



Security & Privacy Disclosure, Final Report

WienMobil for Android (at.wienerlinien.wienmobillab)

Vienna's city-owned public transit app ships a Belarusian biometric ID-verification SDK, logs all API traffic in plaintext via a production debug tool, and hardcodes an unauthenticated Firebase backend, unresolved through 113 days and a 21-day-overdue embargo, with a single generic acknowledgment and zero substantive reply

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26
SEPTEMBER 2026, THREE FINDINGS REMAIN UNADDRESSED**

Target	Wiener Linien GmbH & Co KG, the city-owned public transit operator for Vienna, Austria
Package	at.wienerlinien.wienmobillab
Platform Audited	Android · v8.10.4 (versionCode 14559), static analysis of the production APK
Initial Disclosure (R1)	2026-06-26 (REF WIENMOBIL-2026)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	3 (3 Critical)
Correspondence	10 messages sent by RFI-IRFOS in a single thread, 1 generic acknowledgment received (1 July 2026), 0 substantive replies to any of the three findings
Authorities BCC'd / CC'd	Austrian Datenschutzbehörde (DSB) · Stadt Wien Datenschutzbeauftragter · Wiener Linien Security (security@wienerlinien.at) · Press contact (presse@wienerlinien.at)

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	B1: Regula IDV + Document Reader SDK (Minsk, Belarus) performs biometric identity verification on a public transit app with no disclosed purpose or Art. 44 safeguard	6
4.2	B2: Chucker HTTP interceptor ships in the production build, logging all API traffic in plaintext including auth tokens and ticket-purchase data	7
4.3	B3: Firebase API key and Realtime Database URL hardcoded in the production binary, with pre-consent initialization and unconditional boot-persistence . . .	7
5	Impact Analysis	8
6	The Complete Chain: One Acknowledgment, Nine Unanswered Follow-Ups, and a Belarusian SDK Nobody Explained	8
7	Data Protection — Article by Article	9
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	11

Executive Summary

Wiener Linien operates Vienna's public transit network on behalf of the City of Vienna. Its Android application, WienMobil (at.wienerlinien.wienmobillab, v8.10.4), is used daily by hundreds of thousands of Viennese residents for tickets, subscriptions, and real-time journey information.

Static analysis identified three findings, all CRITICAL. The app bundles the Regula Document Reader and Regula IDV (Identity Verification) SDKs from Regula Forensics, a Belarusian company, capable of optically scanning passports and ID cards and performing liveness/facial-recognition checks, with no stated purpose on a transit/ticketing app and no identified Art. 44 safeguard for transferring biometric data to a country without an EU adequacy decision. The Chucker HTTP interceptor, a development debugging tool, ships in the production build and logs all outgoing and incoming API traffic in plaintext on-device, including authentication tokens, session keys, and ticket-purchase data, retrievable via a notification on any device with ADB or root access. A Firebase API key and Realtime Database URL are hardcoded in the production binary, with FirebaseInitProvider starting pre-consent (initOrder=100, direct-BootAware=true) and a BOOT_COMPLETED receiver restarting the app after every device reboot.

RFI-IRFOS disclosed these findings on 26 June 2026 under REF WIENMOBIL-2026 to datenschutz@wienerlinien.at and security@wienerlinien.at, CC presse@wienerlinien.at and kundenservice@wienerlinien.at, BCC the Austrian DSB and the Magistratsdirektion der Stadt Wien (the latter BCC address bounced and was corrected to the Stadt Wien Datenschutzbeauftragter from the first reply onward). Wiener Linien's data protection team replied the same day it was first checked, 1 July 2026, with a one-line acknowledgment stating only that the findings would be looked into, and never responded substantively to any of the three findings or the specific questions raised across nine further messages sent on 1 July, 6 July, 17 July, 23 July, 31 July, twice on 9 August, 24 August, and 31 August 2026. The stated embargo of 26 September 2026 passed 21 days ago with all three findings still unaddressed.

ID	Severity	Title
B1	CRITICAL	Regula IDV + Document Reader SDK (Minsk, Belarus) performs biometric identity verification on a public transit app with no disclosed purpose or Art. 44 safeguard
B2	CRITICAL	Chucker HTTP interceptor ships in the production build, logging all API traffic in plaintext including auth tokens and ticket-purchase data
B3	CRITICAL	Firebase API key and Realtime Database URL hardcoded in the production binary, with pre-consent initialization and unconditional boot-persistence

Subject & Operator Context

Wiener Linien GmbH & Co KG is the city-owned public transit operator for Vienna, running the subway, tram, and bus network for a metropolitan area of roughly two million people. WienMobil is its primary consumer-facing mobile application, used for ticket purchases, subscription management, and real-time route planning by hundreds of thousands of residents daily.

As with other city-owned infrastructure operators in this disclosure series, WienMobil sits in a position where its users have no realistic alternative provider: residents who want to use Vienna's public transit system use this app or an equivalent official channel, not a competing product. The findings in this report concern a third-country biometric SDK with no disclosed purpose, a production debug tool that exposes the plaintext contents of every API call, and an unauthenticated backend reachable via a hardcoded key, all inside that context.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 26 June 2026 under REF WIENMOBIL-2026 to nschutz@wienerlinien.at and security@wienerlinien.at, CC presse@wienerlinien.at and kundenservice@wienerlinien.at, BCC the Austrian DSB and post@magwien.gv.at. The Magistratsdirektion address bounced; RFI-IRFOS corrected the regulator BCC to datenschutzbeauftragter@wien.gv.at (the Stadt Wien Datenschutzbeauftragter) from the first reply onward.

Wiener Linien's data protection team replied on 1 July 2026, five days after the original disclosure, with a one-line acknowledgment: 'wir bedanken uns für die Hinweise und gehen diesen natürlich nach' ('we thank you for the information and will of course look into it'). No acknowledgment of the specific findings, no answer to any question, and no further written reply of any kind followed. RFI-IRFOS sent nine further messages restating the three findings and the open questions, on 1 July (same-day reply), 6 July, 17 July, 23 July, 31 July, twice on 9 August, 24 August, and 31 August 2026, the last of these 47 days before this report's publication date. The stated embargo of 26 September 2026 passed 21 days before publication, with Wiener Linien having sent exactly one message, a generic acknowledgment, across 113 days and ten sends.

Findings

B1: Regula IDV + Document Reader SDK (Minsk, Belarus) performs biometric identity verification on a public transit app with no disclosed purpose or Art. 44 safeguard

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — undisclosed biometric ID scanning and third-country data transfer with no EU adequacy decision, blast-radius escalated from HIGH

```
com/regula/documentreader/    -- ID document optical scanner
com/regula/documentreader/api/ -- scan API
com/regula/idv/               -- Identity Verification
com/regula/idv/api/           -- IDV API
com/regula/idv/docreader/     -- document reading
com/regula/common/ble/        -- Bluetooth LE integration
```

Vendor: Regula Forensics, Minsk, Belarus
No EU adequacy decision for Belarus (Art. 44 GDPR)
No disclosed purpose identified for ID/passport scanning
on a transit ticketing application

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL because this is not a generic biometric permission, it is a full passport/ID-document optical reader and identity-verification SDK, supplied by a Belarusian company, bundled into a ticketing and journey-planning app with no feature identified during this audit that requires passport scanning. Regula Forensics is based in Minsk, Belarus, a country without an EU adequacy decision, meaning any biometric data processed through this SDK and transmitted off-device would constitute a third-country transfer under Art. 44 with no safeguard identified in the app's available disclosures. Art. 9(2)(a) explicit consent for biometric processing is not evidenced anywhere in WienMobil's public privacy documentation.

B2: Chucker HTTP interceptor ships in the production build, logging all API traffic in plaintext including auth tokens and ticket-purchase data

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — production debug logger exposes authentication tokens and purchase data in plaintext on-device, blast-radius escalated from HIGH

```
com/chuckerteam/chucker/api/ -- full Chucker implementation shipped
                             in the production build
```

Logs all HTTP request/response bodies and headers in plaintext to an on-device database, exposed via a system notification. Confirmed capture scope: auth tokens, session keys, ticket-purchase payloads.

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL because Chucker is a full HTTP debugging tool, not an incidental log line, retained in the shipped production build of an app used daily by hundreds of thousands of people. It intercepts and stores every outgoing and incoming API request in plaintext in an on-device database directly accessible via a system notification, including authentication tokens, session keys, and ticket-purchase data. Any party with ADB access or a rooted device can read the complete API traffic of a WienMobil user without defeating any other control. This is a release-management failure, not a theoretical risk: the same pattern was independently observed in two other apps in this audit round (Jö Bonus Club, KFC UAE), indicating Chucker is being left enabled in production builds as a recurring, avoidable oversight.

B3: Firebase API key and Realtime Database URL hardcoded in the production binary, with pre-consent initialization and unconditional boot-persistence

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9) — unauthenticated backend reachable via a hardcoded key, combined with pre-consent tracking and unconditional boot-persistence, blast-radius escalated from MEDIUM

```
res/values/strings.xml
google_api_key = AIzaSyBvreU5PSo6PFx0c1s5gFbPjl5cYp96-SA
firebase_database_url = https://wienmobil-35754.firebaseio.com
```

```
AndroidManifest.xml
FirebaseInitProvider initOrder=100 directBootAware=true
BOOT_COMPLETED receiver registered
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because three distinct issues compound in a single finding: the Firebase API key and the direct Realtime Database URL (wienmobil-35754.firebaseio.com) are both present in plaintext in the production binary, reachable over the network with no further authentication if the project's

security rules permit it; FirebaseInitProvider starts with `initOrder=100` and `directBootAware=true`, before any consent screen can act, on every single install; and a `BOOT_COMPLETED` receiver restarts the app unconditionally after every device reboot with no user interaction. For a city-owned transit app used by hundreds of thousands of people daily, the combination of a network-reachable unauthenticated backend and unconditional pre-consent initialization exceeds a routine hardcoded-credential finding.

Impact Analysis

All three findings in this report carry CRITICAL severity, a higher concentration than most reports in this disclosure series, because each one combines a technical defect with a scale or sensitivity factor specific to WienMobil's position as Vienna's official public transit app. B1 is the most unusual finding in this audit round: a full biometric identity-verification SDK from a Belarusian vendor, bundled into an app whose stated function is tickets and journey planning, with no third-country transfer safeguard identified. B2 turns a routine release-management oversight into a live exposure of authentication tokens and purchase data for every user, on any device with ADB or root access. B3 combines an unauthenticated, network-reachable backend with pre-consent tracking and unconditional boot-persistence, three issues that would each independently warrant attention.

What distinguishes this case is the correspondence pattern: unlike a case of total silence, Wiener Linien's data protection team did reply, within five days, but that reply addressed none of the three findings and committed to nothing beyond 'we will look into it.' Nine further messages across the following three months received no response of any kind, written or otherwise.

The Complete Chain: One Acknowledgment, Nine Unanswered Follow-Ups, and a Belarusian SDK Nobody Explained

Step 1 — Disclosure sent, one BCC address bounces: RFI-IRFOS sends the original findings to datenschutz@wienerlinien.at and security@wienerlinien.at on 26 June 2026 under REF WIENMOBIL-2026, BCC the Austrian DSB and the Magistratsdirektion der Stadt Wien. The Magistratsdirektion address returns a delivery failure.

Step 2 — A real reply arrives, but it is generic: On 1 July 2026, Wiener Linien's data protection team replies with a single line thanking RFI-IRFOS for the information and stating it will be looked into. No finding is acknowledged individually, no question is answered, and no timeline is given. RFI-IRFOS responds the same day, correcting the bounced regulator BCC to datenschutzbeauftragter@wien.gv.at.

Step 3 — Three questions, a 48-hour deadline, silence: RFI-IRFOS sends a follow-up on 6 July 2026 naming three specific open questions and a 48-hour response window. No reply follows.

Step 4 — Six further follow-ups, zero further replies: Messages sent 17 July, 23 July, 31 July, twice on 9 August, and 24 August 2026 each restate the three findings and the still-open questions, escalating the day-count each time. None receives any reply.

Step 5 — Embargo reached in silence: A final follow-up on 31 August 2026 notes seven days since the previous message. The stated embargo of 26 September 2026 passes with the correspondence record unchanged since 1 July: one generic acknowledgment, nothing more.

Step 6 — Publication: This report publishes 21 days after the embargo date, on the terms stated from the first message.

This case differs from a simple non-response: Wiener Linien engaged just enough to demonstrate the messages were received and read, then provided nothing further across nine additional attempts and nearly three months.

Data Protection — Article by Article

Art. 9(2)(a) GDPR — Processing of special categories of personal data, consent: B1's biometric identity-verification processing has no explicit consent mechanism identified in Wien-Mobil's available disclosures.

Art. 13(1) GDPR — Information to be provided, transparency: B1's use of a third-party biometric SDK is not disclosed as a specific processing purpose anywhere identified in the app's privacy documentation.

Art. 44 GDPR — General principle for transfers: B1's integration of a Belarusian vendor's biometric SDK raises a third-country transfer question with no Art. 46 safeguard (such as standard contractual clauses) identified for data reaching Belarus.

Art. 32 GDPR — Security of processing: B2's production-build HTTP interceptor and B3's hardcoded Firebase credentials both fall short of the technical security measures Art. 32 requires for an app handling payment and ticketing data for hundreds of thousands of residents.

Art. 7(1) GDPR — Conditions for consent: B3's FirebaseInitProvider initializes before any consent mechanism can act, for every single install.

Regulatory & Legal Landscape

Wiener Linien GmbH & Co KG is wholly owned by the City of Vienna, placing it within the jurisdiction of the Austrian Datenschutzbehörde (DSB), BCC'd on the original disclosure, and answerable to the Stadt Wien Datenschutzbeauftragter, corrected onto this thread's BCC line after the original Magistratsdirektion address bounced.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 9 special-category processing and Art. 44 transfer question in B1, up to EUR 20,000,000 or 4% of total worldwide annual turnover; for a municipally owned operator, the relevant comparator is typically set under national implementing law rather than a commercial turnover figure, but the Art. 83(5) tier itself still applies to the underlying violation. Art. 83(4) applies to the Art. 32 and Art. 7 issues in B2 and B3, up to EUR 10,000,000 or 2% of total worldwide annual turnover. That a single generic acknowledgment, with no engagement on any of the three findings, is the entirety of Wiener Linien's response across 113 days and ten sends is itself a fact relevant to any regulator assessing institutional engagement with a disclosed Art. 9 biometric-processing finding.

Indicators of Compromise

The following identifiers, SDK packages, and credentials were extracted from the production APK (v8.10.4, versionCode 14559) via static analysis only. No Wiener Linien servers, accounts, or infrastructure were probed.

```
B1 -- com/regula/documentreader/, com/regula/idv/ (Regula
    Forensics, Minsk, Belarus) -- biometric ID verification

B2 -- com/chuckerteam/chucker/api/ -- full HTTP interceptor
    shipped in production

B3 -- Hardcoded Firebase API key + Realtime Database URL
    (wienmobil-35754.firebaseio.com); FirebaseInitProvider
    initOrder=100 directBootAware=true; BOOT_COMPLETED receiver
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure sent under REF WIENMOBIL-2026 to datenschutz@wienerlinien.at and security@wienerlinien.at. CC: presse@wienerlinien.at, kundenservice@wienerlinien.at. BCC: Austrian DSB, Magistratsdirektion der Stadt Wien (bounces).

2026-07-01 Wiener Linien replies with a one-line generic acknowledgment. RFI-IRFOS responds the same day, correcting the regulator BCC to the Stadt Wien Datenschutzbeauftragter.

2026-07-06 Follow-up sent naming three specific questions and a 48-hour deadline. No reply.

2026-07-17, 2026-07-23, 2026-07-31 Three further follow-ups restating the findings and open questions. No reply to any of them.

2026-08-09 Two follow-up messages sent the same day, 44 days since the original disclosure. No reply.

2026-08-24 Further follow-up, 59 days since the original disclosure. No reply.

2026-08-31 Final follow-up before the embargo, noting seven days since the previous message. No reply.

2026-09-26 Stated embargo date reached. The correspondence record is unchanged since the single 1 July acknowledgment.

2026-10-17 This report published, 21 days after the embargo date. All three findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

B1 — Immediate: Document the specific purpose, legal basis, and Art. 44 transfer safeguard for the Regula IDV and Document Reader SDKs, or remove them if no feature in the shipped app actually requires passport/ID scanning; disclose any retained biometric processing explicitly to users before it occurs.

B2 — Immediate: Remove the Chucker HTTP interceptor from all production builds; audit the release pipeline to confirm no other debug-only dependencies are shipping in the live app.

B3 — Immediate: Rotate the hardcoded Firebase key and database URL, confirm the associated project's security rules require authentication for all read/write operations, and reorder FirebaseInitProvider initialization to occur strictly after an affirmative consent signal.

Across all findings: establish a disclosure-response process that goes beyond acknowledging receipt. Wiener Linien's data protection team replied within five days of the original disclosure, demonstrating the message was read, but provided no further engagement across nine subsequent messages and nearly three months. For a city-owned transit operator serving hundreds of thousands of residents daily, acknowledging a disclosure without ever addressing its substance is itself a process gap worth correcting independently of the findings in this report.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis

of the published application using publicly available tooling. No Wiener Linien servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF WIENMOBIL-2026.