



Security & Privacy Disclosure, Final Report

Krone Sport Android (at.kronesport)

An app-wide cleartext opt-in and a session-replay capability sit inside a political tabloid sport client, nine messages over 73 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, NINE MESSAGES SENT, ZERO REPLIES, THREE QUESTIONS NEVER ANSWERED

Target	Krone Multimedia GmbH & Co KG (Kronen-Zeitung group), Austria. Operator inferred from the self-hosted Sentry DSN; privacy contact datenschutz@krone.at
Package	at.kronesport v3.1.5 (versionCode 50527890), React Native
Platform Audited	Android, static analysis of the production APK
Initial Disclosure (R1)	2026-07-01, to datenschutz@krone.at, BCC Austrian Datenschutzbehoerde and EDPS
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (1 High, 3 Medium, 1 Low, 0 Critical)
Correspondence	9 messages sent by RFI-IRFOS over 73 days (2026-07-01 to 2026-09-12), 0 replies received, 0 bounces, 0 of 3 questions answered
Authorities Notified	Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)
SHA-256 (base APK)	fe0b8ac80962db997b62ded2f5ace3407fe48b26149cd31840b578bd6552b6a6

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: Application-wide cleartext traffic permitted without Network Security Config scoping	6
4.2	M1: Sentry session-replay (rrweb) capability shipped in the release binary . .	6
4.3	M2: Extractable Google/Firebase API key	7
4.4	M3: Reach measurement, advertising and push components initialise before the Didomi consent decision	7
4.5	L1: React Native dev support activity and CAMERA permission in the release artifact	8
5	Impact Analysis	8
6	The Complete Chain: Nine Messages, 73 Days, Zero Replies	8
7	Data Protection – Article by Article	9
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	10

Executive Summary

Krone Sport is a React Native sport client from the Kronen-Zeitung group. Static analysis of production APK v3.1.5 (base.apk sha-256 fe0b8ac8...6b6a6) found one HIGH finding, three MEDIUM findings and one LOW finding, and no CRITICAL finding. The HIGH finding is an application-wide android:usesCleartextTraffic="true" opt-in with no Network Security Config, on a targetSdk where plain HTTP is denied by default.

The binary also ships Sentry session-replay classes (self-hosted at sentry.krone.at, auto-init disabled), reach measurement and push components that start before the Didomi consent dialog can run, and an extractable Google/Firebase API key. Reading behaviour on a tabloid with substantial political coverage, combined with the advertising and reach stack, raises an Art. 9 question about inferred political opinions.

The app also does several things well and the original disclosure said so first: it ships a full IAB-TCF CMP (Didomi), keeps telemetry on a self-hosted Austrian endpoint, disables Facebook auto-init and advertiser-ID collection, sets allowBackup to false, keeps the OneSignal location module dormant (no location permission declared), and contains no Chinese or Russian SDK.

RFI-IRFOS sent the disclosure on 1 July 2026 and eight follow-ups through 12 September 2026. No reply of any kind, not even an acknowledgment of receipt, arrived in 73 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	Application-wide cleartext traffic permitted without Network Security Config scoping
M1	MEDIUM	Sentry session-replay (rrweb) capability shipped in the release binary
M2	MEDIUM	Extractable Google/Firebase API key
M3	MEDIUM	Reach measurement, advertising and push components initialise before the Didomi consent decision
L1	LOW	React Native dev support activity and CAMERA permission in the release artifact

Subject & Operator Context

RFI-IRFOS identified Krone Multimedia GmbH & Co KG, the Kronen-Zeitung group, as the operator of at.kronesport, inferred from the self-hosted Sentry DSN on sentry.krone.at and the deep-link schemes kronenativesport and atakronesport. The binary exposes no privacy contact, so the disclosure went to datenschutz@krone.at. The lead supervisory authority is the Austrian Datenschutzbehörde, which was also notified directly. Krone Sport is a tabloid sport product, and the publisher's political coverage makes the reading behaviour in this ecosystem more sensitive than in a pure sport app.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 1 July 2026 to datenschutz@krone.at, with the Austrian Datenschutzbehörde and the EDPS in BCC per standing practice, stating an embargo date of 29 September 2026. The letter led with what the app does well, then presented one HIGH finding and the medium notes, and asked three questions: why cleartext traffic is permitted application-wide on targetSdk 36; whether session replay is active in production, with which PII masking, and whether a lawful basis under Art. 9(2) exists for political-opinion inference; and whether a data protection impact assessment under Art. 35 exists and a data protection officer is appointed.

Eight follow-ups were sent (6 July, 17 July, 23 July, 31 July, 9 August, 15 August, 31 August and 12 September 2026). The Austrian Datenschutzbehörde moved into visible CC from 23 July and the EDPS from 9 August. None of the nine messages drew a reply or a delivery failure.

Findings

H1: Application-wide cleartext traffic permitted without Network Security Config scoping

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 - global opt-in to plaintext HTTP on targetSdk 36

```
application ... android:usesCleartextTraffic="true"
res/xml/network_security_config.xml: absent
targetSdk: 36 (platform default: cleartext denied)
```

Impact: The manifest sets `android:usesCleartextTraffic="true"` on the application element and no `network_security_config.xml` exists to restrict which domains may use plain HTTP. On targetSdk 36 the platform default is deny, so this is an explicit, global opt-in to plaintext transport. Any plaintext endpoint used by the app, its WebViews (RNCWebView) or its embedded SDKs is exposed to interception and injection on a hostile network. The practical weight is higher for this app than for a pure sport client, because reading behaviour in a political tabloid ecosystem is itself sensitive. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because the audience is the readership of Austria's largest tabloid, whose reading behaviour permits political-opinion inference (Art. 9), and the opt-in is global rather than scoped to one legacy endpoint.

M1: Sentry session-replay (rrweb) capability shipped in the release binary

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 - capability present, mitigated by disabled auto-init and self-hosting

```
dex: io/sentry/rrweb/* (RRWebEvent, RRWebVideoEvent, ...)
manifest line 143: io.sentry.auto-init = false
DSN: https://[REDACTED IN PUBLIC REPORT -- disclosed privately to Krone in R1]@sentry.
krone.at/18
```

Impact: The dex files contain `io.sentry.rrweb.*` classes (RRWebEvent, RRWebIncrementalSnapshotEvent, RRWebInteractionMoveEvent, RRWebVideoEvent) plus `io.sentry.react`. Session replay can record on-screen content and user interactions. The mitigations are real: `io.sentry.auto-init` is set to false and the DSN points at a self-hosted Sentry instance at `sentry.krone.at`, so any data stays with Krone in Austria. Whether replay is switched on in production and which PII masking applies is a documentation question for the operator, and it is one of the three questions on record.

M2: 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

```
dex/classes*.dex -> google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately  
to Krone in R1]
```

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

M3: Reach measurement, advertising and push components initialise before the Didomi consent decision

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 - start-up sequencing against a JavaScript-hosted CMP

```
line 196 de.infonline.lib.iomb.core.IOLInitProvider (enabled)  
line 235 com.google.android.gms.ads.MobileAdsInitProvider (initOrder=100)  
line 223 com.google.firebase.provider.FirebaseInitProvider (initOrder=100)  
lines 164-186 OneSignal FCMBroadcastReceiver, BootUpReceiver (BOOT_COMPLETED)  
CMP: Didomi, inside assets/index.android.bundle (__tcfapi)
```

Impact: INFOnline IOMB (IOLInitProvider, enabled, no initOrder), Google MobileAdsInitProvider (initOrder 100), FirebaseInitProvider (initOrder 100) and the OneSignal receivers, including BootUpReceiver on BOOT_COMPLETED, are declared in the manifest and start with the process. The Didomi CMP lives in the React Native JavaScript bundle and can only run after the RN runtime has started. INFOnline reach measurement and OneSignal registration can therefore execute before a consent decision, and BootUpReceiver allows OneSignal logic to run before the app is ever opened.

L1: React Native dev support activity and CAMERA permission in the release artifact

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

```
lines 7-8  CAMERA, FLASHLIGHT
line 89   com.facebook.react.devsupport.DevSettingsActivity
```

Impact: com.facebook.react.devsupport.DevSettingsActivity is declared in the release manifest. It is normally inert in release builds but ships. android.permission.CAMERA and FLASHLIGHT are declared with no obvious in-app capture flow beyond a WebView file provider. Both are hygiene items.

Impact Analysis

The findings are routine, fixable engineering and documentation gaps, not evidence of malicious design. What sets this case apart is the correspondence: nine messages over 73 days with a regulator in visible copy on five of the follow-ups, and no reply, not even an acknowledgment of receipt, from a company that runs a privacy contact mailbox.

The Complete Chain: Nine Messages, 73 Days, Zero Replies

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

Step 2 – Silence: follow-ups on 6 July, 17 July and 23 July (Datenschutzbehörde moved to visible CC) restate the findings and the three questions. No reply.

Step 3 – Silence continues: follow-ups on 31 July and 9 August (EDPS moved to visible CC), 15 August, 31 August and 12 September 2026. No reply.

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

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

Data Protection – Article by Article

Art. 32 and Art. 5(1)(f) GDPR – Security of processing: H1's global cleartext opt-in and M2's unrestricted-key exposure fall short of the measures these provisions require unless the operator documents otherwise.

Art. 6, Art. 7 and Art. 5(1)(a) GDPR – Lawfulness and consent: M3's start-up sequencing places reach measurement and push registration ahead of the Didomi decision.

Art. 9 GDPR – Special categories: reading behaviour in a political tabloid ecosystem can permit inference of political opinions, which requires an Art. 9(2) exception, typically explicit consent.

Art. 5(1)(c) and Art. 25 GDPR – Minimisation and privacy by design: M1's session-replay capability and L1's unused CAMERA permission.

Art. 35 GDPR – Impact assessment: a combination of reach measurement, advertising ID and push over political reading behaviour warrants a documented DPIA.

Regulatory & Legal Landscape

The Austrian Datenschutzbehörde is the lead supervisory authority for Krone Multimedia GmbH & Co KG. It was in BCC from the original disclosure and in visible CC from 23 July 2026. The EDPS was in BCC from the original disclosure and in visible CC from 9 August 2026.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 and Art. 25 issues in H1, M1 and M2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 6, 7 and 9 issues in M3 and the Art. 9 question, up to EUR 20,000,000 or 4% of total worldwide annual turnover. A sustained absence of any reply to a written disclosure with a supervisory authority in copy is itself a fact an authority may find relevant when assessing internal handling.

Indicators of Compromise

The following items were extracted from the published production APK via static analysis only. No Krone servers, accounts, or infrastructure were probed. The Google/Firebase API key and the Sentry DSN key referenced in M1 and M2 are withheld from this public report; full values were disclosed privately to Krone in the original R1 letter.

```
H1 -- usesCleartextTraffic="true" on application, manifest line 65, no NSC
M1 -- io.sentry.rrweb.* classes, DSN sentry.krone.at (key redacted)
M2 -- Google/Firebase API key in dex (redacted)
M3 -- IOLInitProvider, MobileAdsInitProvider, FirebaseInitProvider,
    OneSignal BootUpReceiver (BOOT_COMPLETED) before Didomi (JS bundle)
L1 -- DevSettingsActivity, CAMERA and FLASHLIGHT permissions
```

Disclosure Timeline & Outcome

2026-07-01 Initial disclosure sent to datenschutz@krone.at, BCC Austrian Datenschutzbehoerde and EDPS. 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, Austrian Datenschutzbehoerde moved to visible CC. No reply.

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

2026-08-09 Follow-up sent, EDPS moved to visible CC. No reply.

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

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

2026-09-12 Follow-up sent, 73 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: nine RFI-IRFOS messages, zero replies, zero bounces, zero of three questions answered.

Residual Risk & Recommendations

H1 – Remove usesCleartextTraffic="true" or scope cleartext to named legacy domains in a Network Security Config; move every endpoint to HTTPS.

M1 – Document whether session replay is enabled in production, the masking rules, and the Art. 9(2) basis where political-opinion inference is possible.

M2 – Restrict the Google/Firebase API key to the production signing certificate and the APIs actually used, then rotate it.

M3 – Defer INFFOnline, Ads, Firebase and OneSignal initialisation until the Didomi decision is recorded, and remove or gate the BOOT_COMPLETED receiver.

L1 – Strip DevSettingsActivity from release builds and remove unused CAMERA and FLASHLIGHT permissions.

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 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No Krone servers, accounts, or infrastructure were probed. Credential values are withheld from this public report and were disclosed privately to Krone in the original R1 letter. Analysis by RFI-IRFOS, ZVR 1015608684, GISA 39261441, Steuernummer 68 696/8736. REF KRONESPORT-2026-R1-001.