Koordinierte Offenlegung, Abschlussbericht

Fluege.de Android (de.unister.fluege)

Betrieben unter dem Paket de.unister.fluege (Invia Group)

STILLE · FALL GESCHLOSSEN UND VERÖFFENTLICHT AM 25. SEPTEMBER 2026, AM ANGEGEBENEN EMBARGO-DATUM, SECHS NACHRICHTEN, KEINE ANTWORT

Ziel	Fluege.de, ein deutscher Flugsuche- und Buchungsdienst
Package	de.unister.fluege, Version 4.48.0
Betreiber	Invia Group, betrieben unter dem Paket de.unister.fluege
Erstmeldung	2026-06-27
Angegebenes Embargo	2026-09-25, dem Betreiber direkt in der Erstmeldung mitgeteilt
Bericht veröffentlicht	2026-09-25, zum angegebenen Datum
Behörden	Germany’s BfDI (federführende Behörde), österreichische DSB, CERT.at
Ausgehende Nachrichten gesamt	6 über 77 Tage, an datenschutz@fluege.de; privacy@fluege.de und security@fluege.de prallten beide ab.
Eingehende Antworten	0. Keine einzige Antwort jeglicher Art wurde je empfangen.

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Am 27. Juni 2026 meldete RFI-IRFOS, dass die Android-App von Fluege.de zwar Usercentrics als zertifizierte Consent-Management-Plattform einbindet, gleichzeitig aber FirebaseInitProvider (initOrder=100) und Adjust über SystemLifecycleContentProvider vor Usercentrics feuern lässt, bevor überhaupt ein Einwilligungssignal vorliegt. Die Einwilligung, die Usercentrics später einholt, kann die bereits beim Geräteboot übertragenen Daten nicht rückwirkend legitimieren. Dieser Befund korrigiert sich auf MEDIUM/6.9.

Der schwerwiegendste Befund: Microsoft Clarity, mit 750 Klassen das größte einzelne SDK in der App, zeichnet vollständige Sitzungswiedergaben auf, jede Interaktion, jedes berührte Formularfeld, Scroll-Tiefe, Rage-Clicks, auf genau den Bildschirmen, auf denen Nutzerinnen und Nutzer Reisedaten, Passagierzahlen und Zahlungsdetails eingeben, und dies noch vor jeder Einwilligung. Dieser Befund korrigiert sich auf HIGH/8.7, den höchsten Wert in diesem Bericht.

Drei weitere Befunde runden das Bild ab. Die App deklariert gleichzeitig alle vier Privacy-Sandbox-Werbe-APIs, persistente Werbe-ID, App-übergreifendes Conversion-Tracking, interessensbasiertes Themen-Profiling und dynamische Zielgruppen-Zugehörigkeit für gezielte Werbung, ohne dass dies unter Art. 13 als spezifischer Verarbeitungszweck offengelegt wird. CALL_PHONE erlaubt der App, Anrufe ohne die übliche Bestätigung über den Android-Dialer zu tätigen. Und Braze (444 Klassen, einschließlich Standortmodul) ermöglicht standortbasiertes Profiling von Reisemustern, kombiniert mit Abflugort, Zielort und Reisedaten, ohne als Auftragsverarbeiter benannt zu sein. Positiv zu vermerken: die Basis-Netzwerksicherheitskonfiguration setzt cleartextTrafficPermitted korrekt auf false, Usercentrics selbst ist eine technisch solide CMP-Wahl, die Lücke liegt in der Initialisierungsreihenfolge, nicht in der Plattform, und es wurden keine Passscanning-, biometrischen oder Zahlungskarten-OCR-SDKs gefunden.

Sechs Nachrichten wurden über 77 Tage gesendet, an datenschutz@fluege.de; privacy@fluege.de und security@fluege.de prallten beide vom ersten Versand an ab. Deutschlands BfDI als federführende Behörde sowie die österreichische DSB und CERT.at waren durchgehend informiert. Keine einzige Antwort, weder automatisiert noch menschlich, wurde je empfangen. Das 90-Tage-Embargo, dem Betreiber direkt in der Erstmeldung mitgeteilt, läuft heute ab. Dieser Bericht und die begleitende Abschlussmitteilung veröffentlichen zum angegebenen Datum.

Scope: Root-Level-Code-Analyse der produktiven Fluege.de-Android-Anwendung (de.unister.fluege, Version 4.48.0), aus dem Google Play Store geladen und am 27. Juni 2026 untersucht. Es wurde kein Konto angelegt, und es fand keine Interaktion mit der Backend-Infrastruktur von Microsoft, Adjust oder Braze statt.

Disposition

Fünf Befunde wurden am 27. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Microsoft Clarity, eine vollständige Session-Recording-Plattform mit 750 Klassen, die noch vor der eigenen Usercentrics-Einwilligung aktiv ist, korrigiert sich auf HIGH. Die strukturelle Umgehung der eigenen Consent-Management-Plattform, die gleichzeitige Deklaration aller vier Privacy-Sandbox-Werbe-APIs, und Braze mit nicht offengelegtem standortbasiertem Profiling korrigieren sich auf MEDIUM. CALL_PHONE ohne Bestätigung korrigiert sich auf LOW. Sechs Nachrichten wurden über 77 Tage gesendet. Keine einzige Antwort wurde je empfangen.

ID	Severity	Title
C2	HIGH	Microsoft Clarity zeichnet vollständige Sitzungswiedergaben vor Einwilligung auf
C1	MEDIUM	Die eigene Consent-Management-Plattform wird strukturell umgangen
C3	MEDIUM	Alle vier Privacy-Sandbox-Werbe-APIs gleichzeitig deklariert
H2	MEDIUM	Braze mit nicht offengelegtem standortbasiertem Profiling
H1	LOW	CALL_PHONE ohne Nutzerbestätigung

Was Fluege.de richtig macht

Die Basis-Netzwerksicherheitskonfiguration setzt cleartextTrafficPermitted korrekt auf false, nur das Trustpilot-Widget und localhost erhalten Klartext-Ausnahmen. Usercentrics ist eine technisch solide CMP-Wahl, die Implementierungslücke liegt in der Initialisierungsreihenfolge, nicht in der Plattform selbst. Es wurden keine Passscanning-, biometrischen oder Zahlungskarten-OCR-SDKs gefunden. Der Berechtigungs-Fußabdruck ist schlanker als bei den meisten Apps dieser Branche.

Sechs Nachrichten, keine Antwort

Alle sechs Nachrichten dieses Falls wurden über 77 Tage an datenschutz@fluege.de gesendet; privacy@fluege.de und security@fluege.de prallten beide vom ersten Versand an ab. Deutschlands BfDI als federführende Behörde sowie die österreichische DSB waren durchgehend informiert. Keine einzige Antwort, weder automatisiert noch menschlich, wurde je empfangen.

Findings

C2: Microsoft Clarity zeichnet vollständige Sitzungswiedergaben vor Einwilligung auf

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.

Microsoft Clarity zeichnet vollständige Sitzungswiedergaben auf: jede UI-Interaktion, jedes berührte Formularfeld, Scroll-Tiefe, Rage-Clicks und Dead-Clicks. Mit 750 Klassen ist dies das größte einzelne SDK in der App. Reisedaten, Abflugort, Zielort und Passagierzahl liegen innerhalb des Erfassungsbereichs von Clarity, bevor irgendeine Einwilligung erteilt wurde. Clarity-Daten werden an Microsoft-Azure-Infrastruktur (USA) übertragen.

Impact: Sensible Reiseplanungs- und Zahlungsdaten werden in vollständiger Sitzungswiedergabe erfasst, bevor der Nutzer überhaupt Gelegenheit hatte, einer Verarbeitung zuzustimmen, und Microsoft Clarity ist nicht als Auftragsverarbeiter nach Art. 13(1)(e) benannt.

Fix: Microsoft Clarity hinter den bereits vorhandenen Usercentrics-Consent-Mechanismus verschieben. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

C1: Die eigene Consent-Management-Plattform wird strukturell umgangen

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) und Adjust über SystemLifeCycleContentProvider feuern beide, bevor Usercentrics, die im Binary vorhandene, zertifizierte Consent-Management-Plattform, überhaupt ein Einwilligungssignal sammeln konnte.

```
google_api_key: AIzaSyAROfZ5e5mbLbKViJi6xq6qqgWtG_ltKn0
project_id: fluege-2
```

Impact: Die App verfügt über eine funktionierende, zertifizierte CMP, lässt aber gleichzeitig zu, dass Firebase und Adjust noch vor deren Einsatz Daten sammeln, eine architektonische Lücke, die die spätere Einwilligung nicht rückwirkend heilen kann.

Fix: FirebaseInitProvider und Adjust hinter Usercentrics' Consent-Signal verschieben. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

C3: Alle vier Privacy-Sandbox-Werbe-APIs gleichzeitig deklariert

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, ACCESS_ADSERVICES_TOPICS und ACCESS_ADSERVICES_CUSTOM_AUDIENCE sind alle vier gleichzeitig deklariert, der vollständige Satz für persistente Werbe-ID, App-übergreifendes Conversion-Tracking, interessensbasiertes Themen-Profiling und dynamische Zielgruppen-Zugehörigkeit.

Impact: Auf einer Flugsuch-Anwendung, deren Nutzerdaten Ziel- und Reisedaten mit hoher Spezifität enthalten, ermöglicht diese Kombination ein sehr präzises Werbeprofil, ohne dass dies als spezifischer Verarbeitungszweck offengelegt wird.

Fix: Jede der vier APIs einzeln unter Art. 13 als spezifischen Verarbeitungszweck offenlegen und hinter Einwilligung gaten. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

H2: Braze mit nicht offengelegtem standortbasiertem Profiling

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 (444 Klassen, einschließlich Standortmodul) ermöglicht geofenced Push-Benachrichtigungen und standortbasierte Verhaltenssegmentierung. In Kombination mit Flugsuch-Kontext, Abflugort, Zielort, Reisedaten, ermöglicht Standortdaten ein hochpräzises Profiling von Reisemustern. Braze ist nicht als Auftragsverarbeiter nach Art. 13(1)(e) benannt.

Impact: Standortdaten fließen in Kombination mit Reiseplanungsdaten an ein US-CRM-System, ohne dass dies offengelegt wird.

Fix: Braze als Auftragsverarbeiter in der Datenschutzerklärung benennen und die Rechtsgrundlage dokumentieren. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

H1: CALL_PHONE ohne Nutzerbestätigung

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.

CALL_PHONE erlaubt der App, direkt einen Anruf zu tätigen, ohne den Android-Dialer anzuzeigen oder eine Nutzerbestätigung einzuholen. Zweck und Umfang dieser Berechtigung sind unter Art. 13 nicht offengelegt.

Impact: Die App verfügt über die technische Fähigkeit, Anrufe ohne Wissen des Nutzers zu tätigen, einschließlich potenziell kostenpflichtiger Nummern.

Fix: Den Standard-Dialer-Flow (Wählen → Bestätigen) verwenden, außer wenn eine spezifische, dokumentierte Funktion dies erfordert. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

Datenschutz, Artikel für Artikel

Die Befunde ordnen sich einer kleinen, spezifischen Gruppe von DSGVO-Bestimmungen zu, hier gesammelt statt über die Befunde verstreut.

Artikel	Befund	Grundlage
Art. 6, Art. 7, Art. 13, Art. 44	C2	Microsoft Clarity zeichnet vollständige Sitzungswiedergaben vor Einwilligung auf.
Art. 6, Art. 7	C1	Die eigene Consent-Management-Plattform wird strukturell umgangen.
Art. 6, Art. 13, Art. 22	C3	Alle vier Privacy-Sandbox-Werbe-APIs gleichzeitig deklariert.
Art. 13, Art. 44	H2	Braze mit nicht offengelegtem standortbasiertem Profiling.
Art. 5(1)(c), Art. 13	H1	CALL_PHONE ohne Nutzerbestätigung.

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 ist die Scoring-Richtlinie von RFI-IRFOS, keine Ober- oder Untergrenze. Sie liefert einen reproduzierbaren, für Dritte nachvollziehbaren Ausgangspunkt für den Schweregrad und erfasst reale Blast-Radius-Effekte nicht von sich aus. In diesem Bericht korrigiert sich C2 auf HIGH, C1, C3 und H2 korrigieren sich auf MEDIUM, und H1 korrigiert sich auf LOW, jeweils auf ihrer eigenen berechneten Stufe, ohne Eskalation. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: fluege.de-2026.