Koordinierte Offenlegung, Abschlussbericht

DER STANDARD Android (derstandard.at.istandardx)

STANDARD Verlagsgesellschaft m.b.H., Wien, Österreich

STILLE · FALL GESCHLOSSEN UND VERÖFFENTLICHT AM 25. SEPTEMBER 2026, AM ANGEGEBENEN EMBARGO-DATUM, SECHS NACHRICHTEN, KEINE INHALTLICHE ANTWORT

Ziel	DER STANDARD, eine der größten österreichischen Tageszeitungen
Package	derstandard.at.istandardx, Version 7.0.24.127275
Betreiber	STANDARD Verlagsgesellschaft m.b.H., Wien, Österreich
Erstmeldung	2026-06-27
Angegebenes Embargo	2026-09-25, dem Betreiber direkt in der Erstmeldung mitgeteilt
Bericht veröffentlicht	2026-09-25, zum angegebenen Datum
Behörden	Österreichische Datenschutzbehörde (DSB), CERT.at
Ausgehende Nachrichten gesamt	6 über 78 Tage, an redaktion@derstandard.at und datenschutz@derstandard.at; zwei automatische Empfangsbestätigungen der Redaktion, nie vom Datenschutz.
Eingehende Antworten	0 inhaltliche Antworten. Zwei automatische Weiterleitungsbestätigungen von redaktion@derstandard.at, keine einzige von datenschutz@derstandard.at.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Am 27. Juni 2026 meldete RFI-IRFOS, dass die Android-App von DER STANDARD einen Firebase-API-Key hardcodiert im Play-Store-Binary enthält, extrahierbar von jedem, der die APK herunterlädt. Dies korrigiert sich auf MEDIUM/6.9 unter CVSS v4.0.

Ein zweiter Befund: drei ContentProvider, FirebaseInitProvider, SentryInitProvider und SentryPerformanceProvider, initialisieren automatisch beim App-Start, vor dem Consent-Dialog. Firebase und Sentry sammeln Daten, bevor der Nutzer irgendetwas eingewilligt hat, ein direkter Verstoß gegen das Erfordernis, dass Einwilligung der Verarbeitung vorausgehen muss. Auch dieser Befund korrigiert sich auf MEDIUM.

Zwei weitere Befunde runden das Bild ab. Das CleverPush-SDK, 477 Smali-Klassen, leitet Nutzerdaten über api.cleverpush.com, ohne dass aus dem Binary ein Art.-28-Auftragsverarbeitungsvertrag nachweisbar ist. Und die App deklariert ACCESS_ADSERVICES_AD_ID sowie ACCESS_ADSERVICES_ATTRIBUTION, Werbe-ID-Tracking in einer Nachrichtenanwendung, aus deren Leseverhalten sich politische Meinungen ableiten lassen, was eine explizite Rechtsgrundlage nach Art. 9 DSGVO erfordert und für die keine gefunden wurde. Beide Befunde korrigieren sich ebenfalls auf MEDIUM. Positiv zu vermerken: die App enthält keine biometrischen Daten, keine Standortberechtigungen, und keine SDK-Einbindungen aus Jurisdiktionen ohne EU-Angemessenheitsbeschluss.

Sechs Nachrichten wurden über 78 Tage gesendet, ursprünglich an redaktion@derstandard.at, ab der zweiten Nachricht direkt an datenschutz@derstandard.at mit redaktion@derstandard.at in Kopie. Die österreichische DSB und CERT.at waren durchgehend informiert. Zwei automatische Weiterleitungsbestätigungen kamen von der Redaktion, keine einzige inhaltliche Antwort kam je von der Datenschutzadresse. Das 90-Tage-Embargo, dem Betreiber direkt in der Erstmeldung mitgeteilt, läuft heute ab. Dieser Bericht und die begleitende Abschlussmitteilung veröffentlichen zum angegebenen Datum.

Scope: Root-Level-Code-Analyse der produktiven DER STANDARD Android-Anwendung (derstandard.at.istandardx, Version 7.0.24.127275), aus dem Google Play Store geladen und am 27. Juni 2026 untersucht. Es wurde kein Konto angelegt, und es fand keine Interaktion mit der Backend-Infrastruktur von Firebase, Sentry oder CleverPush statt.

Disposition

Vier Befunde wurden am 27. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Ein hardcodierter Firebase-API-Key, Pre-Consent-Tracking über drei ContentProvider, das CleverPush-SDK ohne nachweisbaren Art.-28-Auftragsverarbeitungsvertrag, und Werbe-ID-Tracking in einer Nachrichtenanwendung mit potenzieller Ableitung politischer Meinungen korrigieren sich alle auf MEDIUM. Sechs Nachrichten wurden über 78 Tage gesendet. Keine einzige inhaltliche Antwort wurde je empfangen.

ID	Severity	Title
C1	MEDIUM	Firebase-API-Key hardcodiert im Play-Store-Binary

ID	Severity	Title
C2	MEDIUM	Pre-Consent-Tracking über drei automatisch startende ContentProvider
H1	MEDIUM	CleverPush-SDK ohne nachweisbaren Auftragsverarbeitungsvertrag
H2	MEDIUM	Werbe-ID-Tracking in einer Nachrichtenanwendung

Was DER STANDARD richtig macht

Fairness gehört dazu: die App enthält keine biometrischen Daten, keine Standortberechtigungen (ACCESS_FINE_LOCATION ist nicht deklariert), und keine SDK-Einbindungen aus Jurisdiktionen ohne EU-Angemessenheitsbeschluss. Das ist keine Selbstverständlichkeit. Die gefundenen Probleme sind behebbar, das Pre-Consent-Problem etwa lässt sich mit einer Konfigurationsänderung im Manifest lösen.

Sechs Nachrichten, keine inhaltliche Antwort

Die Erstmeldung ging an redaktion@derstandard.at, ausgelöst durch die eigene Berichterstattung des Mediums über Messenger-Überwachung. Zwei automatische Weiterleitungsbestätigungen kamen zurück. Ab der zweiten Nachricht wurde direkt an datenschutz@derstandard.at adressiert, mit redaktion@derstandard.at weiterhin in Kopie, über vier weitere Nachrichten hinweg. Von der Datenschutzadresse kam zu keinem Zeitpunkt eine Antwort, auch keine automatische.

Findings

C1: Firebase-API-Key hardcodiert im Play-Store-Binary

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

Der Firebase-API-Key AIzaSyADHZd1sv3lp0Mm0GRA6QEHCNoP9t67ZxY, zugehörig zum Firebase-Projekt istandard-android-appindexing, ist im Produktions-Binary hardcodiert und für jeden extrahierbar, der die APK herunterlädt.

```
google_api_key: AIzaSyADHZd1sv3lp0Mm0GRA6QEHCNoP9t67ZxY
firebase_project: istandard-android-appindexing
```

Impact: Jeder Akteur kann die API-Kontingente des Projekts anonym erschöpfen und damit den Dienst lahmlegen.

Fix: Den API-Key nach Package-Name und Zertifikat einschränken. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

C2: Pre-Consent-Tracking über drei automatisch startende ContentProvider

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.

FirebaseInitProvider, SentryInitProvider und SentryPerformanceProvider sind alle drei als Android-ContentProvider mit automatischem App-Start registriert. Firebase und Sentry sammeln Daten, bevor der Nutzer dem Consent-Dialog überhaupt begegnet ist.

Impact: Verhaltensdaten der Leserschaft werden gesammelt, bevor irgendeine Einwilligung vorliegt, ein direkter Verstoß gegen das Erfordernis, dass Einwilligung der Verarbeitung vorausgehen muss.

Fix: Alle drei ContentProvider hinter den Consent-Mechanismus verschieben. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

H1: CleverPush-SDK ohne nachweisbaren Auftragsverarbeitungsvertrag

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.

Das CleverPush-SDK, 477 Smali-Klassen einschließlich CleverPushGeofenceTransitionsIntentService, leitet Nutzerdaten über api.cleverpush.com. Ob ein Art.-28-Auftragsverarbeitungsvertrag besteht, ist aus dem Binary nicht nachweisbar.

Impact: Nutzerdaten fließen an einen externen Verarbeiter, ohne dass die Grundlage dieser Verarbeitung öffentlich nachvollziehbar ist.

Fix: Den Art.-28-Auftragsverarbeitungsvertrag für CleverPush öffentlich dokumentieren oder in der Datenschutzerklärung referenzieren. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

H2: Werbe-ID-Tracking in einer Nachrichtenanwendung

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.

Die App deklariert ACCESS_ADSERVICES_AD_ID und ACCESS_ADSERVICES_ATTRIBUTION. Aus dem Leseverhalten einer Nachrichtenanwendung lassen sich politische Meinungen ableiten. Werbe-Tracking auf dieser Datenbasis erfordert eine explizite Rechtsgrundlage nach Art. 9 DSGVO, besondere Datenkategorien.

Impact: Werbe-Tracking, das auf dem Leseverhalten einer Tageszeitung aufbaut, kann strukturell politische Meinungsprofile erzeugen, ohne dass dafür die nach Art. 9 DSGVO erforderliche Rechtsgrundlage dokumentiert ist.

Fix: Die spezifische Art.-9-Rechtsgrundlage für dieses Tracking dokumentieren oder das Werbe-ID-Tracking entfernen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

Datenschutz, Artikel für Artikel

Die Befunde ordnen sich einer kleinen, spezifischen Gruppe von DSGVO-Bestimmungen zu, hier gesammelt statt über die Befunde verstreut.

Artikel	Befund	Grundlage
Art. 32	C1	Hardcodierter Firebase-API-Key im Play-Store-Binary.
Art. 7	C2	Pre-Consent-Tracking über drei automatisch startende Content-Provider.
Art. 28	H1	CleverPush-SDK ohne nachweisbaren Auftrags verarbeitungsvertrag.
Art. 9	H2	Werbe-ID-Tracking mit potenzieller Ableitung politischer Meinungen.

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 ist die Scoring-Richtlinie von RFI-IRFOS, keine Ober- oder Untergrenze. Sie liefert einen reproduzierbaren, für Dritte nachvollziehbaren Ausgangspunkt für den Schweregrad und erfasst reale Blast-Radius-Effekte nicht von sich aus. In diesem Bericht korrigieren sich alle vier Befunde auf MEDIUM, jeweils auf ihrer eigenen berechneten Stufe, ohne Eskalation. Die Erstmeldung bezeichnete die ersten beiden Befunde zu einem Zeitpunkt vor Einführung von CVSS v4.0 in die Methodik als KRITISCH, eine Einordnung, die dieser Bericht nicht rückwirkend anpasst. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: derstandard.at.istandardx.