Coordinated Privacy Disclosure, Final Report

Wizz Air Android (com.wizzair.WizzAirApp)

Wizz Air Hungary Ltd, Budapest, Hungary

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE, FIVE MESSAGES, ZERO REPLY OF ANY KIND

Target	Wizz Air, one of Europe's largest low-cost carriers
Package	com.wizzair.WizzAirApp, version 8.3.6
Operator	Wizz Air Hungary Ltd, Budapest, Hungary
Initial Disclosure	2026-06-27
Stated Embargo	2026-09-25, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, on the stated date
Regulators	NAIH (Hungarian DPA, lead SA), Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	5, across 65 days, to privacy@wizzair.com, security@wizzair.com, and dpo@wizzair.com; several messages experienced repeated delivery delays before final delivery.
Inbound Replies	0. No reply, automated or human, was ever received.

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 Subject & Operator Analysis 5

3 Five Messages, Zero Reply 5

4 Findings 5

4.1 C1: Belarusian SDK Reads Biometric Passport NFC Chip, Including Facial Photograph . . . 6

4.2 C2: System-Wide Overlay Capability, Structural Attack Surface Alongside Biometric Capture . . . 6

4.3 C3: Pre-Consent Firebase Initialization With a Hardcoded API Key . . . 7

4.4 H1: CALL_PHONE Bypasses the System Dialler Confirmation Step . . . 7

4.5 H2: Undisclosed Persistent Device Fingerprinting . . . 8

4.6 H3: Undisclosed US Behavioral-Automation Platform . . . 8

4.7 H4: Bluetooth Triple-Stack Enables Airport Proximity Tracking Without GPS . . . 8

5 Data Protection, Article by Article 9

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Wizz Air Hungary Ltd that its Android app embeds Regula Document Reader, a mobile identity verification SDK developed by Regula Forensics, headquartered in Minsk, Belarus, implementing the full ICAO 9303 RFID/NFC protocol stack to read the contactless chip embedded in EU biometric passports, including Data Group 2, the facial photograph, biometric data under Art. 4(14) GDPR. RFI-IRFOS holds this finding at CRITICAL under an explicit blast-radius escalation beyond its computed HIGH/8.7 band: Regula Forensics is a Belarusian company, and following the EU's significant expansion of restrictive measures against Belarus after the forced diversion of Ryanair flight FR4978 in 2021, routing EU passengers' biometric passport data through a sanctioned-jurisdiction vendor's SDK infrastructure raises a compliance question beyond GDPR alone. This processing is not disclosed anywhere in Wizz Air's privacy policy.

A second finding names the app's SYSTEM_ALERT_WINDOW permission, allowing it to draw UI overlays over every other application on the device, including banking apps and password managers, the same technical capability exploited in overlay-phishing attacks. RFI-IRFOS named the combination explicitly: a passenger presenting biometric passport data on a device where this same app can simultaneously draw arbitrary UI over any other application creates a structural attack surface, even though the overlay permission alone computes to LOW severity in isolation. Pre-consent Firebase initialization, a hardcoded API key, and a database URL round out the third critical finding.

Four further findings compound the picture: CALL_PHONE, allowing the app to place calls without the standard system dialler confirmation step a user would otherwise see; FingerprintJS, generating a persistent device fingerprint from hardware characteristics that in some configurations survives app reinstalls and factory resets, undisclosed as a tracking method; Airship (formerly Urban Airship), a US behavioral-automation and push-messaging platform processing 273 classes' worth of engagement data with no Art. 13(1)(e) disclosure; and a Bluetooth triple-stack (SCAN, CONNECT, ADVERTISE) combined with fine location and nearby-WiFi access, enabling precise proximity tracking within airport terminals without GPS. Genuine positives are worth naming: cleartextTrafficPermitted is correctly set to false as the base network security config, PairIP app protection is implemented, and allowBackup is correctly set to false.

Five messages were sent across 65 days, to privacy@wizzair.com, security@wizzair.com, and dpo@wizzair.com, cc'ing NAIH (Hungary's data protection authority and Wizz Air's lead supervisory authority), the Austrian DSB, Germany's BfDI, and CERT.at throughout. Several messages experienced repeated delivery delays before eventually going through. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the initial disclosure, elapses today. This report and the accompanying closure notice publish on the stated date.

Scope: Root-level static analysis of the production Wizz Air Android application (com.wizzair.WizzAirApp, version 8.3.6), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Regula Forensics', Airship's, FingerprintJS's, or Firebase's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Regula Document Reader, a Belarusian company's SDK reading the biometric facial photograph from EU passengers' ePassport NFC chips, reaches HIGH/8.7 on its own computed band and is held at CRITICAL under an explicit RFI-IRFOS blast-radius escalation, given the combination of Art. 9 biometric data with a vendor headquartered in a jurisdiction under comprehensive EU restrictive measures. Pre-consent Firebase initialization, undisclosed device fingerprinting, and an undisclosed US behavioral-automation platform all correct to MEDIUM. A SYSTEM_ALERT_WINDOW overlay capability, undocumented CALL_PHONE, and a Bluetooth triple-stack enabling airport proximity tracking all correct to LOW individually, though the combination with the biometric finding forms a structural attack surface named explicitly in the original disclosure. Five messages were sent across 65 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	CRITICAL	Belarusian SDK Reads Biometric Passport NFC Chip, Including Facial Photograph
C2	LOW	System-Wide Overlay Capability, Structural Attack Surface Alongside Biometric Capture
C3	MEDIUM	Pre-Consent Firebase Initialization With a Hardcoded API Key
H1	LOW	CALL_PHONE Bypasses the System Dialler Confirmation Step
H2	MEDIUM	Undisclosed Persistent Device Fingerprinting
H3	MEDIUM	Undisclosed US Behavioral-Automation Platform
H4	LOW	Bluetooth Triple-Stack Enables Airport Proximity Tracking Without GPS

Subject & Operator Analysis

Wizz Air Hungary Ltd, Budapest, is one of Europe's largest low-cost carriers. NAIH, the Hungarian data protection authority, is the lead supervisory authority under GDPR Art. 55-56.

Genuine positives are worth naming. cleartextTrafficPermitted is correctly set to false as the base network security config, meaning no global cleartext exposure. PairIP app protection is implemented. allowBackup is correctly set to false, preventing sensitive data from being included in Android backups. The core transport security posture is sound; the compliance and data-processor governance layer is where the gaps in this report sit.

Five Messages, Zero Reply

All five messages in this case's correspondence record were sent to privacy@wizzair.com , security@wizzair.com, and dpo@wizzair.com across 65 days, cc'ing NAIH, the Austrian DSB, Germany's BfDI, and CERT.at throughout. Several messages experienced repeated delivery delays before eventually going through. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Belarusian SDK Reads Biometric Passport NFC Chip, Including Facial Photograph

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.

Regula Document Reader (328 compiled classes) implements the full ICAO 9303 RFID/NFC protocol stack, reading Data Group 1 (MRZ: name, nationality, passport number, DOB, expiry) and Data Group 2 (facial photograph, biometric data under Art. 4(14) GDPR) from EU biometric passport chips. Regula Forensics is headquartered in Minsk, Belarus, a jurisdiction under comprehensive EU restrictive measures since the 2021 forced diversion of Ryanair flight FR4978. This processing is not disclosed in Wizz Air's privacy policy. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because EU passengers' Art. 9 biometric passport data is processed via a Belarusian-h eadquartered vendor's SDK infrastructure, a compliance question beyond GDPR alone given the EU's restrictive measures regime.

```
Regula Document Reader: 328 compiled classes, full ICAO 9303 RFID/NFC protocol
strEnableNfcDescription: reads DG1 (MRZ) and DG2 (facial photograph)
Regula Forensics HQ: Minsk, Belarus (EU restrictive measures jurisdiction)
```

Impact: EU passengers scanning their passport in this app have their biometric facial photograph processed by SDK infrastructure from a company headquartered in a sanctioned jurisdiction, with no disclosure of this specific processing or recipient in the privacy policy.

Fix: Document the specific Art. 44-46 transfer basis and sanctions-compliance assessment for Regula Forensics, or replace the SDK with an EU-based or on-device-only alternative. No confirmation that this has occurred was ever received.

C2: System-Wide Overlay Capability, Structural Attack Surface Alongside Biometric Capture

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

SYSTEM_ALERT_WINDOW is declared, allowing the app to draw windows over all other applications, including banking apps, password managers, and system dialogs, the same capability exploited in overlay-phishing attacks. No documented functional necessity for this permission was found in a flight-booking context.

Impact: Considered alongside C1's biometric passport capture and the device-fingerprinting finding below, a passenger scanning their passport is doing so on a device where this same app can simultaneously draw arbitrary UI over any other application, a structural combination named explicitly in the original disclosure even though this permission alone computes to LOW in isolation.

Fix: Remove SYSTEM_ALERT_WINDOW unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

C3: Pre-Consent Firebase Initialization With a Hardcoded API Key

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

FirebaseInitProvider (initOrder=100, directBootAware=true) launches Firebase Analytics before any consent dialog is shown. A Firebase API key and Realtime Database URL are hardcoded in the production binary.

```
google_api_key: AIzaSyDS7R0APNC3Rfb-qq0y87K3kEP-D2b_nJo
firebase_database_url: https://wizz-mobile.firebaseio.com
```

Impact: Behavioral tracking begins before any consent mechanism runs, and unauthenticated calls against the extractable key can exhaust Firebase quotas, a real availability risk for a service booked passengers depend on.

Fix: Gate Firebase initialization behind consent and restrict the API key by package and certificate. No confirmation that this has occurred was ever received.

H1: CALL_PHONE Bypasses the System Dialler Confirmation Step

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

CALL_PHONE is declared, allowing the app to place calls directly instead of through the standard dialler intent, which requires user confirmation. A flight-booking app's support-calling use case does not require bypassing that confirmation step. Undisclosed in the privacy policy.

Impact: The app can initiate phone calls without the confirmation step a user would otherwise see through the standard system dialler.

Fix: Use the standard dialler intent instead of CALL_PHONE unless a specific feature requires bypassing user confirmation. No confirmation that this has occurred was ever received.

H2: Undisclosed Persistent Device Fingerprinting

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.fingerprintjs.android generates a unique device identifier derived from hardware characteristics, installed apps, and system configuration, persisting across app reinstalls and, in some configurations, factory resets. Not disclosed as a tracking method in the privacy policy.

Impact: Device fingerprinting without consent is not a valid tracking basis under GDPR Art. 6 and the ePrivacy framework, and its persistence beyond normal reset mechanisms compounds the consent gap.

Fix: Remove FingerprintJS or gate it behind explicit, informed consent, and disclose it in the privacy policy. No confirmation that this has occurred was ever received.

H3: Undisclosed US Behavioral-Automation Platform

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.

Airship (formerly Urban Airship), a US-based customer-engagement and behavioral-automation platform, is present with 273 compiled classes processing engagement data, open events, notification interactions, and user-journey triggers, all routed to US infrastructure. Not named as a data recipient or sub-processor in the privacy policy.

Impact: Behavioral engagement data reaches a US processor with no Art. 13(1)(e) disclosure and no documented Art. 46 transfer mechanism.

Fix: Name Airship as a data processor in the privacy policy and document the applicable transfer mechanism. No confirmation that this has occurred was ever received.

H4: Bluetooth Triple-Stack Enables Airport Proximity Tracking Without GPS

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

BLUETOOTH_SCAN, BLUETOOTH_CONNECT, and BLUETOOTH_ADVERTISE are all declared, combined with ACCESS_FINE_LOCATION and NEARBY_WIFI_DEVICES, three separate location-capable channels with no documented, combined justification under data minimisation.

Impact: The combination enables detection of nearby devices and beacons for precise location tracking within airport terminals without requiring GPS, an undocumented capability layered on top of standard location access.

Fix: Document a specific, disclosed purpose for the combined Bluetooth and location permission set, or remove those without one. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 9, Art. 13, Art. 44-46, EU Reg. 765/2006	C1	Biometric passport NFC data processed via a sanctioned-jurisdiction vendor's SDK.
Art. 32, Art. 5(1)(c)	C2	System-wide overlay capability, structural attack surface alongside biometric capture.
Art. 6, Art. 7	C3	Pre-consent Firebase initialization with a hard-coded key.
Art. 5(1)(c), Art. 13	H1	CALL_PHONE bypasses standard dialler confirmation.
Art. 6, Art. 5(1)(a)	H2	Undisclosed persistent device fingerprinting.
Art. 13, Art. 46	H3	Undisclosed US behavioral-automation platform.
Art. 5(1)(c), Art. 13	H4	Bluetooth triple-stack enabling airport proximity tracking.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1 is held at CRITICAL under an explicit, stated blast-radius escalation beyond its computed HIGH/8.7 band. C3, H2, and H3 correct to MEDIUM, and C2, H1, and H4 correct to LOW, all on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: WIZZAIR-2026.