Coordinated Disclosure, Final Report

Cheap Air Tickets Android (com.cheapairtickets)

Anonymous operator, sole contact travelapps001@gmail.com, no registered legal entity identified

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

Target	Cheap Air Tickets, a flight-search Android app
Package	com.cheapairtickets, version 2.0.1
Operator	No registered legal entity identified. Sole documented contact: travelapps001@gmail.com, an anonymous Gmail address.
Initial Disclosure	2026-06-27
Stated Embargo	2026-09-25, restated unchanged across every follow-up
Report Published	2026-09-25, on the stated date
Regulators	Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	6, across 77 days, to travelapps001@gmail.com and, separately, to Google Play Developer Support, which bounced on both attempts.
Inbound Replies	0. No reply, automated or human, was ever received from the operator. No confirmation was ever obtained that Google Play Developer Support received either report.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed that Cheap Air Tickets has no registered legal entity behind it. Its sole documented contact is an anonymous Gmail address. There is no company name, no registered office, no VAT number, no EU representative, and no Data Protection Officer. The application's own internal class name, kotlindsllayoutcontainer, is the default identifier of an unmodified Android Studio Kotlin DSL boilerplate template, the application was never given a real internal name by its developer. A controller with no legal identity cannot comply with GDPR Art. 13, Art. 27, Art. 37, or Art. 44, and none of those obligations have been met here.

Two findings compute to HIGH. EU users' flight-search and geolocation data is processed by api.travelpayouts.com, places.aviasales.ru, api.hotellook.com, and hotellook.ru, all operated by Aviasales, a Russian travel technology company, with no Art. 45 adequacy decision and no documented Art. 46 safeguard; since the controller has no legal identity, it cannot lawfully be party to any binding transfer mechanism in the first place. Separately, the app's network security configuration sets cleartextTrafficPermitted to true as the global base config, meaning every flight search, passenger record, and location point may transmit unencrypted over any public network, exactly the environment travel-app users are in at airports, hotels, and cafés.

Two further findings correct to MEDIUM. FirebaseInitProvider fires before any consent screen is shown, alongside 419 AppsFlyer classes and 34 Adjust classes, three independent tracking SDKs running pre-consent in an app with no revenue model beyond affiliate commissions; two Firebase API keys are hardcoded in the production resources. Separately, the app's actual function is routing user searches to Booking.com and Travelpayouts affiliate links, with the user's destinations, dates, passenger counts, and price sensitivity as the underlying commodity, a data-broker model never disclosed to users who believe they are using a flight-search tool. A fifth finding, precise GPS collection beyond what a price-comparison tool requires, corrects to LOW.

Six messages were sent across 77 days, to travelapps001@gmail.com, and separately to Google Play Developer Support, which bounced on both attempts, meaning no confirmation was ever obtained that either report reached Google at all. The Austrian DSB, Germany's BfDI, and CERT.at were copied throughout. Not one reply of any kind, automated or human, was ever received from the operator. The 90-day embargo, restated unchanged across every follow-up, elapses today. This report and the accompanying closure notice publish on the stated date.

Scope: Root-level static analysis of the production Cheap Air Tickets Android application (com.cheapairtickets, version 2.0.1), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Aviasales', Travelpayouts', AppsFlyer's, or Adjust's backend infrastructure was performed.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. EU user data transferred to Russian infrastructure with no adequacy decision, and a cleartext-TrafficPermitted=true global network configuration, both correct to HIGH. Pre-consent auto-initialization of three tracking SDKs and an undisclosed affiliate data-broker business model both correct to MEDIUM. Over-broad precise-location collection corrects to LOW. Six messages were sent across 77 days. Not one reply of any kind was ever received, and Google Play Developer Support could not be confirmed to have received either report addressed to it.

ID	Severity	Title
C1	HIGH	EU User Data Transferred to Russian Infrastructure With No Legal Basis
C2	HIGH	Cleartext Traffic Permitted Across All Domains
C3	MEDIUM	Three Pre-Consent Tracking SDKs and Hardcoded API Keys
H1	MEDIUM	Undisclosed Affiliate Data-Broker Business Model
H2	LOW	Precise GPS Location Collected Beyond Stated Purpose

The Operator Does Not Exist

The app's sole documented contact is travelapps001@gmail.com, an anonymous Gmail address. There is no registered legal entity, no company name, no registered office, no VAT number, no EU representative, and no Data Protection Officer. GDPR Art. 3(2)(a) applies regardless: the app ships a German-language locale package and is listed in the Austrian and German Google Play stores, EU residents are the target audience. A controller with no legal identity cannot comply with any of the transparency, representation, or transfer-safeguard obligations GDPR sets out, and none of them have been met here.

Six Messages, Zero Reply, Two Bounced Reports to Google

All correspondence with the operator itself was sent to travelapps001@gmail.com across 77 days, cc'ing or bcc'ing the Austrian DSB, Germany's BfDI, and CERT.at throughout. Not one reply, automated or human, was ever received from that address. Separately, two attempts to reach Google Play Developer Support, on 27 June and again on 12 August, both bounced outright, meaning no confirmation was ever obtained that either report ever reached Google at all.

Findings

C1: EU User Data Transferred to Russian Infrastructure With No Legal Basis

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.

Flight search and geolocation data is processed by api.travelpayouts.com, places.aviasales.ru, api.hotellook.com, and hotellook.ru, all operated by Aviasales, a Russian travel technology company. The EU Commission has issued no adequacy decision for Russia under GDPR Art. 45, and no SCCs or other Art. 46 safeguards are documented. Since the operator has no identifiable legal entity, it cannot lawfully be party to any binding transfer mechanism.

```
api.travelpayouts.com
places.aviasales.ru
api.hotellook.com
hotellook.ru
```

Impact: EU users' travel search and location data reaches Russian infrastructure with no adequacy decision, no documented safeguard, and no identifiable controller capable of ever putting one in place.

Fix: Suspend all data transfers to Russian infrastructure immediately, and establish a legal entity capable of documenting a lawful transfer basis before resuming. No confirmation that this has occurred was ever received.

C2: Cleartext Traffic Permitted Across All Domains

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.

The network security configuration sets cleartextTrafficPermitted to true as the global base config. Every network request, flight search queries, passenger data, location data, may transmit as unencrypted HTTP. This configuration additionally trusts user-installed certificates in debug-overrides, leaving production traffic interceptable via a proxy certificate.

Impact: In any public Wi-Fi environment, exactly where travel-app users operate, this enables trivial man-in-the-middle interception and manipulation of passenger data, and no informed consent can exist for a processing architecture that cannot guarantee transmission security in the first place.

Fix: Set cleartextTrafficPermitted to false globally and remove the debug-override certificate trust from the production build. No confirmation that this has occurred was ever received.

C3: Three Pre-Consent Tracking SDKs and Hardcoded API Keys

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) fires at app launch before any consent UI is shown, alongside 419 AppsFlyer classes and 34 Adjust classes for cross-platform attribution tracking. Two Firebase API keys and a storage bucket identifier are hardcoded in the production resources.

```
google_api_key: AIzaSyCWsXRsl84oRRch4h6t_QqFfn9PgqC-OEQ
google_maps_api_key: AIzaSyAo_P3M94ztVs8hgNjW1afU0h67yk8RHUs
firebase_storage_bucket: ait-tickets.firebasestorage.app
```

Impact: Behavioral data, search queries, destinations, interaction patterns, is collected before the user has seen or accepted any consent, by three independent tracking systems running in parallel in an app with no revenue model beyond affiliate commissions.

Fix: Gate all three tracking SDKs behind a consent mechanism, and restrict the exposed API keys by package and certificate. No confirmation that this has occurred was ever received.

H1: Undisclosed Affiliate Data-Broker Business Model

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's actual function is routing user searches to affiliate partner links, a Booking.com affiliate ID and a Travelpayouts car-rental affiliate link. The user's travel search data, destinations, dates, passenger counts, and price sensitivity, is the commodity being sold to affiliate networks, and this commercial purpose is not disclosed anywhere.

Impact: Users who believe they are using a flight-search tool are, structurally, the product being sold to affiliate networks, with no disclosure of that business model anywhere in the app.

Fix: Disclose the affiliate data-broker business model and the specific recipients of user search data. No confirmation that this has occurred was ever received.

H2: Precise GPS Location Collected Beyond Stated Purpose

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.

The app requests both ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION. A flight price comparison tool requires at most coarse location to suggest nearby airports. This data is transmitted over the cleartext-permitted connections named in C2 to the Russian infrastructure named in C1.

Impact: Precise GPS coordinates serve the affiliate tracking and profiling stack, not any user-facing feature, and travel over an unencrypted connection to a jurisdiction with no adequacy decision.

Fix: Request only coarse location, sufficient for nearby-airport suggestions. No confirmation that this has occurred was ever received.

Article	Finding	Basis

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. 44-46	C1	EU user data transferred to Russian infrastructure with no legal basis.
Art. 32(1)(a)	C2	Cleartext traffic permitted across all domains.
Art. 6, Art. 7, Art. 32(1)(b)	C3	Three pre-consent tracking SDKs and hardcoded API keys.
Art. 5(1)(a), Art. 13	H1	Undisclosed affiliate data-broker business model.
Art. 5(1)(c)	H2	Precise GPS location collected beyond stated purpose.
Art. 13, Art. 27, Art. 37	General	No legal entity, no EU representative, no DPO for an app targeting EU residents.

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 and C2 correct to HIGH, C3 and H1 correct to MEDIUM, and H2 corrects to LOW, all on their own computed bands, with no escalation applied. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: com.cheapairtickets.