



Security & Privacy Disclosure, Final Report

Skyscanner Android (net.skyscanner.android.main)

A travel app built explicit consent for China and ships no consent platform for EU users: Firebase and New Relic start before any consent, Braze geofences run with location permissions, and the parent company sits under Chinese intelligence law. Seven messages to Skyscanner drew two automated acknowledgments and no substantive reply, and the report is published 20 days after the embargo.

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 27 SEPTEMBER 2026, NO SUBSTANTIVE REPLY

Target	Skyscanner Limited, Edinburgh, UK, a subsidiary of Trip.com Group Limited, Shanghai
Package	net.skyscanner.android.main v7.197
Platform analysed	Android, static analysis of the production APK from Google Play, 2026-06-27
First report (R1)	2026-06-27 (two messages), re-sent 2026-07-17 to the first working address (REF SKYSCANNER-2026-R1)
Embargo date	2026-09-27 as stated to the working address (2026-09-25 in the first message)
Report published	2026-10-17
Overall severity	CRITICAL
Findings	7 (3 Critical, 3 High, 1 Low)
Correspondence	7 messages to Skyscanner addresses over 77 days, 2 automated acknowledgments, 0 substantive replies, 5 bounced addresses
Third party reply	HelloDPO Law Ltd stated on 2026-09-01 that it does not act for Skyscanner in this matter

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	Architecture & Data Flow	5
4	Correspondence Summary	5
5	Findings	6
5.1	C1: No consent management platform, Firebase and New Relic initialise before any consent mechanism	6
5.2	C2: Explicit China PIPL consent flow built, no equivalent for EU users	7
5.3	C3: Braze geofencing with precise location permissions and boot persistence	8
5.4	H1: Chinese parent company, China National Intelligence Law Art. 7, no disclosed transfer analysis	8
5.5	H2: Hardcoded Google API keys and Firebase project identifiers	9
5.6	H3: US marketing, survey, identity and bot detection stack without disclosure at the point of collection	10
5.7	H4: Biometric authentication permissions in a flight search app	10
6	Impact Analysis	11
7	The Complete Chain	11
8	Data Protection, Article by Article	11
9	Regulatory & Legal Landscape	12
10	Indicators of Compromise & Reproducible Evidence	12
11	Disclosure Timeline & Outcome	12
12	Residual Risk & Recommendations	13

Executive Summary

Skyscanner is a flight and travel search app owned by Trip.com Group of Shanghai. Version 7.197 contains explicit consent strings for China's Personal Information Protection Law and no consent management platform for EU users. Firebase Analytics and the New Relic monitoring SDK are registered to start before any consent mechanism could exist. The Braze SDK includes geofencing, and the app requests precise location and boot persistence.

The governing thesis is a double standard: the product demonstrates that its engineers can build informed consent, and the EU build applies none, while travel and location data of EU users sits with a group subject to Chinese intelligence law. The evidence is static and establishes capability and configuration. It does not establish what the operator's server-side Braze or New Relic settings do.

RFI-IRFOS sent two reports on 27 June 2026. Five of the recipient addresses did not work: privacy@skyscanner.net, press@skyscanner.net and three authority addresses. The dpo@skyscanner.net address returned an automated acknowledgment. On 17 July 2026 RFI-IRFOS re-sent the report to legal@skyscanner.net, which also returned an automated acknowledgment. Follow-ups followed on 27 July, 9 August, 29 August and 12 September. Skyscanner never replied with substance. A third party, HelloDPO, replied that it does not act for Skyscanner. The embargo passed and this report was published on 17 October 2026.

ID	Severity	Title
C1	CRITICAL	No consent management platform, Firebase and New Relic initialise before any consent mechanism
C2	CRITICAL	Explicit China PIPL consent flow built, no equivalent for EU users
C3	CRITICAL	Braze geofencing with precise location permissions and boot persistence
H1	HIGH	Chinese parent company, China National Intelligence Law Art. 7, no disclosed transfer analysis
H2	HIGH	Hardcoded Google API keys and Firebase project identifiers
H3	HIGH	US marketing, survey, identity and bot detection stack without disclosure at the point of collection
H4	LOW	Biometric authentication permissions in a flight search app

Subject & Operator Context

Skyscanner Limited is a company in Edinburgh, Scotland, and a wholly owned subsidiary of Trip.com Group Limited, which is listed on NASDAQ and headquartered in Shanghai. The app offers flight, hotel and car hire search to users in the EU and elsewhere. Because Skyscanner is established in the United Kingdom, the UK Information Commissioner's Office is a relevant authority, and EU data subjects can complain to the authority of their residence.

Architecture & Data Flow

The production APK starts four components at process start in the order MIKitInitProvider, FirebaseInitProvider, NewRelicAppContentProvider and a boot receiver. Braze with BrazeGeofence, Qualtrics, Auth0 and Okta, HUMAN Security and Branch.io are bundled alongside. Location permissions are declared. Positive findings from R1: allowBackup and fullBackupContent are false, the network security configuration blocks cleartext traffic for all domains, local storage is encrypted with SQLCipher (net.zetetic.database), DETECT_SCREEN_CAPTURE is declared, and Auth0 and Okta are appropriate enterprise identity providers.

The analysis is static and did not include traffic capture.

Correspondence Summary

First attempts, 27 June 2026. Message one went to privacy@, security@ and dpo@skyscanner.net with BCC to the Austrian DSB, the German BfDI and CERT.at. It bounced for privacy@skyscanner.net and for the DSB address used in the BCC. Message two went to privacy@, security@ and press@skyscanner.net with BCC to the ICO enquiries address and CERT.at. It bounced for privacy@, press@ and the ICO enquiries address. The dpo@skyscanner.net address answered with an automated acknowledgment from a Zendesk system at 09:53 UTC on 27 June. No bounce was recorded for security@skyscanner.net and no reply came from it.

Second attempt, 17 July 2026. RFI-IRFOS re-sent the report to legal@skyscanner.net with HelloDPO and the ICO in copy, because it believed HelloDPO was Skyscanner's outsourced privacy counsel. legal@ answered with an automated acknowledgment. The ICO address ico@ico.org.uk bounced. Follow-ups on 27 July, 9 August and 29 August repeated the three questions.

Third party. On 1 September 2026 HelloDPO replied that it does not act for Skyscanner in this matter and that the named person is not employed by or working for HelloDPO. RFI-IRFOS replied on 3 September, removed HelloDPO and continued with legal@skyscanner.net. The final follow-up on 12 September set an answer deadline of 18 September.

Corrections to RFI-IRFOS statements. The follow-ups of 27 July and 9 August said that privacy@, security@, dpo@ and press@ all bounced. The Gmail record shows that privacy@ and press@ bounced, that dpo@ returned an automated acknowledgment, and that security@ produced neither a bounce nor a reply. The follow-up of 29 August stated that New Relic initialises at initOrder 0. The manifest value in R1 is initOrder 200, and this report uses 200.

No Skyscanner person ever replied. The only responses from Skyscanner systems were two automated acknowledgments.

Findings

C1: No consent management platform, Firebase and New Relic initialise before any consent mechanism

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

MLKitInitProvider	initOrder=99
FirebaseInitProvider	initOrder=100 directBootAware=true
NewRelicAppContentProvider	initOrder=200 (781 compiled classes)
RECEIVE_BOOT_COMPLETED	fires at device boot
CMP provider	none registered

What the New Relic SDK is built to collect. New Relic APM and real user monitoring record network request latency and payload metadata, unhandled exceptions, screen interaction events and device telemetry, and send them to New Relic infrastructure in the United States. R1 stated that this includes the search parameters of HTTP calls such as destination, dates and passenger count.

Limits of this finding. The analysis is static. RFI-IRFOS did not capture runtime traffic and did not verify which request fields reach New Relic in the shipping configuration. The finding establishes that the SDK starts before any consent mechanism and that no mechanism exists in the build to stop it.

The same dual pre-consent initialisation was described in R1 as two parallel findings, the Firebase and New Relic start in the first report and the absence of any consent platform in the second. This report merges them because they describe one mechanism.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the app is a mass-market travel product used across the EU, the data in question describes planned trips and location, and no consent control of any kind exists in the build.

Impact: The manifest registers four startup components in this order: MLKitInitProvider (initOrder 99), FirebaseInitProvider (initOrder 100, directBootAware), NewRelicAppContentProvider (initOrder 200) and a RECEIVE_BOOT_COMPLETED receiver. No consent management platform provider is registered anywhere in the build. Firebase Analytics and the New Relic APM and real user monitoring SDK (781 classes) therefore start when the process starts, before any consent dialog can exist.

C2: Explicit China PIPL consent flow built, no equivalent for EU users

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

```
key_login_sensitive_personal_data_china_consent  
key_login_share_personal_data_china_consent  
key_login_terms_of_service_privacy_policy_china_consent
```

The finding is the contrast and not the code. A consent flow of this kind shows that the engineering team can build one, and the build applies none to EU users. R1 described the PIPL implementation itself as technically sound. Whether a China-specific flow is actually shown to users in China and on which conditions was not tested. RFI-IRFOS read the strings and the startup sequence and did not run the app in a China locale.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to CRITICAL because the contrast shows that consent capability exists in the product and is not applied to EU users who are protected by GDPR.

Impact: The app contains explicit consent strings written for China's Personal Information Protection Law, while the same app initialises Firebase for EU users before any consent is shown. The strings implement informed consent for sensitive personal data and for sharing personal data.

C3: Braze geofencing with precise location permissions and boot persistence

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0

Braze SDK with BrazeGeofence
 class count: 423 (named classes, R1 of 2026-06-27 first message), 869 (including obfuscated internal package bo/app, R1 of 2026-06-27 second message)
 manifest: ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, RECEIVE_BOOT_COMPLETED

The two class counts come from two counting methods used in two reports sent on the same day. The lower figure counts named classes and the higher figure includes the obfuscated package bo/app.

Limits of this finding. Whether geofences are actually configured on the operator's Braze dashboard, and whether location is collected without user action, depends on server-side configuration that static analysis cannot see. The finding establishes capability, permissions and boot persistence.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to CRITICAL because geofencing turns the physical movements of travellers, for example at airports and hotels, into marketing events, and the build offers no consent control for it.

Impact: The Braze SDK is present with the BrazeGeofence integration. Braze geofences use device location permissions to monitor physical boundaries and trigger messages, push notifications and behavioural events when a device enters or leaves a defined zone. The app requests ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION, and RECEIVE_BOOT_COMPLETED lets monitoring resume at device boot without the user opening the app. No consent management platform exists, so R1 identified no legal basis for this processing.

H1: Chinese parent company, China National Intelligence Law Art. 7, no disclosed transfer analysis

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3

This finding is a legal analysis and not a technical observation. RFI-IRFOS does not claim that any data has been requested or transferred under that law. The point is the disclosure and transfer assessment duty: Art. 13(1)(f) GDPR requires information on transfers to third countries and Art. 44 to 49 require a mechanism and an assessment for each transfer. R1 anticipated that Skyscanner would answer that it is a UK entity and Trip.com merely a shareholder, and argued that corporate ownership does not remove the need for a transfer assessment for intra-group access.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the parent's jurisdiction applies to travel data of EU users and the app disclosed no assessment of it.

Impact: Skyscanner Limited (Edinburgh) is a wholly owned subsidiary of Trip.com Group (formerly Ctrip), a company listed on NASDAQ and headquartered in Shanghai. Article 7 of the National Intelligence Law of the People's Republic of China obliges organisations and

citizens to support and cooperate with national intelligence work. Travel itineraries, passport details entered at booking and location traces held by Skyscanner are controlled by a parent that is subject to that law. The privacy notice did not disclose this structure at the time of R1.

H2: Hardcoded Google API keys and Firebase project identifiers

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

```
google_api_key: [REDACTED IN PUBLIC REPORT, disclosed privately to Skyscanner in R1]
google_maps_key: [REDACTED IN PUBLIC REPORT, disclosed privately to Skyscanner in R1]
firebase_db_url: [REDACTED IN PUBLIC REPORT, disclosed privately to Skyscanner in R1]
project_id: [REDACTED IN PUBLIC REPORT, disclosed privately to Skyscanner in R1]
```

Limits of this finding. RFI-IRFOS sent no request with these keys. Whether they carry API restrictions, and whether the Realtime Database security rules allow unauthenticated access, was not tested. A legacy Firebase project of this kind is a common source of misconfiguration, so the operator should confirm restrictions and rules.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the Firebase project dates from 2015 and the keys sit in the same binary as a pre-consent analytics stack.

Impact: res/values/strings.xml in the production APK contains two Google API keys, a Firebase Realtime Database URL and a project identifier. Both keys are extractable from any downloaded APK with a single command.

H3: US marketing, survey, identity and bot detection stack without disclosure at the point of collection

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

Braze	CRM and messaging, US
Qualtrics	219 classes, in-app experience surveys
Auth0 + Okta	authentication, US
HUMAN Security	18 classes, HSBotDefender + HSAccountDefender
Branch.io	18 classes, deep link attribution

HUMAN Security collects device hardware identifiers, network telemetry, touch and interaction patterns and app environment signals to separate humans from bots. Bot prevention is a legitimate security purpose, and R1 argued that the processing is profiling under Art. 4(4) GDPR and that the processor must be disclosed under Art. 13(1)(e).

Limits of this finding. Static analysis shows the components are present. The privacy notice was read at the time of R1 and not re-read for this report. RFI-IRFOS did not observe runtime transfers.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because five separate US recipients operate in one app, and none of them is gated by a consent control.

Impact: The app embeds Braze (US customer engagement), Qualtrics (219 classes, in-app surveys, SAP-owned), Auth0 and Okta (US identity), HUMAN Security (18 classes, HSBotDefender and HSAccountDefender, device fingerprinting and behavioural signals for bot detection) and Branch.io (18 classes, deep link attribution). R1 found these third country recipients not adequately disclosed at the point of collection.

H4: Biometric authentication permissions in a flight search app

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3

Severity re-assessment since R1. On Android these permissions let the app call the system biometric prompt. The operating system matches the fingerprint or face and returns only a success or failure result to the app. The permission therefore does not show that Skyscanner receives or stores biometric data. RFI-IRFOS has re-assessed this finding as LOW and records it as an observation: a price comparison app declares a biometric permission, probably for optional account unlock, and the operator can state the purpose. The HIGH label in R1 is withdrawn in this report.

Impact: The manifest requests `USE_BIOMETRIC` and `USE_FINGERPRINT`. R1 classified this as HIGH and argued that biometric data is special-category data needing a documented necessity test.

Impact Analysis

Every EU user of the app is affected. Their search behaviour, planned trips and, where location is granted, physical movements are processed by analytics and marketing components that start before any consent control exists. Part of that processing sits with US providers, and the group parent is subject to Chinese intelligence law. For a traveller the concrete result is that the destination and dates of a trip, and the locations they pass through, can feed monitoring and marketing systems without a choice offered to them.

The Complete Chain

A user installs Skyscanner and opens it. The startup components run in a fixed order: ML Kit, then Firebase, then New Relic. No consent dialog and no consent platform exist in the build to stop them. The user searches for flights, and the monitoring SDK is built to record request metadata and interaction events. If the user grants location permission, the Braze geofence integration can use it to trigger messages when the device enters or leaves defined places, and the boot receiver lets this resume after a restart without the app being opened. Qualtrics, Auth0 and Okta, HUMAN Security and Branch.io add further US recipients. Behind all of it stands a group parent in Shanghai. The same app contains a fully built consent flow for users in China. When a researcher reports this, the only response is two automated receipts.

Data Protection, Article by Article

Article	Engaged by	Finding
Art. 4(4)	Profiling by device fingerprinting	H3
Art. 5(1)(a), (c)	Transparency and minimisation	C2, H4
Art. 6(1)	Lawful basis for pre-consent analytics and geofencing	C1, C3
Art. 7	Proof of consent, no platform	C1, C2, C3
Art. 9(1)	Location traces and biometric permission, legal interpretation	C3, H4
Art. 13(1)(e), (f)	Recipients and transfers not disclosed at collection	H1, H3
Art. 32(1)	Hardcoded keys	H2
Art. 44-49	US recipients and a parent under Chinese law	H1, H3

Regulatory & Legal Landscape

Skyscanner is established in the United Kingdom, so the Information Commissioner's Office is the lead authority for UK GDPR matters. For EU data subjects the competent authority is the one of their residence. RFI-IRFOS copied the Austrian DSB, and the verified ICO casework address icocasework@ico.org.uk on the follow-up of 9 August. The ICO enquiries and ico@ico.org.uk addresses bounced.

Indicators of Compromise & Reproducible Evidence

```
package:          net.skyscanner.android.main
version:          7.197 (Google Play, analysed 2026-06-27)
startup providers: MLKitInitProvider (99), FirebaseInitProvider (100),
                  NewRelicAppContentProvider (200)
consent strings:  key_login_sensitive_personal_data_china_consent
                  key_login_share_personal_data_china_consent
                  key_login_terms_of_service_privacy_policy_china_consent
components:       Braze (BrazeGeofence), Qualtrics, Auth0, Okta, HUMAN Security,
                  Branch.io, New Relic
permissions:      ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION,
                  RECEIVE_BOOT_COMPLETED, USE_BIOMETRIC, USE_FINGERPRINT
keys and project IDs: redacted in this public report, disclosed privately in R1
```

A second researcher can reproduce every item by unpacking the APK of the stated version and reading the manifest and resource files.

Disclosure Timeline & Outcome

2026-06-27 Version 7.197 analysed. Two reports sent. Embargo stated as 2026-09-25 in the first message and 2026-09-27 in the second. Bounces for [privacy@](mailto:privacy@skyscanner.net), [press@](mailto:press@skyscanner.net) and two authority addresses. Automated acknowledgment from [dpo@](mailto:dpo@skyscanner.net).

2026-07-17 Report re-sent to legal@skyscanner.net with HelloDPO and ICO in copy. Automated acknowledgment from [legal@](mailto:legal@skyscanner.net). Bounce for ico@ico.org.uk.

2026-07-27 Follow-up, day 10. No reply.

2026-08-09 Follow-up, DSB and the ICO casework address in copy. No reply.

2026-08-29 Follow-up with answer deadline 2026-09-05. No reply.

2026-09-01 HelloDPO replies that it does not act for Skyscanner.

2026-09-03 RFI-IRFOS removes HelloDPO from the correspondence.

2026-09-12 Follow-up to [legal@](mailto:legal@skyscanner.net) with answer deadline 2026-09-18 and embargo 2026-09-27. No reply.

2026-09-27 Embargo date reached, as stated to the working address in every message from 2026-07-27 onward. The earlier message of 2026-06-27 had stated 2026-09-25. Both dates have passed.

2026-10-17 This report published, 20 days after the later embargo date.

Residual Risk & Recommendations

All findings except H4 are open as of publication. RFI-IRFOS recommends that Skyscanner introduce a consent management platform that gates Firebase, New Relic, Braze and the other components before process start, make geofencing opt-in, publish a transfer assessment for intra-group access by Trip.com Group and disclose its US recipients at the point of collection, restrict the Google API keys and review the Firebase rules, and publish a working privacy and security disclosure address, since privacy@, press@ and the authority addresses used did not function. Users can withdraw location permission in Android settings. RFI-IRFOS will record any substantive reply from Skyscanner next to the original findings in the public dataset, whenever it arrives.

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 rest on static analysis of the published application with publicly available tools. No Skyscanner, Trip.com, Braze, New Relic or Google servers, accounts or infrastructure were tested. Technical evidence is archived under chain of custody and is available to supervisory authorities on request. Research conducted under ISO/IEC 29147, the freedom of science (Art. 17 StGG) and GDPR Art. 89. REF SKYSCANNER-2026-R1.