



Security & Privacy Disclosure, Final Report

LAOLA1 Android (at.laola1)

A lean sport-streaming client with a clean transport posture and one start-up sequencing problem, ten messages over 72 days drew no reply of any kind, and none of the three questions on record was ever answered

PUBLIC DISCLOSURE, 17 OCTOBER 2026 - EMBARGO REACHED 29 SEPTEMBER 2026, TEN MESSAGES SENT, ZERO REPLIES, THREE QUESTIONS NEVER ANSWERED

Target	LAOLA1 Multimedia GmbH, Austria. Operator inferred from first-party endpoints; privacy contact datenschutz@laola1.at
Package	at.laola1 v4.8.0 (versionCode 1778685646)
Platform Audited	Android, static analysis of the production APK
Initial Disclosure (R1)	2026-07-01, to datenschutz@laola1.at with the Austrian Datenschutzbehörde and EDPS as direct co-recipients
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (1 High, 2 Medium, 2 Low, 0 Critical)
Correspondence	10 messages sent by RFI-IRFOS over 72 days (2026-07-01 to 2026-09-11), 0 replies received, 0 bounces, 0 of 3 questions answered
Authorities Notified	Austrian Datenschutzbehörde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)
SHA-256 (base APK)	84f73f468fed79b1f7b6347d11b1e8755ae2f2bcc543368a119e05618cc3e81a

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	H1: Reach measurement, push and content SDKs initialise at process start, before the TRUENDO consent dialog	6
4.2	M1: Extractable Google/Firebase API key	6
4.3	M2: allowBackup is true with an unscoped cloud-backup rule while OpenID AppAuth stores login state	7
4.4	L1: Staging API endpoint compiled into the production build	7
4.5	L2: Test instrumentation activities exported in the release manifest	7
5	Impact Analysis	8
6	The Complete Chain: Ten Messages, 72 Days, Zero Replies	8
7	Data Protection – Article by Article	8
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	9
11	Residual Risk & Recommendations	10

Executive Summary

LAOLA1 is a comparatively lean sport-streaming and news client. Static analysis of production APK v4.8.0 (base.apk sha-256 84f73f46...e81a) found one HIGH, two MEDIUM and two LOW findings, and no CRITICAL finding. The HIGH finding is a sequencing problem: INFOonline reach measurement, CleverPush push and the Blaze content SDK initialise at process start, before the TRUENDO consent dialog can be answered.

The remaining items are an extractable Google/Firebase API key, allowBackup set to true with an unscoped cloud-backup rule while OpenID AppAuth stores login state, a staging endpoint in the production build and exported test activities.

The original disclosure opened with what the app gets right, and that list is long: an Austrian IAB-TCF consent platform (TRUENDO), no gambling or betting SDK, no Chinese or Russian SDK, no cleartext configuration on a targetSdk that denies it by default, Pairip integrity protection and a small SDK footprint with no AppsFlyer, Adjust or Taboola.

RFI-IRFOS sent the disclosure on 1 July 2026 and nine follow-ups through 11 September 2026. No reply of any kind arrived in 72 days, and the embargo of 29 September 2026 passed unanswered. This report publishes 18 days after the embargo with the full record intact.

ID	Severity	Title
H1	HIGH	Reach measurement, push and content SDKs initialise at process start, before the TRUENDO consent dialog
M1	MEDIUM	Extractable Google/Firebase API key
M2	MEDIUM	allowBackup is true with an unscoped cloud-backup rule while OpenID AppAuth stores login state
L1	LOW	Staging API endpoint compiled into the production build
L2	LOW	Test instrumentation activities exported in the release manifest

Subject & Operator Context

RFI-IRFOS identified LAOLA1 Multimedia GmbH, Austria, as the operator of at.laola1, inferred from the first-party endpoints api.laola1.at, matchcenter.laola1.at and images.laola1.at. The binary exposes only Datenschutz UI strings and no privacy contact, so the disclosure went to datenschutz@laola1.at. The lead supervisory authority is the Austrian Datenschutzbehörde, which was also notified directly.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 1 July 2026 to datenschutz@laola1.at, with the Austrian Datenschutzbehörde and the EDPS as direct co-recipients, stating an embargo date of 29 September 2026. The letter led with the app's strengths, then presented the HIGH sequencing finding and the medium and low notes, and asked three questions: which Art. 6 basis supports INFOnline, CleverPush and Blaze processing that starts before the TRUENDO dialog; whether a data protection impact assessment under Art. 35 exists and a data protection officer is appointed; and why the backup rules exclude nothing for the login data stored through OpenID AppAuth.

Nine follow-ups were sent (6 July, 17 July, 23 July, 31 July, 9 August, 15 August, 24 August, 31 August and 11 September 2026). The Austrian Datenschutzbehörde and the EDPS stayed in visible CC on every follow-up except the one of 24 August. None of the ten messages drew a reply or a delivery failure.

Findings

H1: Reach measurement, push and content SDKs initialise at process start, before the TRUENDO consent dialog

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, 5.3 - process-start initialisation ahead of a WebView CMP

```
line 157      de.infonline.lib.iomb.core.IOLInitProvider (enabled)
lines 129-135 androidx.startup.InitializationProvider ->
      BlazeApplicationContentProviderInitializer
lines 142-156 CleverPush FCM listener, CleanupService, GeofenceBroadcastReceiver
line 182      com.google.firebase.provider.FirebaseInitProvider (initOrder=100)
CMP: assets/truendo.html (WebView, runs after process start)
```

Impact: The manifest declares de.infonline.lib.iomb.core.IOLInitProvider (enabled, no initOrder, so it fires at process start) and androidx.startup.InitializationProvider hosting the Blaze SDK initializer and WorkManagerInitializer. CleverPush services (FCM listener, clean-up service, geofence receiver) and FirebaseInitProvider (initOrder 100) also start at launch. The only consent mechanism found is the WebView CMP asset truendo.html, which cannot run before the process and its ContentProviders have started. INFOnline reach measurement, CleverPush push-token registration and Blaze content telemetry can therefore execute before the user answers the TRUENDO dialog. The declared AD_ID permission and the AdvertisingIdClient reference in dex put the advertising ID in the same sequencing question. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because the pattern applies to every installation of a mass-market Austrian sport streaming app and every launch, not to an edge-case code path.

M1: Extractable Google/Firebase API key

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - key restriction status is for the operator to document

```
res/values/ -> google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
      LAOLA1 in R1]
```

Impact: A Google/Firebase API key, a Firebase application ID and an OAuth client ID are embedded in the string resources. Such keys are not secret by design, but an unrestricted key enables quota and billing exhaustion against the underlying Google Cloud project. Showing that package-name and SHA-1 restrictions and a per-API allow-list are in place rests with the operator. The key value is withheld from this public report.

M2: allowBackup is true with an unscoped cloud-backup rule while OpenID AppAuth stores login state

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - credential material eligible for cloud backup

```
AndroidManifest.xml line 47: android:allowBackup="true"  
res/xml/data_extraction_rules.xml: <cloud-backup /> (no <exclude>)  
lines 110-136: net.openid.appauth.* (login)
```

Impact: The application sets android:allowBackup="true", and res/xml/data_extraction_rules.xml contains only a bare cloud-backup element with no exclude rules. The app uses OpenID AppAuth for login. OAuth tokens and session state written to app storage are eligible for Google cloud backup with no exclusion, so credentials may leave the device through the backup channel.

L1: Staging API endpoint compiled into the production build

LOW, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 2.3 - hygiene item

```
https://staging-api.laola1.at/uploads/...
```

Impact: A staging endpoint under staging-api.laola1.at is present in the dex strings next to the production api.laola1.at. It is a hygiene item that discloses internal infrastructure naming.

L2: Test instrumentation activities exported in the release manifest

LOW, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 2.3 - hygiene item

```
androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity (exported,  
LAUNCHER)  
...$EmptyActivity, ...$EmptyFloatingActivity
```

Impact: androidx.test.core.app.InstrumentationActivityInvoker BootstrapActivity, EmptyActivity and EmptyFloatingActivity are declared exported with a LAUNCHER category. Test scaffolding ships in the release artifact.

Impact Analysis

The findings are routine, fixable engineering and documentation gaps in an otherwise lean binary, not evidence of malicious design. What sets this case apart is the correspondence: ten messages over 72 days with both regulators in visible copy on nine of them, and no reply, not even an acknowledgment of receipt.

The Complete Chain: Ten Messages, 72 Days, Zero Replies

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings on 1 July 2026 to datenschutz@laola1.at, with the Austrian Datenschutzbehörde and the EDPS as direct co-recipients, stating an embargo of 29 September 2026.

Step 2 – Silence: follow-ups on 6 July, 17 July and 23 July (both regulators in CC) restate the findings and the three questions. No reply.

Step 3 – Silence continues: follow-ups on 31 July, 9 August, 15 August, 24 August, 31 August and 11 September 2026. No reply.

Step 4 – Embargo passes unanswered: 29 September 2026 passes with the correspondence completely unanswered and no delivery failure on record.

Step 5 – Publication: this report publishes 18 days after the embargo, with ten messages sent, zero replies received and zero of three questions answered.

Data Protection – Article by Article

Art. 6, Art. 7 and Art. 5(1)(a) GDPR – Lawfulness and consent: H1's process-start initialisation places reach measurement, push registration and content telemetry ahead of the TRUENDO decision.

Art. 32 GDPR – Security of processing: M1's unrestricted-key exposure and M2's unscoped cloud backup of login state.

Art. 25 GDPR – Privacy by design: M2, L1 and L2 reflect default configurations that were not narrowed for release.

Art. 35 GDPR – Impact assessment: the combination of reach measurement, push token, Blaze telemetry and advertising ID warrants a documented DPIA.

Regulatory & Legal Landscape

The Austrian Datenschutzbehörde is the lead supervisory authority for LAOLA1 Multimedia GmbH. Both it and the EDPS were direct co-recipients of the original disclosure and stayed in visible CC on every follow-up except the one of 24 August 2026.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 25 and Art. 32 issues in M1 and M2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 6 and Art. 7 issue in H1, up to EUR 20,000,000 or 4% of total worldwide annual turnover.

Indicators of Compromise

The following items were extracted from the published production APK via static analysis only. No LAOLA1 servers, accounts, or infrastructure were probed. The Google/Firebase API key referenced in M1 is withheld from this public report; the full value was disclosed privately to LAOLA1 in the original R1 letter.

```
H1 -- IOLInitProvider, androidx.startup (Blaze), CleverPush services,  
    FirebaseInitProvider at process start; CMP is assets/truendo.html  
M1 -- Google/Firebase API key in resources (redacted)  
M2 -- allowBackup=true, data_extraction_rules.xml without excludes  
L1 -- https://staging-api.laola1.at/uploads/...  
L2 -- exported androidx.test InstrumentationActivityInvoker activities
```

Disclosure Timeline & Outcome

2026-07-01 Initial disclosure sent to datenschutz@laola1.at with the Austrian Datenschutzbehörde and EDPS as direct co-recipients. Embargo stated as 2026-09-29.

2026-07-06 Follow-up sent. No reply.

2026-07-17 Follow-up sent. No reply.

2026-07-23 Follow-up sent, both regulators in CC. No reply.

2026-07-31 Follow-up sent. No reply.

2026-08-09 Follow-up sent, both regulators in CC. No reply.

2026-08-15 Follow-up sent. No reply.

2026-08-24 Follow-up sent without regulators in CC. No reply.

2026-08-31 Follow-up sent. No reply.

2026-09-11 Follow-up sent, 72 days since the original disclosure. No reply.

2026-09-29 Embargo date reached and passed with all three questions unanswered.

2026-10-17 This report published, 18 days after the embargo date. Correspondence record: ten RFI-IRFOS messages, zero replies, zero bounces, zero of three questions answered.

Residual Risk & Recommendations

H1 – Defer INFOnline, CleverPush, Blaze and Firebase initialisation until the TRUENDO decision is recorded, for example by disabling the auto-init providers and starting each SDK after consent.

M1 – Restrict the Google/Firebase API key to the production signing certificate and the APIs actually used, then rotate it.

M2 – Add exclude rules for the AppAuth token storage in data_extraction_rules.xml, or set allowBackup to false.

L1 and L2 – Remove the staging endpoint and the androidx.test activities from the release build.

Procedural: RFI-IRFOS remains open to a substantive reply to the three questions at any time; this report will be updated to reflect one if it arrives.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No LAOLA1 servers, accounts, or infrastructure were probed. The API key value is withheld from this public report and was disclosed privately to LAOLA1 in the original R1 letter. Analysis by RFI-IRFOS, ZVR 1015608684, GISA 39261441, Steuernummer 68 696/8736. REF LAOLA1-2026-R1-001.