engagement offer was also included in this and subsequent notices, historical record only, not a currently open offer
2026-06-28	Follow-up (8 days, no reply), restates findings table, three standing questions, 2026-07-02 deadline
2026-06-30	Berger replies: findings 'nicht bestätigt' in general terms; three questions answered only in the abstract

Date	Event
2026-06-30	RFI-IRFOS replies same day with apktool/grep reproduction steps, requests DPO-level confirmation, 2026-07-07 deadline
2026-07-07	Berger replies: declines further correspondence, frames disclosure as an unsolicited commercial contact, states no further correspondence will follow
2026-07-07	RFI-IRFOS replies same day, cc dsb@dsb.gv.at from this point onward, disputes the commercial-offer framing
2026-07-23	Follow-up, 17 days of silence since Berger's refusal, cc dsb@dsb.gv.at
2026-08-15	Follow-up, 56 days since disclosure, 23 days since Berger's refusal, cc dsb@dsb.gv.at
2026-08-31	Follow-up, 16 days since prior message, 55 days since Berger's refusal, cc dsb@dsb.gv.at; no further ÖBB reply received
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Strip the Firebase App Distribution API from production builds and confirm App Check enforcement for the exposed project.
- Deploy a network_security_config.xml covering all payment and identity-bearing endpoints.
- Name FairTiq AG explicitly as a processor with its transfer mechanism, and confirm the applicable Art. 46 safeguard for any China-routed payment path reachable through shared infrastructure.
- Document the Art. 6(1) legal basis for on-device movement inference and confirm whether an Art. 35 DPIA was conducted.
- Remove or justify the READ_PHONE_STATE/IMEI collection against a specific, documented purpose.

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 Coordinated disclosure per ISO/IEC 29147. Research

activity protected under Austria’s Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 13, 32, 33, 35, 44, 46. REF OEBB-2026-R1.