Coordinated Privacy Disclosure, Final Report

Expedia Android (com.expedia.bookings)

Expedia Group Inc., Seattle, USA

DEFLECTED · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE, PRIVACY TEAM DECLINED ENGAGEMENT, REDIRECTED TO BUG-BOUNTY CHANNEL

Target	Expedia, a major international travel-booking platform
Package	com.expedia.bookings, version 2026.25.0
Operator	Expedia Group Inc., Seattle, USA
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
Total Outbound Messages	6, across 71 days, to privacy@expedia.com; security@expedia.com and dpo@expedia.com both hard-bounced.
Inbound Replies	One reply from Expedia's Privacy team, 51 days after the initial disclosure, declining to engage on the grounds that 'the Privacy group does not address security vulnerabilities,' redirecting to a bug-bounty inbox. No further reply of any kind followed.

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 Expedia Group Inc. that its Android app declares SHA-256 certificate pins exclusively for usebutton.com, an affiliate marketing platform, while Expedia's own booking, authentication, and payment endpoints remain unpinned. This inverts the expected risk model: the affiliate partner's traffic is hardened against interception while EU users' own credentials, session tokens, and payment data transiting Expedia's own infrastructure are not. This computes to HIGH/8.6 under CVSS v4.0, the single highest-scoring finding in this report.

Five further findings correct to MEDIUM. Salesforce Marketing Cloud, 1,780 compiled classes spanning push notifications, behavioral tracking, journey automation, and location services, initializes via two separate ContentProviders before any consent dialog is shown, alongside a pre-consent Firebase initialization with a hardcoded API key. Separately, the RECEIVE_BOOT_COMPLETED permission allows tracking infrastructure to activate at device boot, before the app is even opened or any consent screen has been seen, a point in the processing lifecycle where consent as a legal basis is structurally impossible under Art. 7. The app additionally declares GET_ACCOUNTS, enumerating every account registered on the device, together with READ_PRIVILEGED_PHONE_STATE, granting access to non-resettable hardware identifiers including IMEI and IMSI, a permission normally reserved for system applications. A Datadog WebView monitoring layer records user interaction on embedded third-party hotel-partner and booking-widget pages that are not operated by Expedia and have not consented to that monitoring. And Affirm, a Buy Now Pay Later provider processing credit-adjacent financial signals, is not named as a data processor anywhere in the privacy policy. Genuine positives are worth naming: allowBackup is correctly set to false, ArkoseLabs bot detection is a legitimate security measure, Braintree's fraud-prevention data collector follows established patterns, and biometric authentication is present.

Six messages were sent across 71 days to privacy@expedia.com; security@expedia.com and dpo@expedia.com both hard-bounced from the first send onward. The Austrian DSB, Germany's BfDI, and CERT.at were copied throughout. One reply arrived, 51 days after the initial disclosure, from Expedia's Privacy team, stating that 'the Privacy group does not address security vulnerabilities' and redirecting to a bug-bounty submission address, despite the disclosure being addressed to the Data Protection Officer with three specific GDPR questions. RFI-IRFOS responded the same day, noting the category mismatch and restating the three questions unchanged. No further reply of any kind followed. 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 Expedia Android application (com.expedia.bookings, version 2026.25.0), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Salesforce's, Datadog's, Affirm's, or Button's backend infrastructure was performed.

Disposition

Six findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. An inverted certificate-pinning configuration, hardened for an affiliate partner's domain while Expedia's own payment infrastructure is left unpinned, corrects to HIGH. Pre-consent Salesforce Marketing Cloud and Firebase initialization, tracking infrastructure that activates at device boot, full device account enumeration combined with a privileged, non-resettable hardware identifier, an undisclosed WebView monitoring layer covering third-party partner content, and an undisclosed Buy Now Pay Later processor all correct to MEDIUM. Six messages were sent across 71 days. One reply arrived, a deflection classifying the disclosure as out of scope for the Privacy team and redirecting to a security bug-bounty channel; no further reply followed.

ID	Severity	Title
H1	HIGH	Certificate Pinning Applied to an Affiliate Partner, Not to Expedia's Own Payment Infrastructure
C1	MEDIUM	Salesforce Marketing Cloud, 1,780 Classes, Initializes Pre-Consent via Two Providers
C2	MEDIUM	Tracking Infrastructure Activates at Device Boot, Before the App Is Opened
C3	MEDIUM	Full Device Account Enumeration Combined With a Non-Resettable Hardware Identifier
H2	MEDIUM	Datadog WebView Monitoring Covers Third-Party Partner Content
H3	MEDIUM	Undisclosed Buy Now Pay Later Processor

Subject & Operator Analysis

Expedia Group Inc., Seattle, USA, operates one of the largest travel-booking platforms distributed to EU residents. GDPR Art. 3(2) applies regardless of the operator's US establishment.

Genuine positives are worth naming. allowBackup is correctly set to false. ArkoseLabs bot detection is a legitimate security measure. Braintree's fraud-prevention data collector follows established secure patterns. USE_BIOMETRIC is present for authentication.

One Reply, a Deflection to the Wrong Channel

Six messages were sent across 71 days to privacy@expedia.com; security@expedia.com and dpo@expedia.com both hard-bounced from the first send onward. Fifty-one days after the initial disclosure, Expedia's Privacy team replied that 'the Privacy group does not address security vulnerabilities' and redirected to a bug-bounty submission address, despite the disclosure being addressed directly to the Data Protection Officer with three specific GDPR questions about consent timing, DPO notification, and DPIA existence. RFI-IRFOS responded the same day noting this was a data-protection disclosure, not a security-bounty submission, and restated the three questions unchanged. No further reply of any kind followed.

Findings

H1: Certificate Pinning Applied to an Affiliate Partner, Not to Expedia's Own Payment Infrastructure

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 contains SHA-256 pins exclusively for usebutton.com, an affiliate marketing platform, while Expedia's own booking, authentication, and payment endpoints are unpinned. This inverts the expected risk model: the affiliate partner's traffic is hardened, EU user credentials, session tokens, and payment data transiting Expedia's own infrastructure are not protected against MITM attacks by certificate pinning.

Impact: On a hostile network, an attacker can intercept Expedia's own authentication and payment traffic while the affiliate partner's traffic remains protected, exactly backwards from where the protection is most needed.

Fix: Extend certificate pinning to Expedia's own booking, authentication, and payment domains. No confirmation that this has occurred was ever received.

C1: Salesforce Marketing Cloud, 1,780 Classes, Initializes Pre-Consent via Two Providers

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.

com.salesforce.marketingcloud.MCInitContentProvider and com.salesforce.marketingcloud.sfmcsdk.SFMCSdkInitContentProvider both fire automatically at app startup, before any consent UI is shown. 1,780 compiled classes span push notifications, behavioral event tracking, journey automation, in-app messaging, and location services. Firebase also initializes pre-consent with a hardcoded API key.

```
google_api_key: AIzaSyDGeezqeG4YqDY03iNAPg3cGvvpt06zB1A
project_id: expedia-native-apps
```

Impact: Search queries, destination preferences, booking behavior, and session events are routed to Salesforce's US infrastructure before the user has consented to any processing, and Salesforce is not disclosed as a named data processor.

Fix: Gate both Salesforce providers and the Firebase initialization behind a consent mechanism, and restrict the exposed API key. No confirmation that this has occurred was ever received.

C2: Tracking Infrastructure Activates at Device Boot, Before the App Is Opened

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.

RECEIVE_BOOT_COMPLETED allows the app to register a BroadcastReceiver that fires when Android finishes booting, before the user has unlocked the device, opened the app, or seen any consent dialog. Combined with the two Salesforce Marketing Cloud providers, tracking infrastructure activates independently of any user interaction.

Impact: Processing begins at a point in the device lifecycle where consent as a legal basis is structurally impossible, since consent requires a prior, freely given, specific act.

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

C3: Full Device Account Enumeration Combined With a Non-Resettable Hardware Identifier

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1.

GET_ACCOUNTS allows enumeration of all accounts registered on the device, Google accounts, email accounts, and other installed apps' accounts, not required for Expedia's own account management. READ_PRIVILEGED_PHONE_STATE grants access to IMEI and IMSI, hardware identifiers that cannot be reset or rotated, not resettable the way advertising IDs are, and is normally reserved for system and carrier applications.

Impact: The combination of permanent hardware identifiers and full device account enumeration creates a cross-device identity profile that the user cannot delete or reset, with no legal basis disclosed for either permission.

Fix: Remove GET_ACCOUNTS and document a specific, necessary function for READ_PRIVILEGED_PHONE_STATE, or remove it. No confirmation that this has occurred was ever received.

H2: Datadog WebView Monitoring Covers Third-Party Partner Content

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 Datadog integration, 170 classes across WebView, RUM, HTTP, trace, and GraphQL modules, injects monitoring scripts into embedded WebView content. When a user views hotel listings, partner booking pages, or payment widgets inside the app, Datadog records interactions on pages that are not operated by Expedia and whose operators have not consented to that monitoring.

Impact: Third-party partners' content is monitored without their consent, and Expedia users' interactions on that content are recorded and transmitted to US infrastructure with no corresponding disclosure.

Fix: Restrict Datadog's WebView monitoring to first-party content only, and disclose the monitoring scope to partner sites. No confirmation that this has occurred was ever received.

H3: Undisclosed Buy Now Pay Later Processor

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.

Affirm's SDK, 306 classes, collects device signals, behavioral data, and financial context to support instalment payment decisions. Affirm is not named as a data processor anywhere in Expedia's privacy policy.

Impact: Credit-adjacent financial assessment data reaches a US processor with no Art. 13 disclosure naming it as a recipient, in a jurisdiction where processing such data for financial decisions carries additional obligations.

Fix: Name Affirm as a data processor in the privacy policy and document the applicable legal basis. 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. 32	H1	Certificate pinning applied to an affiliate partner, not to Expedia's own payment infrastructure.
Art. 6, Art. 7, Art. 13, Art. 44	C1	Salesforce Marketing Cloud and Firebase initialize pre-consent.
Art. 6, Art. 7	C2	Tracking infrastructure activates at device boot.
Art. 5(1)(c), Art. 13	C3	Full device account enumeration combined with a non-resettable hardware identifier.
Art. 13, Art. 32, Art. 44	H2	Datadog WebView monitoring covers third-party partner content.
Art. 13, Art. 44	H3	Undisclosed Buy Now Pay Later processor.

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, H1 corrects to HIGH, all other findings correct

to MEDIUM, 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: EXPEDIA-2026.