Coordinated Privacy Disclosure, Final Report

Joyn AT Android (at.zappn)

ProSiebenSat.1 Digital GmbH, Unterföhring bei München, Germany

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, TWO DAYS AFTER THE EMBARGO STATED IN THE ORIGINAL 25 JUNE 2026 NOTICE

Target	Joyn AT (formerly Zappn), a free streaming platform for Austrian public and commercial TV
Package	at.zappn
Operator	ProSiebenSat.1 Digital GmbH, Medienallee 7, 85774 Unterföhring bei München
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators	Bayerisches Landesamt für Datenschutzaufsicht (BayLDA, lead SA), Austrian DSB, CERT.at
Total Outbound Messages	5, across 79 days to datenschutz@joyn.de / privacy@joyn.at / dpo@prosiebensat1.com.
Inbound Replies	4 automated acknowledgments confirming receipt only. No substantive human reply 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 25 June 2026, RFI-IRFOS disclosed to ProSiebenSat.1 Digital GmbH that its Joyn AT Android streaming app ships Braze with full geofencing enabled, a continuously-running location foreground service (foregroundServiceType=location) that monitors when a viewer enters or exits defined geographic zones, confirmed active via getBrazeGeofenceReEligibilityManager and getGeofencesEnabledFromConfiguration. No disclosed feature of a TV streaming platform requires geofence-precision physical location; this is a marketing-automation capability, proximity-triggered push notifications and location-based audience segmentation, layered onto a product whose core function is watching television. Braze Inc. is a US company subject to the CLOUD Act, and the geofencing data is sent to a US datacenter in Ashburn, Virginia.

A second finding names a redundant dual-measurement gap, not a single data flow: Nielsen Digital Content Ratings and Comscore Streaming Tag both run simultaneously, two competing US audience-measurement platforms both capturing what content is watched, for how long, and at what time, and both transmitting that data to US servers. A third names a proprietary ProSiebenSat.1 tracking framework, EasyTracking, with a JavaScript execution bridge allowing tracking logic to be updated server-side at any time without an app update, the same transparency gap as Google Tag Manager but built in-house.

Five messages were sent across 79 days to datenschutz@joyn.de, privacy@joyn.at, and dpo@prosiebensat1.com. Four drew an identical automated acknowledgment confirming receipt only. Not one substantive human reply was ever received. The 90-day embargo, set at first contact on 25 June 2026, elapsed on 23 September 2026. This report and the accompanying closure notice publish two days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Joyn AT Android application (at.zappn, version 6.6.1-AOS-JOYN_AT-2099528, 82.7 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with ProSiebenSat.1's, Braze's, Nielsen's, or Comscore's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Braze geofencing, running as a continuous location foreground service in a TV streaming app, reaches HIGH on the computed CVSS score alone, no editorial escalation needed. Pre-consent Firebase initialization, dual Nielsen/Comscore US audience measurement, a proprietary runtime-JavaScript tracking SDK, and advertising-attribution tracking all correct to MEDIUM. An undocumented SCHEDULE_EXACT_ALARM permission corrects to LOW, and boot-time auto-start corrects to OBSERVATIONAL. Five messages were sent across 79 days, drawing four identical automated acknowledgments and zero substantive human reply.

ID	Severity	Title
C1	MEDIUM	Firebase Initializes Before the App's Own Consent Management Platform Can Load
H1	HIGH	Braze Geofencing Runs as a Continuous Location Foreground Service in a TV Streaming App
H2	MEDIUM	Two Competing US Audience-Measurement Platforms Run Simultaneously
H3	MEDIUM	A Proprietary Runtime-JavaScript Tracking SDK With the Same Transparency Gap as Google Tag Manager
H4	MEDIUM	Advertising ID and Attribution Tracking in a Free-to-Air Streaming App
M1	LOW	Undocumented SCHEDULE_EXACT_ALARM Permission
M2	OBSERVATION	Boot-Time Auto-Start

Subject & Operator Analysis

Joyn AT, formerly Zappn, is a free streaming platform for Austrian public and commercial TV, operated by ProSiebenSat.1 Digital GmbH.

Several genuine positives are worth naming. allowBackup is correctly set to false. A network security configuration is present. A consent management platform exists and is served from the operator's own infrastructure. The app's permission set is otherwise clean for a streaming product: no camera, no microphone, no contacts access. FOREGROUND_SERVICE_MEDIA_PLAYBACK is justified by the core video-playback function.

Five Messages, Four Automated Acknowledgments, Zero Substantive Reply

This case's correspondence record involved a working contact channel from the first message; no address bounced. Five messages were sent across 79 days to datenschutz@joyn.de, privacy@joyn.at, and dpo@prosiebensat1.com, cc'ing the Bavarian data protection authority (BayLDA) as lead SA and the Austrian DSB. Four of the five drew an identical automated acknowledgment confirming receipt only. Not one substantive human reply, addressing any specific finding, was ever received.

Findings

C1: Firebase Initializes Before the App's Own Consent Management Platform Can Load

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.

FirebaseInitProvider is declared with android:initOrder=0x64 (100) and android:directBootAware=true, executing before any Activity and before any consent screen. The app does implement a consent management platform (CMP) at s-int.p7s1.io/cmp/views/joyn-at-app.html, but Firebase initializes before that CMP can load, making any consent gate configured there structurally unable to cover Firebase's own processing.

```
com.google.firebase.provider.FirebaseInitProvider
  android:initOrder=0x64 (100), android:directBootAware=true
CMP: s-int.p7s1.io/cmp/views/joyn-at-app.html (present, but initializes after Firebase
    )
```

Impact: A CMP that a user could reasonably believe gates all tracking does not, in practice, gate the app's own Firebase initialization, which has already run by the time the CMP can render.

Fix: Defer FirebaseInitProvider initialization until after the existing CMP has recorded a consent decision. No confirmation that this has occurred was ever received.

H1: Braze Geofencing Runs as a Continuous Location Foreground Service in a TV Streaming App

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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

Braze is configured to run geofencing via a foreground service declared foregroundServiceType=0x1 (location), confirmed active through getBrazeGeofenceReEligibilityManager and getGeofencesEnabledFromConfiguration. No disclosed streaming-platform feature requires geofence-precision physical location; this is a marketing-automation capability, proximity-triggered push notifications and location-based audience segmentation, not a function of watching television. Braze Inc. is a US company subject to the CLOUD Act; geofence data is sent to sdk.iad-01.braze.com, a US datacenter in Ashburn, Virginia.

```
foregroundServiceType=0x1 (location)
getBrazeGeofenceReEligibilityManager (active)
getGeofencesEnabledFromConfiguration (enabled)
https://sdk.iad-01.braze.com/api/v3/  (US datacenter, Ashburn, Virginia)
```

Impact: A viewer of a free TV streaming app has their real-world physical location continuously monitored against defined geographic zones and sent to a US-based CRM platform, for a purpose unrelated to the app's core streaming function.

Fix: Remove geofencing or gate it behind an explicit, separate, opt-in consent flow distinct from general app usage. No confirmation that this has occurred was ever received.

H2: Two Competing US Audience-Measurement Platforms Run Simultaneously

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.

Nielsen Digital Content Ratings and Comscore Streaming Tag are both active simultaneously, each independently capturing what content is watched, for how long, and at what time, and transmitting it to US servers. Both Nielsen Holdings and Comscore, Inc. are US companies subject to the CLOUD Act.

```
de.joyn.player3.nielsen   -- Nielsen Digital Content Ratings
de.joyn.tracking.comscore -- Comscore Streaming Tag
aos_toggle_enable_nielsen_new_player (enabled)
```

Impact: Detailed viewing behavior is duplicated across two separate US-based measurement processors instead of a single documented pipeline, widening the population of parties holding viewing-history data on the same users.

Fix: Consolidate to a single audience-measurement processor, document both under Art. 28 and Art. 13(1)(e) if both are retained, and confirm SCCs cover the US transfer. No confirmation that this has occurred was ever received.

H3: A Proprietary Runtime-JavaScript Tracking SDK With the Same Transparency Gap as Google Tag Manager

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9.

ProSiebenSat.1's proprietary EasyTracking framework includes a JavaScript execution bridge (oasisjsbridge.JsValue) allowing tracking logic to run and be updated at runtime. The specific tags and scripts active in the current production configuration are not visible in the static binary, since they can be changed server-side without an app update.

```
de.prosiebensat1.easytracking
de.prosiebensat1.easytracking.js.a/b/c
de.prosiebensat1digital.oasisjsbridge.JsValue
```

Impact: The app's actual tracking behavior can change at any time via a server-side push, invisible to app-store review and to a user who reviewed the app's data practices only at install time.

Fix: Disclose the EasyTracking JS bridge's runtime-injection capability explicitly and commit to a change-notification process for material tracking updates. No confirmation that this has occurred was ever received.

H4: Advertising ID and Attribution Tracking in a Free-to-Air Streaming App

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.

AD_ID, ACCESS_ADSERVICES_AD_ID, and ACCESS_ADSERVICES_ATTRIBUTION are all declared, enabling cross-app behavioral profiling that links a user's Joyn AT viewing activity to their broader device usage, beyond what ad delivery alone requires.

Impact: A user's viewing activity on a free streaming platform can be linked to their advertising profile across other apps they have never consciously associated with Joyn.

Fix: Document an individual Art. 6(1) legal basis and Art. 13(1)(c) disclosure for the advertising-attribution pipeline. No confirmation that this has occurred was ever received.

M1: Undocumented SCHEDULE_EXACT_ALARM Permission

LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0.

SCHEDULE_EXACT_ALARM is declared, requiring explicit user grant on Android 12 and above, but its purpose is not documented anywhere in the app's privacy materials as reviewed.

Impact: The permission's purpose, plausibly recording reminders, is undocumented; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low despite the undocumented access.

Fix: Document the specific feature SCHEDULE_EXACT_ALARM supports. No confirmation that this has occurred was ever received.

M2: Boot-Time Auto-Start

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

BOOT_COMPLETED is declared alongside an active Adjust SDK integration, meaning the app starts automatically at device boot.

Impact: The app begins running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove it if not load-bearing for a specific, disclosed feature. 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. 7, Art. 25	C1	Firebase pre-consent initialization structurally ahead of the app's own CMP.
Art. 5(1)(b)/(c), Art. 6(1), Art. 13(1)(e)	H1	Continuous location foreground service for marketing geofencing in a streaming app.
Art. 13(1)(e), Art. 28, Art. 44-49	H2	Duplicated, undisclosed US audience-measurement transfer.
Art. 5(1)(a), Art. 13(1)(e)	H3	Runtime tracking-injection capability outside app-store review.
Art. 5(1)(b), Art. 6(1)	H4	Undisclosed advertising-attribution tracking.

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, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, H1 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; C1, H2, H3, and H4 correct to MEDIUM to match their own computed bands; M1 corrects to LOW on its own computed band; M2 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: JOYN-2026-R1.