Coordinated Security & Privacy Disclosure, Final Report

OÖNachrichten for Android (de.fcms.webapp.oon)

Eight written notices, ninety days, two substantive named replies, one finding narrowed by genuine technical dialogue, two confirmed and in remediation, one unaddressed

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – GENUINE TECHNICAL ENGAGEMENT, THREE OF FOUR FINDINGS ACKNOWLEDGED

Target	Wimmer Medien GmbH & Co.KG (OÖ Nachrichten), A-4020 Linz, Promenade 23, Landesgericht Linz FN 166228d
Product audited	OÖNachrichten for Android, de.fcms.webapp.oon, v4.1.17 (versionCode 2400495), Flutter/Dart, Firebase project ooen-app
Disclosure reference	REF OONACHRICHTEN-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H1 no certificate pinning, CVSS v4.0 8.6, confirmed, partial mitigation planned; H2 allowBackup subscription-data exposure, CVSS v4.0 8.7, confirmed, fix planned)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production OÖNachrichten Android application and identified four findings: a hardcoded Firebase API key originally assessed as CRITICAL against fifteen concrete attack scenarios, a complete absence of Network Security Config or certificate pinning on any connection, allowBackup left enabled with no exclusion rules so Piano subscription credentials and read history sync unencrypted into a US third-country Google Cloud backup, and an undisclosed processor list (Piano, Chartbeat) alongside an ad-tech standard (MRAID.js) bundled inside a paid, subscription-gated app.

This case produced genuine, named, technically substantive engagement, rare across this disclosure wave. Alexander Wagner, Datenschutz / Online Technik at OÖ Nachrichten, replied on 30 June 2026 confirming the Network Security Config gap and the allowBackup finding as valid, reported the allowBackup matter proactively to the Austrian Datenschutzbehörde under Art. 33 GDPR as a precaution, and disputed the CRITICAL severity of the Firebase key finding on the grounds that Firebase client keys are by-design public identifiers, not secrets. On 25 August 2026, following an internal engineering review, Wagner reported that only Firebase Cloud Messaging is provisioned in the project, indirectly, via a single component, with Firebase Auth, Firestore, Realtime Database, Storage, and Remote Config all unused, and asked RFI-IRFOS to name any of its fifteen scenarios that survives without those products. RFI-IRFOS's own R3, sent the same day, conceded eight of fifteen scenarios no longer applied, formally withdrew a ninth as technically incorrect, and narrowed its remaining live concern to a single unverified quota-denial-of-service scenario against the Firebase Installations API underlying FCM.

Given that narrowing, this report labels the Firebase key finding DISPUTED rather than CRITICAL: OÖ Nachrichten's technical position, that no exploitable Firebase product beyond FCM is provisioned, was substantiated by an internal review RFI-IRFOS could not independently verify but also could not refute. The certificate-pinning and allowBackup findings remain confirmed by the target's own admission; OÖ Nachrichten declined classic certificate pinning as disproportionate for a non-banking news app and stated it will instead rely on a Network Security Config, Certificate Transparency, and an Android 16 trusted-certificate-source restriction under evaluation, while allowBackup=false was stated as planned for the near-term Build #498. The undisclosed-processor finding was corrected in the app's privacy policy shortly after RFI-IRFOS's inquiry. The MRAID.js finding was never addressed by either side. Six unresolved technical questions, on Firebase App Check, Security Rules configuration, Firebase Analytics usage, key rotation, whether Build #498 shipped, and whether a formal Art. 35 DPIA was completed for the Auto-Backup path, remain open as of the embargo date.

Scope: Static analysis of the publicly downloaded production OÖNachrichten Android APK (v4.1.17), on an authorized test device, only. No OÖ Nachrichten account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@nachrichten.at, bcc dsb@dsb.gv.at and cert@cert.at. Across eight written notices over ninety days, Alexander Wagner (Datenschutz / Online Technik) sent two detailed, named, technically substantive replies, 30 June and 25 August 2026, confirming two findings outright and mounting a reasoned, evidence-backed dispute of a third's severity. RFI-IRFOS's own R3 conceded most of the disputed scenarios and narrowed its remaining claim accordingly. One finding was never addressed by either side.

ID	Severity	Title
C1	DISPUTED	Hardcoded Firebase API key, severity narrowed by substantive technical dialogue
H1	HIGH	No Network Security Config, zero certificate pinning on any connection
H2	HIGH	allowBackup="true" with no exclusion rules, subscription data synced to Google Cloud
M1	MEDIUM	Undisclosed US processors, Piano and Chartbeat, corrected during disclosure
M2	MEDIUM	MRAID.js ad-tech standard bundled inside a paid subscription app

Subject & Operator Analysis

Wimmer Medien GmbH & Co.KG, trading as OÖ Nachrichten / Medienhaus Wimmer, is registered at Promenade 23, 4020 Linz, Austria (Landesgericht Linz, FN 166228d), with Wimmer Medien GmbH (FN 166226a) as Komplementär, under the direct jurisdiction of the Austrian Datenschutzbehörde.

Findings

C1: Hardcoded Firebase API key, severity narrowed by substantive technical dialogue

DISPUTED, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9 (narrowed from an original CRITICAL assessment)

google_api_key AIzaSyDGhlIBg3y8IQ7bh5szBm0MwrPGSjddiN0, project_id ooen-app, found in res/values/strings.xml. R1 originally presented fifteen concrete attack scenarios, quota-denial-of-service, subscriber enumeration, forged push notifications, and potential Firebase Security Rules exposure among them.

OÖ Nachrichten disputed CRITICAL severity on 30 June 2026, arguing the key is a client-side, by-design public identifier secured through Application Restrictions and Firebase Security Rules rather than through secrecy. Following an internal engineering review, Wagner reported on 25 August 2026 that only Firebase Cloud Messaging is provisioned, indirectly, via a single component, with Auth, Firestore, Realtime Database, Storage, and Remote Config all unused, and asked RFI-IRFOS to name any surviving scenario. RFI-IRFOS's own R3, sent the same day, conceded eight of fifteen scenarios no longer applied given that scope, formally withdrew a ninth (an FCM-HTTP phishing-blast scenario requiring a separate server key or OAuth token, not the client key found) as technically incorrect, and narrowed its remaining live concern to one unverified scenario: quota-exhaustion denial-of-service against the Firebase Installations API that underlies FCM. Whether Firebase App Check is enabled, whether Security Rules are exported as deny-by-default proof, and whether Firebase Analytics is separately active were asked on 25 August and remain unanswered.

Impact: The originally-asserted broad attack surface (subscriber enumeration, forged push, Security Rules exposure across five Firebase products) does not survive OÖ Nachrichten's confirmed single-product scope. A narrower, unverified quota-denial-of-service exposure against FCM's underlying Installations API remains an open question pending App Check confirmation.

Fix: Confirm whether Firebase App Check is enabled for the FCM-only project, and publish a Security Rules export or equivalent proof of deny-by-default configuration.

H1: No Network Security Config, zero certificate pinning on any connection

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

No android:networkSecurityConfig in the manifest, no NSC file present. Piano subscription API traffic, article content, and login credentials are protected only by Android platform TLS defaults.

OÖ Nachrichten confirmed this finding as valid on 30 June 2026 without dispute, but explicitly declined classic certificate pinning as disproportionate for a non-banking news application, stating it will instead rely on a new Network Security Config, Certificate Transparency, and an Android 16 trusted-certificate-source restriction feature under evaluation. As of 4 September 2026, RFI-IRFOS had received no confirmation that any of these mitigations had shipped.

Impact: On an adjacent, attacker-controlled network (open Wi-Fi, ARP spoofing), an attacker can intercept and manipulate Piano subscription-authentication traffic and delivered article content without triggering a pinning failure.

Fix: Ship the planned Network Security Config restricting trust to a defined certificate set, and confirm the timeline for the Android 16 trusted-certificate-source restriction.

H2: allowBackup="true" with no exclusion rules, subscription data synced to Google Cloud

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

android:allowBackup="true" with no android:dataExtractionRules and no android:fullBackupContent. All app data, Piano subscription status and credentials, article read history, offline cache, and Sentry crash dumps, defaults into the user's Google Cloud backup, a US third-country processor not named as such in the app's privacy policy at disclosure time.

OÖ Nachrichten confirmed this finding as valid on 30 June 2026, stated allowBackup will be set to false in the planned Build #498, and disclosed that it had proactively documented the matter internally and reported it to the Austrian Datenschutzbehörde under Art. 33 GDPR as a precaution. OÖ Nachrichten disputes sole legal responsibility, arguing Android Auto-Backup is a user- and OS-controlled mechanism rather than a Google processing relationship it directly enters into. As of 4 September 2026, RFI-IRFOS had received no confirmation that Build #498 had shipped or that a formal Art. 35 DPIA had been completed for this processing path.

Impact: Piano subscription credentials and full app state are transferred to a US third-country processor via a default OS mechanism the app never opted out of, without a matching Art. 13(1)(f) transfer disclosure at the time of finding.

Fix: Ship Build #498 with allowBackup set to false or a data-extraction-rules exclusion list covering subscription credentials and cached personal data, and complete a documented Art. 35 assessment of the Auto-Backup path.

M1: Undisclosed US processors, Piano and Chartbeat, corrected during disclosure

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

Piano Software s.r.o./Inc. (526 smali references) and Chartbeat Inc., New York (53 smali references) both require Art. 46 GDPR standard contractual clauses and explicit naming in the app's privacy policy.

OÖ Nachrichten stated on 30 June 2026 that Piano processing rests on consent-banner consent under Art. 6(1)(a) and that Piano is named there, but conceded the separate app privacy policy had incorrectly omitted the full processor list, and stated this was corrected promptly following RFI-IRFOS's inquiry.

Impact: Resolved during the disclosure window; documented here for the public record and as a data point on the target's responsiveness to concrete, evidenced findings.

Fix: Confirmed corrected by the target; no further action required beyond periodic re-verification.

M2: MRAID.js ad-tech standard bundled inside a paid subscription app

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

A 27KB IAB Mobile Rich Media Ad Standard JavaScript asset is present inside the Piano-paywalled subscription app.

If MRAID infrastructure remains active for paying subscribers, this exceeds the stated purpose of a subscription product under Art. 5(1)(c) and Art. 6(1). This finding was never addressed in either of OÖ Nachrichten's two substantive replies.

Impact: Paying subscribers may retain ad-tech attack surface and ad-mediation data flows their subscription is meant to remove.

Fix: Confirm whether MRAID-capable ad infrastructure is active for authenticated Piano subscribers, and strip it from the subscriber code path if so.

A Rare Case: Genuine, Named, Technical Engagement

Of over two hundred companies contacted across this disclosure campaign, the large majority never reply at all. OÖ Nachrichten is one of a small number of cases to produce detailed, named, technically substantive engagement: two full replies from Alexander Wagner, Datenschutz / Online Technik, each addressing specific findings on their technical merits, confirming two outright, disputing a third with evidence rather than dismissal, and proactively self-reporting one matter to the Austrian Datenschutzbehörde under Art. 33 without being asked to. RFI-IRFOS's own follow-ups were not error-free in return: the 24 July and 9 August messages mistakenly repeated already-resolved H1/H2 language instead of the still-open C1 questions from the 30 June reply, an error RFI-IRFOS acknowledged and corrected in its 25 August R3. Documented here for transparency, since accuracy in a disclosure record cuts both ways.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Firebase key exposure, severity narrowed by confirmed single-product scope; App Check status unconfirmed
H1	GDPR Art. 32(1)(a)	No certificate pinning or Network Security Config, confirmed, mitigation planned
H2	GDPR Art. 13(1)(f), Art. 44, Art. 35	Subscription data synced to US Google Cloud backup, confirmed, fix planned, self-reported under Art. 33
M1	GDPR Art. 13(1)(e), Art. 46	Undisclosed processors, corrected during disclosure
M2	GDPR Art. 5(1)(c), Art. 6(1)	Ad-tech standard inside paid subscription app, unaddressed

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@nachrichten.at (bcc dsb@dsb.gv.at, cert@cert.at); C1 (originally CRITICAL), H1, H2 disclosed; embargo stated as 2026-09-19
2026-06-28	Follow-up restating C1/H1/H2 as a table, seven days, no reply yet
2026-06-30	Wagner replies: H1 and H2 confirmed valid, allowBackup fix planned for Build #498, Art. 33 self-report to DSB disclosed; C1 severity disputed
2026-06-30	RFI-IRFOS sends R2 same day, fifteen concrete C1 attack scenarios, public ledger reference for H1/H2
2026-06-30	Attempted regulator bcc to post@dsb.gv.at bounces, 'User unknown', wrong DSB address
2026-07-24	Follow-up, DSB added to visible cc from this message onward
2026-08-09	Follow-up, forty days since last reply
2026-08-15	Follow-up, fifty-five days since disclosure, twenty-three since last reply
2026-08-25	Wagner replies again: internal review confirms FCM-only Firebase usage, no Auth/Firestore/RTDB/Storage/Remote Config; asks RFI-IRFOS to name any surviving scenario
2026-08-25	RFI-IRFOS sends R3 same day, concedes eight of fifteen C1 scenarios, formally withdraws one, narrows remaining claim to a quota-DoS scenario, corrects its own prior tracking error
2026-09-04	Further follow-up sent (asks about key rotation and Build #498 status; restates weekly SHA-256 archival and the 2026-09-19 embargo date)
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Confirm Firebase App Check status and publish a Security Rules export for the FCM-only project, closing the last open question on the narrowed C1 finding.
- Ship the planned Network Security Config and confirm the Android 16 trusted-certificate-source restriction timeline.
- Confirm Build #498 shipped with allowBackup=false or an equivalent data-extraction-rules exclusion, and complete a documented Art. 35 assessment of the Auto-Backup path.
- Confirm whether MRAID-capable ad infrastructure remains active for authenticated Piano subscribers.

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 Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 9, 13, 25, 32, 33, 35, 44, 46. REF OONACHRICHTEN-2026-R1.