Coordinated Privacy Disclosure, Final Report

Momondo Android (com.momondo.flightsearch)

Momondo A/S, Copenhagen, Denmark, operating on Kayak Software Corporation infrastructure

ENGAGED, THEN DECLINED EVIDENCE · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE

Target	Momondo, a European flight-search platform
Package	com.momondo.flightsearch, version 258.2
Operator	Momondo A/S, Copenhagen, Denmark, running on Kayak Software Corporation's own infrastructure
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	Danish Datatilsynet (lead supervisory authority), Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	9, across 87 days, to privacy@momondo.com, dpo@momondo.com, and, from 27 August, directly to Kayak's Senior Privacy and Cybersecurity Counsel.
Inbound Replies	Two substantive replies from Kayak's Senior Privacy and Cybersecurity Counsel, 27 August and 22 September, after 61 days of account-management auto-replies only. Kayak ultimately declined to provide the specific evidence requested.

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 the Momondo Android app contains 32,895 compiled classes under com.kayak.android, eighteen times larger than the largest third-party SDK found anywhere else in this research series, running on Kayak's own Firebase project, Kayak's own CDN, and Kayak's own affiliate booking infrastructure. The only Momondo-branded string anywhere in the binary is a single deep-link verification file. This is not a shared library; it is a complete second application. Users who consented to processing by Momondo A/S have not consented to processing by Kayak Software Corporation, a legally distinct US entity operating on the same infrastructure. This computes to MEDIUM/6.9 under CVSS v4.0.

The single highest-scoring finding: FullStory session recording, instrumented across every View, Flutter widget, and WebView in the app through a native Rust bridge (RustInterface) that makes the actual scope of data collection unverifiable from static analysis in either direction. FullStory's own data-type registry lists EMAIL as a capturable field. This computes to HIGH/8.7. Two further HIGH findings: the app's base network security configuration permits cleartext HTTP transmission of flight searches, booking data, and session traffic across all network paths; and Kayak's own internal PKI root certificate and intermediate authority certificate, used internally to inspect Kayak's own traffic, are shipped inside the public Momondo production binary on Google Play, confirming the shared build pipeline and exposing internal infrastructure to public inspection.

Two further findings correct to MEDIUM. Three ContentProviders (Firebase, Sentry, Adjust) initialize automatically before any consent signal exists, and RECEIVE_BOOT_COMPLETED fires tracking infrastructure at device boot, before the app is even opened. MoEngage, a 273-class US customer-engagement platform running push targeting and behavioral event tracking, is not named as a data processor. Genuine positives are worth naming: allowBackup is correctly set to false, biometric authentication is used properly, no passport-scanning or biometric-collection SDKs were found, and the overall permission footprint is leaner than comparable apps.

Nine messages were sent across 87 days. The first 61 days produced only an automated account-management reply. On 27 August, Loren Maloney, Kayak's Senior Privacy and Cybersecurity Counsel, replied substantively, describing corporate contact policies, an Art. 27 EU-representative designation, and a general shared-portfolio disclosure clause, and asserting that FullStory masks personal data with email excluded. RFI-IRFOS's response the same week pointed out that none of the three described mechanisms is the specific Art. 26 joint-controller transparency GDPR requires, and asked for the exact user-facing sentence naming Kayak Software Corporation as joint controller, or for FullStory's own field-exclusion export, not a restated assurance. On 22 September, Kayak's counsel replied a second time, declining to provide either document on grounds that the requested materials 'contain confidential information concerning KAYAK's internal processes, systems and governance arrangements.' The 90-day embargo, restated unchanged throughout, elapses today. This report and the accompanying closure notice publish on the stated date, with every original finding unremediated and the specific evidentiary gap unresolved.

Scope: Root-level static analysis of the production Momondo Android application (com.momondo.flightsearch, version 258.2), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Kayak's, FullStory's, or MoEngage's backend infrastructure was performed.

Disposition

Six findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. FullStory session recording with an unauditable native Rust bridge, cleartext HTTP transmission of flight-search and booking data, and Kayak's own internal PKI root and intermediate certificates shipped in the public production binary all correct to HIGH. An undisclosed Kayak rebrand with an unresolved Art. 26 joint-controller gap, pre-consent tracking infrastructure, and an undisclosed US CRM platform all correct to MEDIUM. Nine messages were sent across 87 days. Kayak's counsel engaged substantively twice, then declined to provide the specific documentation requested.

ID	Severity	Title
C2	HIGH	FullStory Session Recording via an Unauditable Native Rust Bridge
C4	HIGH	Cleartext HTTP Permitted for All Flight Search and Booking Traffic
H1	HIGH	Kayak's Own Internal PKI Certificates Shipped in the Public Production Binary
C1	MEDIUM	Momondo Is an Undisclosed Kayak Rebrand, Art. 26 Joint-Controller Gap Unresolved
C3	MEDIUM	Three Pre-Consent Providers, Tracking Starts at Device Boot
H2	MEDIUM	Undisclosed US CRM Platform

What Momondo Got Right

allowBackup is correctly set to false. USE_BIOMETRIC is used for authentication, not identification. No passport-scanning or biometric-collection SDKs were found. The overall permission footprint is leaner than comparable apps in this campaign.

Nine Messages, Two Substantive Replies, a Final Refusal

Nine messages were sent across 87 days. The first 61 days produced only an automated account-management auto-reply. On 27 August 2026, Loren Maloney, Kayak's Senior Privacy and Cybersecurity Counsel, replied substantively, the first human-authored response on the thread, describing corporate contact policies, an Art. 27 EU-representative designation, and a general shared-portfolio disclosure clause, and asserting that FullStory masks personal data with email excluded. RFI-IRFOS's response pointed out precisely that none of the three described mechanisms is the specific Art. 26 transparency GDPR requires, and asked for the exact user-facing sentence naming Kayak Software Corporation, or for FullStory's own field-exclusion export, not a restated position. On 22 September 2026, Kayak's counsel replied a second time, declining to provide either document on the stated grounds that the requested materials contain confidential information about Kayak's internal processes, systems, and governance arrangements. The Danish Datatilsynet, lead supervisory authority, remained in copy throughout.

Findings

C2: FullStory Session Recording via an Unauditable Native Rust Bridge

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.

FullStory (164 classes plus a native com/fullstory/rust/RustInterface bridge) instruments every View, Flutter widget, and WebView in the app. Its own data-type registry lists EMAIL as a capturable field. The native Rust bridge means the actual scope of what is collected and transmitted cannot be determined from the APK alone, in either direction.

```
InstrumentInjectorBridgeImpl (>=60 view injector instances)
FSFlutterDelegate -> Flutter widget tree instrumentation
RustInterface -> native Rust data processing + transmission
activate_capture_snippet -> WebView JS injection
EMAIL -> listed as a capturable field type
```

Impact: Kayak asserted email is excluded from capture, but this cannot be independently verified because the masking configuration lives in FullStory's dashboard and Kayak's own backend, not in anything visible in the binary, and Kayak declined to provide the field-exclusion export that would settle the question.

Fix: Provide FullStory's field-exclusion export for this app's organisation, or a DPIA documenting the configuration and its date. No confirmation that this has occurred was ever received.

C4: Cleartext HTTP Permitted for All Flight Search and Booking Traffic

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.

cleartextTrafficPermitted is set to true as the global base config. Flight search queries, booking data, and session traffic, revealing travel dates, destinations, passenger count, and price sensitivity, may all be transmitted over unencrypted HTTP on every network path.

Impact: Any network observer can intercept and read flight-search and booking traffic in cleartext, on any public network.

Fix: Set cleartextTrafficPermitted to false globally. No confirmation that this has occurred was ever received.

H1: Kayak's Own Internal PKI Certificates Shipped in the Public Production Binary

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.

Kayak's internal root CA and R9 Intermediate Authority 2 certificates, used internally by Kayak engineers to inspect their own traffic, are distributed inside every Momondo install on the Play Store. Their validity periods (root 2018-2028, intermediate 2022-2027) confirm active use.

```
CN=KAYAK Internal Root CA (issued 2018, valid to 2028)
CN=R9 Intermediate Authority 2 (issued 2022, valid to 2027)
```

Impact: Any party obtaining these certificates can impersonate Kayak or Momondo internal services to a device running a debug build, and their presence definitively confirms Momondo's build pipeline is Kayak's build pipeline.

Fix: Remove Kayak's internal PKI certificates from any publicly distributed binary, regardless of configuration scope. No confirmation that this has occurred was ever received.

C1: Momondo Is an Undisclosed Kayak Rebrand, Art. 26 Joint-Controller Gap Unresolved

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.

32,895 compiled classes under com.kayak.android are present in the Momondo APK, running on Kayak's own Firebase project, Kayak's own CDN, and Kayak's own affiliate booking infrastructure. The only Momondo-branded string in the entire binary is a single deep-link verification file. Kayak's counsel described corporate contact policies, an Art. 27 EU-representative designation, and a general shared-portfolio clause, none of which names Kayak Software Corporation to a Momondo user as joint controller with the essence of that arrangement, as Art. 26(2) requires.

```
compiled classes: 32,895 (com.kayak.android.*)
firebase project: android-kayak-app
backend CDN: kayak.com
only Momondo-branded string: /.well-known/assetlinks.json
```

Impact: A user who consented to Momondo A/S processing their travel data has not consented to Kayak Software Corporation, a legally distinct US entity, processing the same data on the same infrastructure, and no document naming that arrangement to the user by name has been produced.

Fix: Publish the specific user-facing document naming Kayak Software Corporation as joint controller, with the essence of the arrangement as Art. 26(2) requires. No confirmation that this has occurred was ever received.

C3: Three Pre-Consent Providers, Tracking Starts at Device Boot

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), SentryPerformanceProvider (initOrder=200), and SystemLifecycleContentProvider (Adjust attribution) all initialize automatically before any consent signal exists. RECEIVE_BOOT_COMPLETED fires tracking infrastructure at device boot, before the app is opened.

Impact: Kayak's Firebase infrastructure receives data before any EU user has had an opportunity to consent or refuse, at a point in the processing lifecycle where consent as a legal basis is structurally impossible.

Fix: Gate all three providers and RECEIVE_BOOT_COMPLETED behind a consent mechanism. No confirmation that this has occurred was ever received.

H2: Undisclosed US CRM Platform

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.

MoEngage, 273 classes, runs push notification targeting, campaign automation, and behavioural event tracking. Combined with the Kayak Firebase backend and FullStory session recording, this forms a three-layer data intelligence stack entirely invisible in the Momondo-branded privacy policy.

Impact: Behavioral and engagement data reaches a third US processor with no Art. 13(1)(e) disclosure naming it as a recipient.

Fix: Name MoEngage 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. 5(1)(a), Art. 9, Art. 13, Art. 44	C2	FullStory session recording via an unauditable native Rust bridge.
Art. 32	C4	Cleartext HTTP permitted for all flight search and booking traffic.
Art. 25, Art. 32	H1	Kayak's own internal PKI certificates shipped in the public production binary.
Art. 13(1)(a), Art. 13(1)(e), Art. 26	C1	Momondo is an undisclosed Kayak rebrand, Art. 26 joint-controller gap unresolved.
Art. 6, Art. 7	C3	Three pre-consent providers, tracking starts at device boot.
Art. 13, Art. 44	H2	Undisclosed US CRM platform.

not capture real-world blast radius on its own. In this report, C2, C4, and H1 correct to HIGH, C1, C3, 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: MOMONDO-2026-R1.