Coordinated Security & Privacy Disclosure, Final Report

FAIRTIQ for Android (com.fairtiq.android, v7.5.4) and the FAIRTIQ SDK embedded in OeBB Tickets (at.oebb.ts, v5.2623)

Nine written notices, a genuine technical dispute on two findings, four findings never substantively addressed, silence since 23 June

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – TWO FINDINGS GENUINELY DISPUTED ON TECHNICAL GROUNDS, FOUR NEVER ADDRESSED

Target	FAIRTIQ AG, Switzerland – check-in/check-out ticketing SDK used by European rail operators including OeBB and SBB
Product audited	FAIRTIQ for Android, com.fairtiq.android, v7.5.4, and the FAIRTIQ SDK as embedded in OeBB Tickets, at.oebb.ts, v5.2623
Disclosure reference	REF FAIRTIQ-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H2 simultaneous EU and US PostHog analytics endpoints hardcoded with no adequacy decision cited for the US routing, CVSS v4.0 8.7, never substantively addressed)

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 FAIRTIQ Android application and identified two findings initially rated CRITICAL and four rated HIGH: a Firebase API key hardcoded in the production APK, a Network Security Configuration containing a debug-overrides block alongside user-certificate trust-anchors in the same document as the production domain configuration, whose exact scope of applicability RFI-IRFOS could not resolve from static analysis alone, China UnionPay support present as a payment method with no EU adequacy decision cited for the associated PRC entity, simultaneous EU and US PostHog analytics endpoints hardcoded in the binary with no adequacy decision cited for the US routing, an undisclosed Swiss Federal Railways (SBB) integration sharing infrastructure with Austrian OeBB passenger data, and a companion co-traveler tracking feature capable of tracking individuals who never installed FAIRTIQ or consented, alongside a Tencent-origin supply-chain dependency (MMKV).

FAIRTIQ's security team engaged quickly and substantively: on 22 June, security@fairtiq.com disputed the severity of both CRITICAL findings on specific technical grounds, citing Google's own documentation that Firebase API keys are not secrets when properly restricted, and arguing that exploiting the NSC finding would require either a debuggable production build, which FAIRTIQ states does not exist, or physical device access sufficient to install a custom certificate authority, a threat model in which far more sensitive data would already be exposed regardless. These are substantive technical arguments RFI-IRFOS could not fully refute from static analysis alone; the residual open question in both cases, whether the Firebase key is actually application-restricted and whether the NSC's certificate trust-anchors apply inside or outside the debug-overrides scope, was never conclusively confirmed by either side. On 23 June, a named FAIRTIQ security contact replied further, declining to treat unvalidated static-analysis observations as findings without independent verification, explicitly declining further engagement on the four HIGH findings, and noting that pairing a priced engagement offer with an announced public-disclosure date in an initial contact is, in FAIRTIQ's words, 'very easy to misunderstand', a concern the field independently reflects in RFI-IRFOS's subsequent decision to remove pricing language from all disclosure correspondence. No further reply of any kind was received after 23 June, despite four subsequent written notices, and none of H1 through H4 were ever substantively addressed.

Scope: Static analysis of the publicly downloaded production FAIRTIQ Android APK (v7.5.4) and the FAIRTIQ SDK as embedded in the OeBB Tickets APK, on an authorized test device, only. No FAIRTIQ account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to privacy@fairtiq.com and security@fairtiq.com, with a parallel copy to dataprotection@fairtiq.com and info@fairtiq.com, cc the Austrian Datenschutzbehoerde, CERT.at, and the Swiss EDOEB (bounced, invalid address, on every attempt). FAIRTIQ's security team engaged substantively and quickly, disputing the severity of two CRITICAL findings on specific technical grounds within three days, and a named security contact then declined to engage further on any finding, characterizing unvalidated static-analysis observations as insufficient to constitute findings. No further reply of any kind was received after 23 June, despite four subsequent written notices.

ID	Severity	Title
C1	DISPUTED	Firebase API key hardcoded, restriction status never confirmed
C2	DISPUTED	Network Security Config debug-overrides and user-certificate trust, scope unresolved
H1	HIGH	China UnionPay as a supported payment method
H2	HIGH	Simultaneous EU and US PostHog analytics endpoints hardcoded
H3	HIGH	Undisclosed cross-border data sharing with Swiss Federal Railways
H4	HIGH	Companion co-traveler tracking of non-consenting third parties, Tencent supply-chain dependency

Subject & Operator Analysis

FAIRTIQ AG, headquartered in Switzerland, provides a check-in/check-out ticketing SDK used by multiple European rail operators, including OeBB and SBB, both as a standalone app and embedded within partner apps.

Findings

C1: Firebase API key hardcoded, restriction status never confirmed

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

Firebase key AIzaSyAn05fI9745KS0c_snEtIlGsY-PhXtOFZg, App ID 1:491886649431:android:ddd371ef1a00cb39, and a disabled Firebase database URL are hardcoded in the production APK.

FAIRTIQ's security team disputed this finding's severity on 22 June, citing Google's own documentation that Firebase API keys are not secrets and are designed to ship in client code, provided the corresponding Firebase Security Rules and API restrictions are properly configured. This is a technically accurate general principle. The residual, unresolved question is specific rather than categorical: whether this particular key is application-restricted (by package name and SHA-256 signing fingerprint) and whether the corresponding Firebase Security Rules are deny-by-default. Neither RFI-IRFOS nor FAIRTIQ confirmed this from the correspondence available.

Impact: Whether this specific key carries residual risk depends entirely on a restriction and rules configuration that remains unconfirmed by either party.

Fix: Publicly confirm that the key is restricted to the correct package name and SHA-256 signing fingerprint, and that Firebase Security Rules are deny-by-default, resolving the question either party could answer in one sentence.

C2: Network Security Config debug-overrides and user-certificate trust, scope unresolved

MEDIUM, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 5.3

The Network Security Configuration binary contains a debug-overrides block with user-certificate trust-anchors in the same document as the production fairtiq.com domain configuration. Whether the user-trust-anchors apply exclusively within the debug-overrides element, as intended, or also extend to production scope, was not resolvable from static analysis alone.

FAIRTIQ's 22 June reply argued that exploitation would require either a debuggable production build, which they state does not exist, or physical access to the device sufficient to install a custom certificate authority, a scenario in which, in their stated threat model, an attacker would already have access to far more sensitive on-device data regardless. This is a reasonable threat-model argument that meaningfully narrows the finding's practical severity, reflected in the CVSS vector above requiring physical access as a precondition. The scope question itself, whether user-trust-anchors apply outside the debug-overrides element, was never confirmed by either side.

Impact: If the user-certificate trust-anchors extend beyond the intended debug scope, an attacker with physical device access could intercept FAIRTIQ traffic via a custom CA; FAIRTIQ's own stated threat model treats this precondition as already granting broader access regardless.

Fix: Confirm and publish whether the user-certificate trust-anchors are scoped exclusively to the debug-overrides element, resolving the single open technical question in this finding.

H1: China UnionPay as a supported payment method

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

com/fairtiq/sdk/internal/domains/user/payment/methods/ChinaUnionPayPaymentMethodRest confirms China UnionPay support. UnionPay is controlled by the People's Bank of China; no EU adequacy decision exists for China.

This finding was never addressed in any FAIRTIQ reply.

Impact: Payment processing through a PRC state-controlled payment network may lack a documented Art. 44 transfer mechanism for the associated data flows.

Fix: Document the Art. 44 transfer mechanism, if any, covering China UnionPay payment processing, or disclose its absence.

H2: Simultaneous EU and US PostHog analytics endpoints hardcoded

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

https://eu.posthog.com, https://us.posthog.com, https://us.i.posthog.com, and https://us-assets.i.posthog.com are all hardcoded in the production APK. There is no general EU adequacy decision for the US.

This finding was never addressed in any FAIRTIQ reply.

Impact: Analytics data may be routed to US infrastructure alongside the EU endpoint with no confirmed transfer mechanism for the US-bound traffic specifically.

Fix: Confirm and disclose which analytics traffic is routed to the US endpoints and under what Art. 44-49 transfer mechanism.

H3: Undisclosed cross-border data sharing with Swiss Federal Railways

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

A Swiss Federal Railways (SBB) integration (164 classes) is present in the production APK. Austrian OeBB passengers are not informed that their journey data shares infrastructure with SBB.

This finding was never addressed in any FAIRTIQ reply.

Impact: OeBB passenger journey data may be processed through shared infrastructure with a Swiss operator with no disclosure of that specific arrangement to those passengers.

Fix: Disclose the SBB infrastructure-sharing arrangement explicitly to OeBB passengers using the FAIRTIQ SDK.

H4: Companion co-traveler tracking of non-consenting third parties, Tencent supply-chain dependency

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

SupportedOneTimeCompanionConfigurationRest enables tracking of co-travelers who have neither installed FAIRTIQ nor consented. Separately, com/tencent (Tencent MMKV) is present as a Chinese-origin supply-chain dependency.

This finding was never addressed in any FAIRTIQ reply.

Impact: Non-users' location and travel data may be processed through the companion-tracking feature with no consent mechanism applicable to them specifically, an Art. 14 concern distinct from FAIRTIQ's own users.

Fix: Document the Art. 14 disclosure and legal basis for processing non-consenting companions' data, and confirm the Tencent MMKV dependency's data handling.

A Genuine Technical Dispute, Then Silence

This case stands apart from most in this disclosure wave: FAIRTIQ's security team engaged within two days with specific, technically grounded counter-arguments on both CRITICAL findings, arguments RFI-IRFOS could not fully refute from static analysis alone. On 23 June, a named security contact replied further, declining to treat unvalidated decompiled-artifact observations as confirmed findings without independent verification, and explicitly declining further engagement on the four HIGH findings, stating it was not FAIRTIQ's responsibility to disprove them. That same reply also noted that combining a priced engagement offer with an announced disclosure date in an initial contact is 'very easy to misunderstand', an observation this report records because it independently reflects the reasoning behind RFI-IRFOS's own subsequent decision to remove all pricing and tier language from disclosure correspondence going forward. No further reply of any kind was received after 23 June, despite four subsequent written notices over the following eleven weeks, and H1 through H4 were never substantively addressed at any point.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Firebase key restriction status disputed, never conclusively confirmed by either party
C2	GDPR Art. 32(1)(a)	NSC certificate-trust scope disputed, exploitation precondition narrowed by FAIRTIQ's own threat model
H1	GDPR Art. 44	Payment processing via a PRC state-controlled network, transfer mechanism undisclosed
H2	GDPR Art. 13(1)(f), Art. 44	Simultaneous EU/US analytics routing, US transfer mechanism undisclosed
H3	GDPR Art. 5(1)(b), Art. 13(1)(e)	Undisclosed cross-border infrastructure sharing
H4	GDPR Art. 14, Art. 25	Non-consenting companion tracking; Chinese-origin supply-chain dependency

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@/security@fairtiq.com and a parallel copy to data protection@/info@fairtiq.com; bcc Austrian DSB/CERT.at/Swiss EDOEB (bounced); automated Zendesk acknowledgment same day
2026-06-22	security@fairtiq.com disputes C1 and C2 on technical grounds; RFI-IRFOS rebuts the same day and re-raises H1-H4
2026-06-23	A named FAIRTIQ security contact declines to treat H1-H4 as confirmed findings without independent validation, declines further engagement
2026-08-15	Follow-up, fifty-four days since FAIRTIQ's last reply, four of six findings restated as still unaddressed
2026-08-24	Follow-up, sixty-three days, restates all six findings, reiterates the Art. 33(4) 72-hour notification point
2026-09-04	Follow-up, seventy-four days since the last reply, most recent message on file
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Confirm publicly whether the Firebase key is application-restricted and Security Rules are deny-by-default, resolving C1 definitively.
- Confirm publicly whether the NSC's user-certificate trust-anchors are scoped exclusively to the debug-overrides element, resolving C2 definitively.
- Address H1 through H4, none of which received any substantive reply across nine notices.
- Disclose the SBB infrastructure-sharing arrangement to OeBB passengers specifically.
- Document the Art. 14 basis for companion co-traveler tracking of non-consenting third parties.

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. GDPR Art. 5, 13, 14, 25, 32, 44. REF FAIRTIQ-R1.