Coordinated Privacy Disclosure, Final Report

TripAdvisor Android (com.tripadvisor.tripadvisor)

TripAdvisor LLC, Massachusetts, USA

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE, SIX MESSAGES, NO SUBSTANTIVE REPLY

Target	TripAdvisor, one of the largest global travel review and booking platforms
Package	com.tripadvisor.tripadvisor, version 68.7.2
Operator	TripAdvisor LLC, Massachusetts, 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	Irish Data Protection Commission (lead supervisory authority), Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	6, across 77 days, to privacy@tripadvisor.com; security@tripadvisor.com and dpo@tripadvisor.com both hard-bounced.
Inbound Replies	0 substantive replies from TripAdvisor. One automated administrative message from the Irish DPC's general inbox, clarifying its own jurisdictional scope, not a reply from TripAdvisor.

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 TripAdvisor LLC that its Android app integrates BehavioSec, a LexisNexis Risk Solutions product, to capture individual keystrokes character by character as users type. The decompiled bytecode confirms methods that fire on every character change, capturing not just submitted text but typing rhythm, correction patterns, and hesitation pauses, a behavioral biometric profile under GDPR Art. 4(14) and Recital 51. BehavioSec's WebView component is integrated with LexisNexis ThreatMetrix device fingerprinting, meaning behavioral biometric data is joined with device fingerprinting before transmission to LexisNexis's US servers. This computes to HIGH/8.7 under CVSS v4.0. Processing biometric data at this scale requires explicit Art. 9(2)(a) consent and a mandatory Art. 35(3)(b) DPIA, neither confirmed. BehavioSec is not named as a data processor in TripAdvisor's privacy policy.

A second HIGH finding: the network security configuration grants cleartextTrafficPermitted=true to a named list of over 50 hotel reservation and advertising-verification domains, including several advertising-verification services whose cleartext inclusion confirms ad-tracking data flows unencrypted. When users browse hotel listings loading content from these partners, their search queries, dates, and session identifiers travel over unencrypted HTTP, visible to any network observer.

Three further findings correct to MEDIUM. OneTrust, a 466-class consent management platform, is compiled into the app but structurally bypassed: FirebaseInitProvider and MobileAdsInitProvider both initialize at the same priority level before any consent signal is available, architecturally equivalent to locking the door after the data has already left. Braze and AppsFlyer, 442 and 432 classes respectively, build behavioral marketing and cross-app attribution profiles with no Art. 13(1)(e) disclosure naming either as a processor. And three Privacy Sandbox Ad Services APIs are declared simultaneously, combined with boot-time tracking and a persistent foreground-service location capability, giving TripAdvisor's data collection architecture reach across the app's full device lifecycle. Genuine positives are worth naming: the base network security configuration correctly blocks cleartext traffic for all TripAdvisor-owned domains, the cleartext exception list is scoped to third parties only; OneTrust's presence shows some awareness of consent obligations even where the implementation fails; no passport-scanning or biometric-identification SDKs were found; and Braintree follows established secure payment patterns.

Six messages were sent across 77 days to privacy@tripadvisor.com; security@tripadvisor.com and dpo@tripadvisor.com both hard-bounced from the first send onward. The Irish Data Protection Commission, as lead supervisory authority for TripAdvisor's EU operations, along with the Austrian DSB, Germany's BfDI, and CERT.at, were copied throughout. One automated message arrived from the Irish DPC's own general inbox clarifying that channel's jurisdictional scope, not a reply from TripAdvisor. TripAdvisor itself never substantively replied 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 TripAdvisor Android application (com.tripadvisor.tripadvisor, version 68.7.2), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with LexisNexis's, OneTrust's, Braze's, or AppsFlyer's backend infrastructure was performed.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. A behavioral-biometric keystroke capture SDK integrated with device fingerprinting, and cleartext HTTP transmission to 50-plus hotel partner domains, both correct to HIGH. A structurally bypassed consent platform, undisclosed US behavioral-marketing infrastructure, and a full-lifecycle advertising and location-tracking API stack all correct to MEDIUM. Six messages were sent across 77 days. TripAdvisor itself never substantively replied.

ID	Severity	Title
C1	HIGH	BehavioSec Captures Keystroke Biometrics, Integrated With Device Fingerprinting
C3	HIGH	Cleartext HTTP to Over 50 Hotel Partner and Ad-Verification Domains
C2	MEDIUM	OneTrust Consent Platform Present but Structurally Bypassed
H1	MEDIUM	Undisclosed US Behavioral Marketing and Attribution Infrastructure
H2	MEDIUM	Full-Lifecycle Advertising and Location-Tracking API Stack

Subject & Operator Analysis

TripAdvisor LLC, Massachusetts, USA, operates one of the largest global travel review and booking platforms. The Irish Data Protection Commission is the competent lead supervisory authority for TripAdvisor's EU operations.

Genuine positives are worth naming. The base network security configuration correctly sets cleartextTrafficPermitted to false for all TripAdvisor-owned domains, the cleartext exception list is scoped to third-party partners only. OneTrust's presence shows some awareness of consent obligations even where the implementation fails. No passport-scanning or biometric-identification SDKs beyond BehavioSec were found. Braintree, TripAdvisor's payment processor, is a well-established provider following secure patterns.

Six Messages, No Substantive Reply

All six messages in this case's correspondence record were sent to privacy@tripadvisor.com across 77 days; security@tripadvisor.com and dpo@tripadvisor.com both hard-bounced from the first send onward. The Irish DPC, Austrian DSB, Germany's BfDI, and CERT.at were copied throughout. One automated message arrived, from the Irish DPC's own general inbox, clarifying that its channel does not accept AI Act market-surveillance queries, an administrative note about the regulator's own scope, not a reply from TripAdvisor. TripAdvisor itself never substantively replied at any point.

Findings

C1: BehavioSec Captures Keystroke Biometrics, Integrated With Device Fingerprinting

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.

BehavioSecClient.keyboardTargetTextChanged fires on every single character the user types, capturing typing rhythm, correction patterns, and hesitation pauses, a behavioral biometric profile under GDPR Art. 4(14) and Recital 51. BehavioWebView's TMXCallbackHandler confirms integration with LexisNexis ThreatMetrix device fingerprinting, joining behavioral biometric data with device fingerprints before transmission to LexisNexis servers in the US.

```
BehavioSecClient.registerKeyboardTarget(fieldId, Z, Activity)
BehavioSecClient.keyboardTargetTextChanged(fieldId, old, new, Activity)
BehavioSecClient.sendData(Activity)
BehavioWebView$TMXCallbackHandler
```

Impact: A persistent behavioral biometric identity, built from typing rhythm and correction patterns and joined with device fingerprinting, travels with the user across sessions without the explicit Art. 9(2)(a) consent or mandatory Art. 35(3)(b) DPIA this scale of biometric processing requires.

Fix: Obtain explicit, granular Art. 9(2)(a) consent before any BehavioSec capture, and complete the mandatory DPIA. No confirmation that this has occurred was ever received.

C3: Cleartext HTTP to Over 50 Hotel Partner and Ad-Verification 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 explicitly grants cleartextTrafficPermitted=true to a named list of over 50 hotel reservation and distribution system domains, including doubleclick.net, doubleverify.com, and adsafeprotected.com, advertising-verification domains whose cleartext inclusion confirms ad-tracking data flows unencrypted.

```
amazonaws.com, cloudfront.net, expedia.com, agoda.net,
doubleclick.net, doubleverify.com, adsafeprotected.com, moatads.com,
bookwize.com, dirs21.de, e4jconnect.com, synxis.com, innroad.com,
arrivalist.com, yieldoptimizer.com, flashtalking.com, serving-sys.com
+ 35 additional hotel CRS/GDS domains
```

Impact: When users browse hotel listings loading content from these partners, their search queries, dates, and session identifiers travel over unencrypted HTTP, visible to any network observer on the same connection.

Fix: Remove the cleartext exception for these domains and require HTTPS across all third-party partner connections. No confirmation that this has occurred was ever received.

C2: OneTrust Consent Platform Present but Structurally Bypassed

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.

OneTrust, a 466-class consent management platform, is compiled into the app, but FirebaseInitProvider and MobileAdsInitProvider both initialize at the same priority level before any consent signal is available. The presence of OneTrust does not constitute GDPR-compliant consent when Firebase Analytics and Google Ads are already running before OneTrust has had an opportunity to present the consent layer.

```
firebaseApiKey: AIzaSyDlYn-hW-KiUgjE62jNRl0ffHmbmL6ajq8
google_api_key: AIzaSyB7v8Byw4j_O7FUs9L216qsfafFKkAG5M8
project_id: api-project-1070328450902
```

Impact: The presence of a technically capable consent platform is architecturally undermined by two tracking providers that initialize at the same priority level and win the race to collect data first.

Fix: Gate Firebase and Google Mobile Ads behind OneTrust's consent signal. No confirmation that this has occurred was ever received.

H1: Undisclosed US Behavioral Marketing and Attribution Infrastructure

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 (442 classes) handles push notification targeting, behavioral automation, and persistent campaign tracking. AppsFlyer (432 classes) builds cross-app attribution profiles. Neither is named as a data processor under Art. 13(1)(e).

Impact: Large-scale behavioral marketing and attribution data reaches two separate US processors with no Art. 13 disclosure and no documented Art. 46 transfer safeguard for either.

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

H2: Full-Lifecycle Advertising and Location-Tracking API Stack

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.

ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_TOPICS are all declared simultaneously, combined with RECEIVE_BOOT_COMPLETED and FOREGROUND_SERVICE_LOCATION.

Impact: Advertising-ID linkage, cross-app attribution, and interest-based profiling operate in parallel with tracking that starts at device boot and persistent location access through a foreground service, giving the collection architecture reach across the full device lifecycle.

Fix: Document a specific, disclosed purpose for the combined API and permission set, or remove those without one. 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. 9, Art. 35, Art. 44	C1	BehavioSec captures keystroke biometrics, integrated with device fingerprinting.
Art. 32	C3	Cleartext HTTP to over 50 hotel partner and ad-verification domains.
Art. 6, Art. 7	C2	OneTrust consent platform present but structurally bypassed.
Art. 13, Art. 44	H1	Undisclosed US behavioral marketing and attribution infrastructure.
Art. 6, Art. 22	H2	Full-lifecycle advertising and location-tracking API stack.

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 C3 correct to HIGH, C2, H1, and H2 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: com.tripadvisor.tripadvisor.