Coordinated Privacy Disclosure, Final Report

FlixBus Android (de.flixbus.app)

FlixMobility SE, Munich, Germany

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO, TWELVE MESSAGES, ZERO REPLY OF ANY KIND

Target	FlixBus, a long-distance bus and travel booking Android app
Package	de.flixbus.app
Operator	FlixMobility SE, Munich, Germany
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six 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	12, across 79 days: an initial attempt to datenschutz@flixbus.com bounced outright; press@flixbus.com accepted all eleven further messages.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

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 FlixMobility SE that its FlixBus Android app enables com_braze_optin_when_push_authorized, a configuration flag that causes a single tap granting push-notification permission to simultaneously enroll the user in Braze's behavioral marketing platform, with no second, purpose-specific consent dialog. GDPR Art. 7(2) requires that when consent for one purpose is bundled with other matters, the request must be presented in a manner clearly distinguishable from those other matters; push notifications and behavioral marketing CRM are legally distinct processing purposes, and a single tap cannot lawfully serve as consent for both. The same Braze integration runs active geofence and continuous location tracking, brazeGeofenceApi and brazeLocationApi both confirmed active, sending persistent location data, capable of tracking when a user enters or exits bus stations and terminals, to a US datacenter in Ashburn, Virginia.

A second finding names a build-hygiene gap, not a single tracking flow: a Google Maps API key is hardcoded in plaintext in the AndroidManifest.xml metadata block, extractable without any decompilation, a straightforward quota-exhaustion denial-of-service vector against FlixBus's own station-finder and in-app maps. A production-shipped DebugSettingsActivity ships alongside an inconsistent consent architecture: Crashlytics collection is explicitly enabled with no consent gate, while Analytics collection is correctly disabled, an internal inconsistency in how the same consent framework is applied across two comparable SDKs.

Twelve messages were sent across 79 days. The first attempt, to datenschutz@flixbus.com, bounced outright; press@flixbus.com accepted delivery for all eleven further messages, cc'ing the Bavarian data protection authority (BayLDA), the Austrian DSB, and CERT.at. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six 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 FlixBus Android application (de.flixbus.app, version 9.81.0, 18.6 MB), as reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with FlixMobility's or Braze's backend infrastructure was performed.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. A Braze configuration flag that conflates push-notification permission with a separate marketing-consent action, combined with active Braze geofence and continuous location tracking to a US datacenter, reaches HIGH on the computed CVSS score alone. A hardcoded Google Maps API key, a production-shipped debug settings activity with an inconsistent consent architecture, and undisclosed advertising-attribution tracking all correct to MEDIUM. Boot-time auto-start corrects to OBSERVATIONAL. Twelve messages were sent across 79 days. Not one reply of any kind was ever received.

ID	Severity	Title
H1	HIGH	Push-Notification Consent Conflated With Marketing Opt-In, Alongside Active Geofence Tracking
H2	MEDIUM	Google Maps API Key Hardcoded in the Manifest
H3	MEDIUM	Debug Settings Activity in Production, Alongside an Inconsistent Consent Architecture
H4	MEDIUM	Advertising Attribution Tracking in a Bus-Ticket Booking App
M1	OBSERVATIONAL	Boot-Time Auto-Start

Subject & Operator Analysis

FlixBus is a long-distance bus and travel booking platform operated by FlixMobility SE, headquartered in Munich, Germany, placing the Bavarian data protection authority (BayLDA) as lead supervisory authority.

Several genuine positives are worth naming. allowBackup is correctly set to false. usesCleartextTraffic defaults correctly to false. firebase_analytics_collection_enabled is correctly set to false, and google_analytics_automatic_screen_reporting_enabled is also correctly disabled. Adyen, a reputable payment processor, handles payments. The permission footprint is otherwise minimal, no microphone overreach, no biometric abuse. The overall hygiene is largely present; the Braze opt-in flag and the hardcoded Maps key are both fixable within a single release cycle.

Twelve Messages, One Bounce, Zero Reply

This case's correspondence record involved one address failure before a working channel was confirmed. The first message, to datenschutz@flixbus.com, bounced outright on 25 June 2026. press@flixbus.com accepted delivery for all eleven further messages across the following 79 days, cc'ing the Bavarian data protection authority, the Austrian DSB, and CERT.at. Not one reply, automated or human, was ever received on any address at any point.

Findings

H1: Push-Notification Consent Conflated With Marketing Opt-In, Alongside Active Geofence Tracking

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.

com_braze_optin_when_push_authorized is enabled, causing the Braze SDK to treat a user's push-notification permission grant as simultaneous consent to Braze's behavioral marketing platform, with no second, purpose-specific consent dialog, a direct conflict with GDPR Art. 7(2)'s distinguishability requirement. The same integration runs active geofence and continuous location tracking (brazeGeofenceApi, brazeLocationApi, com_braze_enable_location_collection all confirmed active), sending persistent location data to sdk.iad-01.braze.com, a US datacenter in Ashburn, Virginia. Braze Inc. is a US company subject to the CLOUD Act.

```
com_braze_optin_when_push_authorized (enabled) -- push permission grant = automatic
    Braze marketing optin
brazeGeofenceApi (active), brazeLocationApi (active)
com_braze_enable_location_collection (enabled)
https://sdk.iad-01.braze.com/api/v3/ (US datacenter, Ashburn, Virginia)
```

Impact: A single tap intended to grant notification permission also enrolls a user in behavioral marketing tracking with no separate consent, and geofence-based location tracking capable of recording station and terminal visits is sent to a US-based processor.

Fix: Separate push-notification permission from Braze marketing enrollment into two distinct, purpose-specific consent actions, and gate geofence/location collection behind its own explicit opt-in. No confirmation that this has occurred was ever received.

H2: Google Maps API Key Hardcoded in the Manifest

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

A Google Maps API key is hardcoded in plaintext in the AndroidManifest.xml meta-data block, extractable with a simple aapt dump, no decompilation required. A quota-exhaustion denial-of-service against FlixBus's own station-finder and in-app maps is a straightforward abuse vector.

```
com.google.android.geo.API_KEY = AIzaSyB34C0IkbqHHabPOwhrPOtiuJGu_NKXX1g (
    AndroidManifest.xml, meta-data block)
```

Impact: The key is trivially extractable without decompilation, and repeated API calls against it could exhaust quota until FlixBus's own station-finder and maps features fail for legitimate users.

Fix: Restrict the Maps API key by package name and SHA-1 certificate fingerprint. No confirmation that this has occurred was ever received.

H3: Debug Settings Activity in Production, Alongside an Inconsistent Consent Architecture

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.

DebugSettingsActivity is registered in the production AndroidManifest.xml; debug configuration surfaces should not ship in production builds. Separately, firebase_crashlytics_collection_enabled is explicitly set to true with no consent gate, while firebase_analytics_collection_enabled is correctly set to false, an inconsistency in how the same consent framework is applied across two comparable Firebase SDKs.

```
de.flixbus.settings.DebugSettingsActivity (registered in production manifest)
firebase_crashlytics_collection_enabled=true (explicit, not consent-gated)
firebase_analytics_collection_enabled=false (correctly disabled)
```

Impact: A debug configuration surface ships in the production binary, and Crashlytics collection proceeds without the same consent gate correctly applied to Analytics, an internally inconsistent implementation of the same consent framework.

Fix: Remove DebugSettingsActivity from production builds and apply the same consent gate to Crashlytics that is already correctly applied to Analytics. No confirmation that this has occurred was ever received.

H4: Advertising Attribution Tracking in a Bus-Ticket Booking 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_ATTRIBUTION, and ACCESS_ADSERVICES_AD_ID are all declared. Advertising attribution linking bus-ticket booking behavior to a user's cross-app behavioral profile has no documented purpose in this context and is not disclosed in the app's privacy documentation as reviewed.

```
com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
```

Impact: A user's ticket-booking activity can be linked to their advertising profile across other apps, with no disclosed purpose or legal basis located.

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

M1: 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, meaning the app starts automatically at device boot without user interaction.

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.

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(2), Art. 6(1), Art. 13(1)(e)	H1	Push-notification consent conflated with marketing opt-in, plus undisclosed geofence tracking.
Art. 5(1)(f), Art. 32	H2	Hardcoded, trivially extractable Google Maps API key.
Art. 32	H3	Debug activity in production and inconsistent consent gating across comparable SDKs.
Art. 5(1)(b), Art. 6(1)	H4	Undisclosed advertising-attribution tracking in a booking app.

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; H2, H3, and H4 correct to MEDIUM to match their own computed bands; M1 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: FLIXBUS-2026-R1.