Coordinated Security & Privacy Disclosure, Final Report

Diagnosia (com.diagnosia.fachinformation)

Österreichische Apotheker-Verlagsgesellschaft m.b.H.

RESOLVED · CASE CLOSED 22 SEPTEMBER 2026, ONE DAY BEFORE THE ORIGINAL EMBARGO

Target	Diagnosia, professional drug-interaction and dosage reference app for healthcare professionals
Package	com.diagnosia.fachinformation
Operator	Österreichische Apotheker-Verlagsgesellschaft m.b.H., FN 127484b, Nordbergstraße 1/1/61, 1090 Vienna, Austria
Predecessor Entity	Diagnosia Internetservices GmbH, merged into the operator above 2021-09-01
Initial Disclosure	2026-06-22 (redelivered after an initial bounce, formally acknowledged 2026-06-25)
Original Embargo	90 days, expiring 2026-09-23
Case Status	RESOLVED, closed by mutual written agreement 2026-09-22
Final Verified Build	v7.1.2, versionCode 7120, independently pulled and decompiled by RFI-IRFOS 2026-09-21

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 22 June 2026, RFI-IRFOS disclosed to Diagnosia, a professional drug-interaction and dosage reference application used by physicians and pharmacists, that its Firebase and Sentry SDKs initialize automatically at process start, before any consent screen can render, and that a hardcoded Firebase API key shipped without any externally verifiable restriction, alongside a complete absence of Firebase App Check anywhere in the binary. Two further suspected pathways, an embedded Facebook/Meta SDK and a cloud backup channel exposing the local search-history database, were named as additional concerns.

Over the following three months, under a dedicated compliance function established 6 August 2026, the operator investigated every point raised. Two claims, the Facebook/Meta SDK and the search-history backup exposure, did not hold up under independent re-verification and were withdrawn by RFI-IRFOS itself, the backup claim after RFI-IRFOS identified its own misreading of the app's own backup-rule XML. RFI-IRFOS's own framing of the confirmed SDK-initialization finding, published initially as confirmed third-party tracking, was itself corrected on 21 September 2026 after the operator repeatedly and correctly pointed out that initialization timing had been confirmed, an actual data transfer at that instant had not.

The operator then shipped a build, v7.1.2, that independently, freshly verified by RFI-IRFOS against a device pull on the day of closure, disables the automatic FCM registration and automatic Sentry initialization paths, and supplied verifiable evidence, matched byte for byte against the live binary, that the Firebase API key carries a genuine server-side Application and API restriction. RFI-IRFOS credited all three conditions it had itself named as required for closure, and, following a further, well-reasoned exchange in which the operator distinguished those closure conditions from a set of broader structural observations never demonstrated as active exploits against the current build, RFI-IRFOS closed DIAGNOSIA-R1 on 22 September 2026, one day ahead of the original embargo.

Scope: Root-level static analysis of the production Diagnosia Android application (com.diagnosia.fachinformation), covering the AndroidManifest, resource strings, and decompiled dex across every publicly pulled build from the original audit (June 2026) through the final closure verification (v7.1.2, versionCode 7120, 21 September 2026). No dynamic instrumentation, live traffic capture, or interaction with the operator's production backend was performed at any point; every finding and every remediation claim in this report was verified from the client binary itself.

Disposition

Two originally-suspected findings, a Facebook/Meta SDK and a cloud backup exposure of the local search-history database, were withdrawn by RFI-IRFOS in full after independent verification showed neither existed as claimed. The confirmed core finding, Firebase and Sentry SDKs initializing before any consent screen renders, was independently re-verified against a freshly pulled production build on the day of closure, and the specific behaviors that carried real consequence, automatic FCM token registration and automatic analytics collection, are now confirmed disabled pending user consent. A remaining set of structural observations, FCM token enumeration risk given the continued absence of Firebase App Check, a US CLOUD Act third-country transfer question, and the Article 9 classification of professional drug searches, were never demonstrated as reproducible exploits against the current build and are documented here as ongoing observations. They did not block this closure. This is the fastest full resolution RFI-IRFOS has recorded in this disclosure programme to date, closed a day before the original 90-day embargo. It closed on the strength of genuine, sustained technical engagement, not on a deadline.

ID	Severity	Title
C1	MEDIUM	Pre-Consent Auto-Initialization of Firebase and Sentry, Remediated

Subject & Operator Analysis

Diagnosia is a professional drug-interaction, dosage, and prescribing-information reference application, marketed to physicians, pharmacists, and other healthcare professionals in Austria and Germany. The application is operated by Österreichische Apotheker-Verlagsgese llschaft m.b.H. (FN 127484b, Vienna), the publisher of Austria's official pharmacists' trade journal. The app was originally built and operated under a separately incorporated entity, Diagnosia Internetservices GmbH, which was merged into Österreichische Apotheker-Verla gsgesellschaft m.b.H. on 1 September 2021 and deregistered from the Austrian companies register on 7 September 2021, independently confirmed by RFI-IRFOS against two separate register extracts. RFI-IRFOS's original report named the pre-merger entity and described the operator as a "healthcare provider"; both were corrected on the public ledger on 21–22 September 2026. The operator's actual registered business purpose is publishing and IT services for healthcare professions, not patient care.

Initial disclosure correspondence was misdirected for approximately six weeks to an address without an active compliance function. A dedicated Quality & Compliance function, under Ruprecht Leitner, took over the case on 6 August 2026, after which the exchange moved from silence to a sustained, technically substantive back-and-forth, several rounds of which were resolved within hours of each other.

Architecture & Data Flow

Diagnosia is a native Android application that bundles the Firebase SDK (Analytics, Cloud Messaging, Installations) and the Sentry Android SDK for crash and performance telemetry, alongside Expo/React Native components used for push-notification handling (expo-notifications). Push delivery on Android is implemented over Firebase Cloud Messaging, which is the documented reason FirebaseInitProvider is present in the manifest at all: it is pulled in transitively by the Firebase Messaging library via the Android manifest merger, not added directly by the operator's own code.

Local search-history persistence uses Room/expo-sqlite, a separate storage domain from the app's SecureStore-scoped Android Backup rules (secure_store_backup_rules.xml, secure_store_data_extraction_rules.xml), which explicitly do not cover the database domain the search history is stored in. No dynamic instrumentation of this architecture was performed; every claim in this section is drawn from static analysis of the manifest, decompiled resources, and dex bytecode of the versions listed in the Disclosure Timeline below.

Findings

C1: Pre-Consent Auto-Initialization of Firebase and Sentry, Remediated

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 at time of disclosure. REMEDIATED 2026-09-21.

com.google.firebase.provider.FirebaseInitProvider and io.sentry.android.core.SentryInitProvider / SentryPerformanceProvider are registered as Android ContentProviders, which the platform guarantees run at process start, before Application.onCreate() and before any Activity, including any consent screen. Leitner's own 13 August 2026 reply did not dispute the presence of either provider. This was the case's central finding from the original 22 June 2026 disclosure through the correction described below.

Correction, made by RFI-IRFOS on 21 September 2026: the original published finding stated this as confirmed third-party tracking, describing the providers as initializing "third-party data transmission." The operator asked repeatedly, first on 14 August and again in later rounds, for a concrete transmission proof, the endpoint, the timing, the data category actually transferred. RFI-IRFOS never supplied one. What was, and remains, independently confirmed is the initialization timing itself: two third-party SDKs bootstrap before the user has made any consent choice. Whether that bootstrap alone transmitted identifying data at that instant was never demonstrated. The finding is stated here, and was corrected on the public ledger, as what was actually verified: pre-consent SDK initialization, not a confirmed data transfer.

Remediation, independently verified by RFI-IRFOS on 21 September 2026 against a freshly pulled and decompiled build, v7.1.2, versionCode 7120: the AndroidManifest now sets firebase_messaging_auto_init_enabled="false" and firebase_analytics_collection_enabled="false", and io.sentry.auto-init="false" has been present and confirmed intentional since v7.1.1. Together these stop the automatic FCM token registration and the automatic Sentry ContentProvider initialization path. FCM registration and Sentry's application-context initialization now occur only after the user has made an active choice.

Residual, not rescored: FirebaseInitProvider and the Sentry providers remain registered in the manifest and continue to bootstrap the underlying SDK objects unconditionally at process start. That is inert library scaffolding, not the behavior that carried the original consequence, RFI-IRFOS treats it as a documented architectural fact, not a further open finding.

Impact: At the time of the original disclosure, this exposed device- and installation-level identifiers to two US-headquartered third parties before an EU-based healthcare professional had made any consent decision, on an application used in a clinical context. Following the confirmed 21 September 2026 remediation, the specific mechanisms that generated an actual token or analytics event are gated behind user consent.

Fix: Firebase and Sentry auto-initialization is gated behind explicit consent in v7.1.1/v7.1.2 (firebase_messaging_auto_init_enabled, firebase_analytics_collection_enabled, io.sentry.auto-init all set to false). Independently confirmed by RFI-IRFOS against the live binary, not taken on the operator's word alone.

Withdrawn and Narrowed Findings

H3, Facebook/Meta SDK claim, WITHDRAWN 2026-08-13

The original report identified com/facebook/... smali classes and inferred an embedded Meta SDK. Following the operator's 13 August 2026 reply, RFI-IRFOS traced the classes to com.facebook.react, the React Native framework package namespace, not a Meta analytics or advertising SDK. Withdrawn in full the same day, without requiring further evidence from the operator.

C2, Search-History Cloud Backup Exposure, WITHDRAWN 2026-08-14

The original report read secure_store_backup_rules.xml and secure_store_data_extraction_rules.xml as covering the app's search-history database. Following the operator's 13 August 2026 rebuttal, RFI-IRFOS re-read both rules against a freshly pulled v7.0.3 build and confirmed both rules scope exclusively to the sharedpref domain, explicitly excluding the SecureStore sub-path; the search history persists via Room/expo-sqlite, the database domain, which neither rule includes. RFI-IRFOS's original report had quoted the rule text correctly but overreached in its conclusion. Withdrawn in full, with the error stated plainly as RFI-IRFOS's own.

H2, Firebase API Key Exposure, NARROWED 2026-08-14, RESTRICTION CONFIRMED 2026-09-21

The original 22 June 2026 report listed ten potential abuse paths against the hardcoded, unrotated Firebase client API key (AIzaSy...bLZA, project diagnosia-android), reasoning from the presence of the Firebase SDK generally. On 14 August 2026, RFI-IRFOS re-pulled the then-current build (v7.0.3) and withdrew eight of the ten paths, Firestore, Storage, Authentication, Cloud Functions, and Remote Config abuse, because none of those Firebase SDKs are actually present in the binary; the key can only reach the services actually bundled. Two paths remained open on narrower grounds: FCM token enumeration (structural, never demonstrated as a working exploit) and the complete absence of Firebase App Check anywhere in the app (a real, confirmed architectural fact, not itself a demonstrated exploit path). On 21 September 2026, the operator supplied, and RFI-IRFOS independently verified against the live binary, a genuine server-side Application and API restriction on the key: bound to the Diagnosia package name and SHA-1 certificate fingerprint, limited to the FCM Registration, Firebase Cloud Messaging, and Firebase Installations APIs. That restriction closes the key-theft/reuse-elsewhere risk this finding originally raised. The narrower FCM-enumeration and App Check observations remain, documented as residual, undemonstrated structural risk. They did not block this report's closure, see Residual Risk & Recommendations.

Impact Analysis

The population affected by the confirmed, now-remediated C1 finding is Diagnosia's actual user base: physicians and pharmacists using the app at the point of care. Before the 21 September 2026 fix, every install generated an FCM registration token and an initial analytics event on first launch, before the user had made any choice, timestamped to the moment of app installation on a professional device that, in many clinical settings, is used by more than one staff member. No evidence was found, at any point in this engagement, that the drug-search queries themselves, medication names, dosage lookups, or interaction checks, were transmitted through either SDK; that specific claim was investigated and never confirmed.

The two withdrawn findings, taken together, illustrate the actual risk of overreaching a code-level observation into a data-flow claim without direct evidence, exactly the standard RFI-IRFOS applied against its own C1 headline on 21 September 2026.

The Complete Chain

A healthcare professional installs Diagnosia to check a drug interaction or dosage in a clinical context. Before any consent screen can render, Android's ContentProvider contract guarantees that FirebaseInitProvider and Sentry's providers run, and through v7.1.1, that unconditional initialization generated an FCM registration token and fired an initial analytics event, sending device- and installation-level identifiers to Google and Sentry before the professional had made any privacy choice. The app's hardcoded Firebase key carried no externally verifiable restriction at that point, and Firebase App Check was absent entirely, meaning the structural precondition for token-enumeration abuse existed, though RFI-IRFOS never demonstrated it as a working exploit.

Two parallel threads, a suspected Meta SDK and a suspected search-history backup leak, would have extended that chain into the content of a clinical search itself; both were investigated and found not to exist as claimed, closing that branch of the chain without ever needing the operator's cooperation to disprove them. The remaining branch, the SDK-initialization timing, was real, confirmed, and, as of 21 September 2026, remediated at the exact point that mattered: the automatic token-generation and analytics-collection steps are now gated behind consent. What is left standing, structural FCM-enumeration risk without App Check, the Cloud Act question for a US-owned SDK vendor, and the Article 9 status of a professional drug search, are documented risk observations that were never walked the rest of the way to a demonstrated, reproducible harm against the current build, which is precisely the operator's own closing argument, and RFI-IRFOS accepted it as sound.

Data Protection, Article by Article

Every GDPR article engaged over the life of this case, and its final status as of closure, is listed below, article by article. Each row stands on its own, not bundled into a single paragraph.

Article	Engagement	Status
Art. 6(1) / Art. 7	Lawful basis and consent for the pre-consent Firebase/Sentry initialization	Remediated 2026-09-21, auto-registration and auto-analytics now consent-gated
Art. 9	Whether a professional drug-interaction search implies the treated patient's health status	Precised 2026-08-15 to require actual personal reference; remains RFI-IRFOS's documented interpretive position, not a demonstrated data-flow finding
Art. 32(1)	Security of processing, hardcoded and unrotated Firebase client key	Application/API restriction independently confirmed 2026-09-21; key itself remains unrotated since the original June 2026 audit, both sides treat this descriptively, not as an active vulnerability
Art. 44–49	Third-country transfer via US-headquartered Firebase/Sentry	Raised 2026-08-15 with a US CLOUD Act argument. The operator disputes this as a general legal question, not a finding against the current build. Documented here as an open regulatory observation

Regulatory & Legal Landscape

18 U.S.C. § 2713 (the US CLOUD Act) obliges US-headquartered providers to produce data in their possession, custody, or control on request, independent of where that data is physically stored. The EDPB and EDPS jointly found in 2019 that CLOUD Act access without a qualifying international agreement is in tension with Art. 48 GDPR. The EU-US Data Privacy Framework remains formally in force, but its structural basis has been under scrutiny since the 29 June 2026 Trump v. Slaughter ruling affecting FTC independence; EDPB chair Anu Talus formally asked the European Commission on 31 July 2026 to assess the impact on the DPF's foundation, a response is still pending as of this report. RFI-IRFOS raised this as a general third-country-transfer consideration applicable to any pre-consent initialization of a US-owned SDK. The operator's position is that this is a legal question distinct from a concrete technical finding against Diagnosia specifically. That position is recorded here as the operator's own, not adjudicated by RFI-IRFOS.

Indicators of Compromise / Reproducible Evidence

Item	Value
Package	com.diagnosia.fachinformation
Original audited build	v7.0.3
Final verified build	v7.1.2, versionCode 7120
FirebaseInitProvider	com.google.firebase.provider.FirebaseInitProvider, initOrder=100
Sentry providers	io.sentry.android.core.SentryInitProvider, io.sentry.android.core.SentryPerformanceProvider
Remediation flags, confirmed live 2026-09-21	firebase_messaging_auto_init_enabled=false, firebase_analytics_collection_enabled=false (v7.1.2); io.sentry.auto-init=false (v7.1.1)
Firebase key restriction, confirmed live 2026-09-21	Application restriction: Android apps, package name + SHA-1 binding; API restriction: FCM Registration API, Firebase Cloud Messaging API, Firebase Installations API

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent (initial delivery bounced on a second, separate address; redelivered same day)
2026-06-25	Formal acknowledgment of receipt
2026-08-06	Dedicated compliance function (Leitner) takes over the case
2026-08-13	Operator's first substantive reply; H3 (Facebook/Meta) withdrawn by RFI-IRFOS the same day
2026-08-14	RFI-IRFOS pulls v7.0.3 fresh; C2 (backup) withdrawn in full; H2 narrowed from ten to two abuse paths
2026-08-15	RFI-IRFOS's full position on the operator's six points; entity correction accepted; C1, FCM-enumeration, App Check, and Cloud Act positions maintained
2026-08-31	Routine no-pressure follow-up, no substantive movement
2026-09-16	Operator requests closure; RFI-IRFOS's own fresh pull of v7.1.1 finds an unannounced `io.sentry.auto-init=false` fix; three explicit closure conditions set
2026-09-21	Operator supplies all three: key-restriction screenshots, v7.1.2 auto-init flags, Sentry-flag intent confirmed
2026-09-21/22	RFI-IRFOS independently verifies all three against a fresh v7.1.2 pull; corrects its own "confirmed tracking" overreach; applies the long-pending entity correction
2026-09-22	Operator distinguishes the three met closure conditions from broader, undemonstrated structural observations; RFI-IRFOS accepts the distinction and closes DIAGNOSIA-R1, one day ahead of the original embargo

Residual Risk & Recommendations

- Integrate Firebase App Check for any Firebase surface reachable from the client, including FCM, to close the structural FCM-token-enumeration gap even though it was never demonstrated as an active exploit.
- Consider rotating the Firebase client API key as routine hygiene; both parties agree the current, unrotated key is not itself a demonstrated vulnerability given the confirmed server-side restriction.
- Revisit the US CLOUD Act / third-country transfer question as EDPB guidance on the EU-US Data Privacy Framework's post-Trump v. Slaughter footing develops.
- RFI-IRFOS will re-pull and re-verify the current production build at any point in the future without further notice, standard practice for every case in this programme; a silent regression on any of the three remediated flags would be treated as a fresh finding, not a reopening of this closed case.

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 Severity scored per CVSS v4.0 where a finding was confirmed and reproducible; structural or undemonstrated observations are documented without a CVSS score, per RFI-IRFOS's own scoring discipline. RFI-IRFOS reserves the right to weigh real-world blast radius above the bare CVSS score where warranted; no such escalation applied in this report. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF DIAGNOSIA-R1.