Coordinated Privacy Disclosure, Final Report

Raisin Android (com.raisin.app)

Raisin SE, Berlin, Germany, savings deposit marketplace

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, TEN MESSAGES, ZERO REPLY OF ANY KIND

Target	Raisin, a European savings and deposit marketplace
Package	com.raisin.app, version 5.41.3, versionCode 835
Operator	Raisin SE, Berlin, Germany
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Berliner Beauftragte für Datenschutz und Informationsfreiheit (lead SA), Austrian DSB, CERT.at, EDPS, Berlin's mailbox@datenschutz-berlin.de
Total Outbound Messages	10, across 79 days, all delivered to datenschutz@raisin.com and security@raisin.com.
Inbound Replies	0. No reply, automated or human, was ever received.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 4

2 Subject & Operator Analysis 5

3 Ten Messages, Zero Reply 6

4 Findings 6
- 4.1 C1: Four SDKs Auto-Initialize Before the Consent Screen . . . 6
- 4.2 H1: Fully Extractable Firebase Project Configuration . . . 7
- 4.3 H2: Facebook SDK Embedded in a Deposit and Savings App . . . 7
- 4.4 M1: Permission Footprint Exceeds a Savings Marketplace . . . 8
- 4.5 M2: No Certificate Pinning in the Network Security Configuration . . . 8

5 Data Protection, Article by Article 9

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Raisin SE that its Android savings-deposit app registers four separate ContentProviders, Adjust (attribution), Exponea/Bloomreach (a behavioral customer data platform, not crash-reporting plumbing), Datadog RUM, and Firebase, all of which auto-initialize at process start, before any Activity, before any consent UI, before the user has agreed to anything. On an application that brokers deposits and processes identity-verification data, a behavioral profiling platform beginning to process user data before consent is a direct Art. 6(1) and Art. 7 lawful-basis question, not a cosmetic finding.

A second finding names Raisin's fully extractable Firebase configuration, project ID, app ID, and three separate API keys all hardcoded in the production binary. RFI-IRFOS explicitly declined to probe the associated Firebase Realtime Database, since doing so would exceed its authorization, and instead names the burden of proof: Raisin has to demonstrate key restriction by package and certificate, enforced Firebase App Check, and deny-by-default security rules, none of which is visible from the outside. A third finding names the Facebook SDK embedded in a deposit-marketplace app, an event-data flow to a US third party with transparency and Art. 44 transfer implications.

Two further findings round out the disclosure: a permission footprint, microphone, fine location, high-sampling-rate motion sensors, INSTALL_PACKAGES, and all-files access, that exceeds what a savings marketplace's documented functionality requires, though camera and NFC are correctly attributed to the app's KYC stack; and the absence of certificate pinning at the network-security-config layer, worth a deliberate decision for a financial app, not a silent default. Genuine positives are worth naming: the app's cleartext policy is correctly scoped to the emulator only, its KYC is handled by established providers (IDnow, Fourthline, Postident), not a home-rolled system, and it targets a current Android SDK.

Ten messages were sent across 79 days, all delivered to datenschutz@raisin.com and security@raisin.com, cc'ing the Berlin data protection authority (lead supervisory authority for Raisin's Berlin establishment), the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the initial disclosure, 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 Raisin Android application (com.raisin.app, version 5.41.3, versionCode 835, SHA-256 3d66c0db30c99835a60b961069644f154a785d9711cccabc327287592aafbdd0), pulled from a production device and reviewed on 25 June 2026. No account was created and no interaction with Raisin's, Adjust's, Exponea's, Datadog's, Firebase's, or Meta's backend infrastructure was performed, including the Firebase Realtime Database named in the findings below.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All five correct to MEDIUM or LOW on their own computed bands. Four SDKs (Adjust, Exponea, Datadog, Firebase) auto-initialize via ContentProvider before any consent screen; a fully extractable Firebase project configuration; the Facebook SDK embedded in a deposit marketplace with third-country transfer implications; and the absence of certificate pinning in the network security configuration all correct to MEDIUM. A broad permission footprint exceeding what a savings marketplace requires corrects to LOW. Ten messages were sent across 79 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Four SDKs Auto-Initialize Before the Consent Screen
H1	MEDIUM	Fully Extractable Firebase Project Configuration
H2	MEDIUM	Facebook SDK Embedded in a Deposit and Savings App
M1	LOW	Permission Footprint Exceeds a Savings Marketplace
M2	MEDIUM	No Certificate Pinning in the Network Security Configuration

Subject & Operator Analysis

Raisin SE is a savings and deposit marketplace established in Berlin, Germany, making the Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) the lead supervisory authority, with BaFin as the financial regulator in the background.

Genuine positives are worth naming. Cleartext traffic is correctly scoped to the emulator loopback only, not production, more disciplined than most apps in this audit series. KYC is handled by established providers (IDnow, Fourthline, Postident), not a home-rolled system. The app targets a current Android SDK (36). Every finding in this report is a configuration and consent-sequencing problem, fixable without re-architecting the app.

Ten Messages, Zero Reply

All ten messages in this case's correspondence record were delivered successfully to daten schutz@raisin.com and security@raisin.com across 79 days, cc'ing Berlin's data protection authority, the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Four SDKs Auto-Initialize Before the Consent Screen

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.

Four tracking and profiling SDKs each register an Android ContentProvider in the manifest: com.adjust.sdk.SystemLifecycleContentProvider (attribution), com.exponea.sdk.services.ExponeaContextProvider (a behavioral customer data platform, not crash-reporting plumbing), com.datadog.android.rum.DdRumContentProvider (real-user monitoring), and com.google.firebase.provider.FirebaseInitProvider. Android auto-initializes all registered ContentProviders during Application.onCreate(), before the first Activity and before any consent UI.

```
com.adjust.sdk.SystemLifecycleContentProvider
com.exponea.sdk.services.ExponeaContextProvider
com.datadog.android.rum.DdRumContentProvider
com.google.firebase.provider.FirebaseInitProvider
```

Impact: On an application that brokers deposits and processes identity-verification data, a behavioral customer data platform and an attribution SDK beginning to process user data before consent implicates the lawful-basis and consent requirements of Art. 6(1) and Art. 7 directly.

Fix: Gate all four ContentProviders' initialization behind an app-native consent flow. No confirmation that this has occurred was ever received.

H1: Fully Extractable Firebase Project Configuration

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

The complete Firebase project configuration, project ID, app ID, and three separate API keys, is hardcoded in res/values/strings.xml and extractable with apktool in under a minute. RFI-IRFOS did not probe the associated Realtime Database, as doing so would exceed its authorization.

```
project_id: raisin-1d5bb
google_api_key: AIzaSyBXHDlDMNoaAt-HfZs8k-NFAh7zCJUQVf4 (+2 further keys)
realtime db: https://raisin-1d5bb.firebaseio.com
```

Impact: An extractable key is only safe if the project is fully locked down, and that has to be demonstrated, not assumed: it can drive quota-exhaustion denial of service, and if security rules are not deny-by-default, it grants direct read or write access without enforced App Check.

Fix: Restrict all keys by package name and certificate fingerprint, enforce Firebase App Check, and confirm deny-by-default security rules. No confirmation that this has occurred was ever received.

H2: Facebook SDK Embedded in a Deposit and Savings 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.

The Facebook SDK is present in the binary, alongside Sentry and Datadog RUM as additional monitoring infrastructure. Meta Platforms is an independent third party and a US recipient; event data from an app that manages people's savings flowing to Meta is a transparency and international-transfer question.

Impact: Event data from a financial savings-deposit app reaching a US third party raises both transparency (Art. 13(1)(e)) and third-country transfer (Art. 44) questions, neither addressed in the reply record.

Fix: Document the Facebook SDK's specific purpose, its default auto-logging behavior, and the Art. 44 transfer mechanism covering it. No confirmation that this has occurred was ever received.

M1: Permission Footprint Exceeds a Savings Marketplace

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.

RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, HIGH_SAMPLING_RATE_SENSORS, INSTALL_PACKAGES, MANAGE_ALL_FILES_ACCESS_PERMISSION, and READ_PHONE_STATE are all declared. Camera and NFC are correctly attributable to the app's KYC stack (IDnow, Fourthline, Postident); the remaining permissions are not self-explanatory for a deposit marketplace.

Impact: Microphone, precise location, high-rate motion sensors, install privileges, and all-files access together exceed what a documented deposit-marketplace feature set requires under Art. 5(1)(c) data minimisation.

Fix: Document a specific purpose for each of the named permissions, or remove those without one. No confirmation that this has occurred was ever received.

M2: No Certificate Pinning in the Network Security Configuration

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3.

No pin-set is present in network_security_config.xml. Cleartext traffic is correctly restricted to the emulator loopback only (10.0.2.2/localhost), a genuinely disciplined default, but no certificate pinning is present at the network-security-config layer for production traffic.

Impact: For a financial application, the absence of certificate pinning is a decision worth making deliberately, since it removes a layer of defense against certificate-authority compromise or interception.

Fix: Add a pin-set for production API domains, or document a specific reason pinning is not used. 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. 6(1), Art. 7, Art. 5(1)(a)	C1	Pre-consent initialization of four tracking and profiling SDKs.
Art. 32	H1	Fully extractable Firebase project configuration and API keys.
Art. 13(1)(e), Art. 44	H2	Facebook SDK embedded with US third-country transfer implications.
Art. 5(1)(c)	M1	Permission footprint exceeding a savings marketplace's needs.
Art. 32	M2	No certificate pinning in the network security configuration.

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. In this report, C1, H1, H2, and M2 correct to MEDIUM on their own computed bands. M1 corrects to LOW. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: RAISIN-R1.