Coordinated Privacy Disclosure, Final Report

Agoda Android (com.agoda.mobile.consumer)

Agoda Company Pte. Ltd., Bangkok, Thailand, a subsidiary of Booking Holdings Inc. (NASDAQ: BKNG)

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

Target	Agoda, a major international travel booking platform
Package	com.agoda.mobile.consumer, version 14.22.0
Operator	Agoda Company Pte. Ltd., Bangkok, Thailand, a Booking Holdings Inc. subsidiary
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	Austrian DSB, Germany's BfDI, CERT.at, EDPS
Total Outbound Messages	5, across 77 days, to privacy@agoda.com, security@agoda.com, and dpo@agoda.com; one BCC address bounced outright.
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

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Agoda Company Pte. Ltd. that its Android app embeds two distinct Alipay security SDKs from Ant Group, an Alibaba affiliate headquartered in the People's Republic of China: com.alipay.apmobilesecuritysdk and com.alipay.mobilesecuritysdk. Together they collect device telemetry, including hardware fingerprints, network environment, and installed-app signals, and transmit it to Ant Group's infrastructure as part of payment fraud prevention. China's National Intelligence Law, Art. 7, requires any Chinese organisation to support, assist, and cooperate with the state's intelligence work, placing EU passenger device data processed by Ant Group's infrastructure within scope of that obligation. This computes to HIGH/8.7 under CVSS v4.0 and is held at that computed band, no escalation applied. This relationship is not disclosed in Agoda's privacy policy as a Chinese data sub-processor.

A second HIGH finding: the app's base network security configuration trusts both system and user-installed certificates with no domain restriction, meaning any device carrying a user-installed proxy certificate can intercept all production Agoda traffic in cleartext, including payment flows, booking data, and session tokens. This is a production misconfiguration, not a theoretical gap.

Three further findings compound the picture at MEDIUM. Four ContentProviders auto-initialise at app launch before any consent UI is shown, including Google's MobileAdsInitProvider, meaning the Advertising ID is collected and ad targeting begins before a user has consented to anything; Firebase and Google Maps API keys are hardcoded in the production binary. Braze, a US customer-engagement platform, runs 1,384 compiled classes of location, push, and persistent-storage tracking, running in parallel with 460 classes of AppsFlyer cross-app attribution, neither named as a data processor in the privacy policy. And the app routes EU user data through two simultaneous third-country transfers, Thailand (primary infrastructure) and China (Ant Group security telemetry), neither documented with Art. 46 safeguards. A sixth finding, undocumented DETECT_SCREEN_CAPTURE, RECORD_AUDIO, and ACTIVITY_RECOGNITION access, corrects to LOW. Genuine positives are worth naming: allowBackup is correctly set to false, USE_BIOMETRIC is implemented for authentication, not identification, and the Braintree payment integration follows established secure SDK patterns.

Five messages were sent across 77 days, to privacy@agoda.com, security@agoda.com, and dpo@agoda.com, cc'ing the Austrian DSB, Germany's BfDI, CERT.at, and the EDPS across the correspondence. One BCC address bounced outright. 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 Agoda Android application (com.agoda.mobile.consumer, version 14.22.0), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Ant Group's, Braze's, AppsFlyer's, or Google's backend infrastructure was performed.

Disposition

Six findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Two Alipay security SDKs routing EU device telemetry to Ant Group infrastructure in the People's Republic of China, and a network security configuration trusting user-installed certificates in the base config, both correct to HIGH. Pre-consent auto-initialization of four ContentProviders including Google Mobile Ads, a 1,384-class Braze behavioral tracking layer alongside 460-class AppsFlyer attribution tracking, and an undocumented dual Thailand-China third-country transfer all correct to MEDIUM. Undisclosed screen-capture detection, microphone, and activity-recognition access corrects to LOW. Five messages were sent across 77 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	Dual Alipay Security SDKs Route Device Telemetry to Ant Group, PRC
H1	HIGH	Base Network Security Config Trusts User-Installed Certificates Globally
C2	MEDIUM	Four Pre-Consent Auto-Initializing Providers, Including Google Mobile Ads
C3	MEDIUM	Braze and AppsFlyer Run 1,844 Combined Classes of Undisclosed US Behavioral Tracking
H2	MEDIUM	Undocumented Dual Thailand-China Third-Country Transfer
H3	LOW	Undocumented Screen-Capture, Microphone, and Activity-Recognition Access

Subject & Operator Analysis

Agoda Company Pte. Ltd., Bangkok, Thailand, a subsidiary of Booking Holdings Inc. (NASDAQ: BKNG), operates one of the largest international travel booking platforms. Thailand has no EU adequacy decision under GDPR Art. 45.

Genuine positives are worth naming. allowBackup is correctly set to false. USE_BIOMETRIC is implemented for authentication, not identification. The Braintree payment integration follows established secure payment SDK patterns. The core payment-authentication posture is sound; the transfer-governance and pre-consent SDK 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@agoda.com, security@agoda.com, and dpo@agoda.com across 77 days, cc'ing the Austrian DSB, Germany's BfDI, CERT.at, and the EDPS throughout the correspondence. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Dual Alipay Security SDKs Route Device Telemetry to Ant Group, PRC

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.

com.alipay.apmobilesecuritysdk and com.alipay.mobilesecuritysdk, two distinct Ant Group security SDKs, collect device fingerprint, hardware identifiers, network environment, and installed-app signals and transmit them to Ant Group's infrastructure as part of payment fraud prevention. China's National Intelligence Law Art. 7 requires any Chinese organisation to support, assist, and cooperate with the state's intelligence work. This relationship is not disclosed in Agoda's privacy policy as a Chinese data sub-processor.

```
com.alipay.sdk
com.alipay.apmobilesecuritysdk
com.alipay.mobilesecuritysdk
com.alipay.tscenter
```

Impact: EU travellers' device telemetry, including hardware identifiers and network environment, is processed by infrastructure operated by a PRC entity subject to a legal obligation to cooperate with state intelligence work, with no disclosure of this specific processing or recipient in the privacy policy.

Fix: Document the specific Art. 44-46 transfer basis for Ant Group processing, or replace the SDK with an EU-based or on-device-only fraud-prevention alternative. No confirmation that this has occurred was ever received.

H1: Base Network Security Config Trusts User-Installed Certificates Globally

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 trusts both system and user-installed certificates in the base config with no domain restriction. Any device with a user-installed proxy certificate (Burp Suite, mitmproxy, Charles Proxy) can intercept all production Agoda traffic in cleartext, including payment flows, booking data, and session tokens.

Impact: This is a production misconfiguration that allows on-path interception of payment and booking traffic on any device where a user-installed certificate is present, whether placed by the device owner or by malware.

Fix: Restrict the base network security config to system-trusted certificates only, and pin certificates for payment-critical domains. No confirmation that this has occurred was ever received.

C2: Four Pre-Consent Auto-Initializing Providers, Including Google Mobile Ads

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.

AnalyticsInitProvider (initOrder=9999), AppStartTimeProvider (initOrder=9999), FirebaseInitProvider (initOrder=100, directBootAware=true), and MobileAdsInitProvider (initOrder=100) all fire automatically at startup before any consent dialog is shown. ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_TOPICS confirm advertising-grade data collection is active. Firebase and Google Maps API keys are hardcoded in the production binary.

```
google_api_key: AIzaSyDfFR8B4OUA7qwjbSA6jxbYdOnba-RW6o8
google_maps_key: AIzaSyCoox8MGhZNVHgObAggGuK3GVY1_7OzOos
project_id: agoda-dd55
```

Impact: Google's advertising SDK begins collecting the Advertising ID and initialising ad targeting before the user has consented to any tracking, and Agoda's own analytics fires before everything else on the device.

Fix: Gate all four providers behind consent, and restrict the exposed API keys by package and certificate. No confirmation that this has occurred was ever received.

C3: Braze and AppsFlyer Run 1,844 Combined Classes of Undisclosed US Behavioral Tracking

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.

Braze (US), a customer-engagement platform, runs 1,384 compiled classes across location, push, storage, managers, events, and models modules, a full behavioural intelligence layer collecting location data, user events, and persistent device profiles. AppsFlyer (460 classes) runs cross-app attribution tracking in parallel. Neither is named as a data processor in Agoda's privacy policy.

Impact: Location data, behavioral events, and persistent device profiles reach two separate US processors with no Art. 13(1)(e) disclosure and no documented Art. 46 transfer mechanism for either.

Fix: Name Braze and AppsFlyer as data processors in the privacy policy and document the applicable transfer mechanism for each. No confirmation that this has occurred was ever received.

H2: Undocumented Dual Thailand-China Third-Country Transfer

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.

Agoda processes EU user data in Thailand (no GDPR Art. 45 adequacy decision) via its primary infrastructure, and separately routes payment and security telemetry through Ant Group's Chinese infrastructure (also no adequacy decision), two simultaneous third-country transfers without documented SCCs or binding corporate rules.

Impact: EU user data reaches two separate non-adequate jurisdictions through two independent processing paths, with Art. 13(1)(f)'s requirement to disclose the specific transfer mechanism at the point of collection unmet for either.

Fix: Document the specific Art. 46 transfer mechanism for both the Thailand and China transfer paths at the point of collection. No confirmation that this has occurred was ever received.

H3: Undocumented Screen-Capture, Microphone, and Activity-Recognition Access

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.

DETECT_SCREEN_CAPTURE monitors when users take screenshots of the app. RECORD_AUDIO accesses the microphone. ACTIVITY_RECOGNITION tracks physical movement. None of these are disclosed as processing activities with documented legal bases in Agoda's privacy policy.

Impact: Three separate sensor-access capabilities operate with no disclosed purpose or legal basis, leaving users unable to assess why a travel-booking app screens for screenshots, listens for audio, or tracks physical activity.

Fix: Document the specific purpose and legal basis for each permission, 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. 13, Art. 44-46	C1	Dual Alipay SDKs route device telemetry to Ant Group infrastructure in the PRC.
Art. 32	H1	Base network security config trusts user-installed certificates globally.
Art. 6, Art. 7	C2	Four pre-consent auto-initializing providers, including Google Mobile Ads.
Art. 13, Art. 46	C3	Braze and AppsFlyer run undisclosed US behavioral tracking.
Art. 13(1)(f), Art. 44-46	H2	Undocumented dual Thailand-China third-country transfer.
Art. 5(1)(c), Art. 13	H3	Undocumented screen-capture, microphone, and activity-recognition access.

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 H1 correct to HIGH, C2, C3, and H2 correct to MEDIUM, and H3 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: AGODA-2026.