Coordinated Security & Privacy Disclosure, Final Report

RTL+ for Android (de.rtlplus.app)

Eight written notices, ninety-one days, two automated ticket receipts, one non-substantive human reply, one self-contradicting jurisdictional deflection from the state media regulator, zero technical engagement

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – FIVE FINDINGS ON A MAJOR STREAMING PLATFORM, ZERO TECHNICAL ENGAGEMENT

Target	RTL interactive GmbH / RTL Deutschland GmbH, Picassoplatz 1, 50679 Köln, part of RTL Group (Bertelsmann); jointly referenced with SUPER RTL Fernsehen GmbH (TOGGO)
Product audited	RTL+ for Android, de.rtlplus.app
Disclosure reference	REF: de.rtlplus.app
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (H1 Zipline server-controlled dynamic JavaScript execution bypassing Play Store review, CVSS v4.0 9.2, unaddressed)

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 RTL+ Android application and identified five findings: a hardcoded Firebase API key in the 'rtl-de' project, a minSdk of 22 (Android 5.1, 2015, eight years without security updates as of 2019) accepting subscription-billing and login traffic with a possible PSD2 RTS Art. 4 dimension, Cash App's Zipline library enabling server-controlled, runtime-loaded JavaScript that bypasses Google Play Store review entirely, usage and session data transmitted to Nielsen, New Relic, and NPAW YouBora US infrastructure with no disclosed Art. 44-49 transfer mechanism, and USE_BIOMETRIC/USE_FINGERPRINT permissions with no identifiable Art. 9(2) legal basis for biometric data processing.

RTL/RTL+ never engaged with any of the three core technical findings (Firebase key, minSdk 22, Zipline) across the entire disclosure period. Two automated RTL Zuschauerservice ticket acknowledgments (28 June, 4 July) and one named but non-substantive RTL+ support reply (Jan Siewert, 6 July: 'we cannot yet tell from your message what you need help with') were the only responses from the company itself. On 19 August 2026, the Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) replied, asserting that, as RTL Deutschland is a private broadcaster under state media law (§ 49 Abs. 2 LMG NRW), the Landesanstalt für Medien NRW's own data protection officer, not LDI NRW, holds jurisdiction 'soweit deren Programmtätigkeit betroffen ist' (insofar as broadcasting activity is concerned). RFI-IRFOS disputed this the same day: an Android app's Firebase configuration, minimum SDK version, and third-party SDK data flows are not broadcasting programme activity, and the reply itself left unclear whether the media-law carve-out applies to RTL Deutschland's entire activity or only its programme content specifically.

The Zipline finding (H1) is scored CRITICAL: a mechanism that loads server-controlled JavaScript at runtime, entirely outside app-store review, on a platform serving a large subscriber base, represents a persistent, self-updating code-execution channel RFI-IRFOS could not verify to be safely sandboxed. RTL+'s embedded FairTiq-unrelated third-party analytics stack (Nielsen, New Relic, NPAW YouBora) compounds the data-protection exposure with an undisclosed US transfer mechanism. This case shares its ultimate parent company and disclosure timeline with RFI-IRFOS's separate report on TOGGO (SUPER RTL Fernsehen GmbH), disclosed jointly as sibling platforms bundled together in RTL Group's own 'TOGGO + RTL+' offering, and reported here under its own reference.

Scope: Static analysis of the publicly downloaded production RTL+ Android APK (de.rtlplus.app), on an authorized test device, only. No RTL+ account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@rtl.de and privacy@rtl.de (privacy@rtl.de bounced immediately). Across eight written notices over ninety-one days, cc'd to the Austrian DSB and, from 6 July onward, to the Landesbeauftragte für Datenschutz und Informationsfreiheit NRW, RTL/RTL+ produced two automated ticket-acknowledgment auto-replies and one named but non-substantive human reply ('we cannot tell what your request is'). The state media regulator LDI NRW replied once, asserting jurisdiction under state media law rather than the general GDPR framework, in terms RFI-IRFOS disputed as internally inconsistent the same day. None of the five findings ever received a technical response.

ID	Severity	Title
C1	HIGH	Hardcoded Firebase API key in production binary
C2	MEDIUM	minSdk 22 (Android 5.1, 2015) on a subscription-billing and login platform
H1	CRITICAL	Zipline server-controlled dynamic JavaScript execution bypasses Play Store review
H3/H5	HIGH	Nielsen, New Relic, and NPAW YouBora usage/session data sent to US infrastructure
H4	MEDIUM	Biometric permissions with no identifiable legal basis

Subject & Operator Analysis

RTL interactive GmbH and RTL Deutschland GmbH, Picassoplatz 1, 50679 Köln (Geschäftsführer:innen Andreas Fischer und Julia Kloke), operate RTL+ as part of RTL Group (Bertelsmann), jointly referenced with sibling entity SUPER RTL Fernsehen GmbH for the TOGGO platform, under the jurisdiction of the Landesbeauftragte für Datenschutz und Informationsfreiheit NRW and, per RTL's own disputed jurisdictional claim, the Landesanstalt für Medien NRW's data protection officer for programme-related activity.

Findings

C1: Hardcoded Firebase API key in production binary

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N, 8.8

A hardcoded Firebase API key for project 'rtl-de' (AIzaSyCvwRNE1OSgdzE9CJ7tV0U3Ya2EixWofIw) is present in the production binary.

Never addressed technically across eight notices; only automated ticket receipts and one 'cannot tell what you need' reply were received.

Impact: On a major streaming platform's large subscriber base, exposure spans quota/billing denial-of-service and forged push notifications against the Firebase project.

Fix: Rotate the exposed key, confirm Firebase App Check enforcement, and publish a Security Rules export proving deny-by-default configuration.

C2: minSdk 22 (Android 5.1, 2015) on a subscription-billing and login platform

MEDIUM, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 5.3

Subscription billing and login accept devices running Android 5.1 (API 22), a platform baseline that has received no security updates since 2019, with a possible PSD2 RTS Art. 4 dimension for the payment pipeline.

RFI-IRFOS asked what justifies this baseline on a payment-handling platform in 2026, and whether the LDI NRW or the LfM was notified under Art. 33; neither question received an answer. Scored to reflect that exploitation requires an attacker with local access to an already-compromised, unpatched device rather than remote reachability.

Impact: Billing and authentication credentials processed on unpatched, eight-plus-year-old device software carry elevated compromise risk that current Android security baselines exist specifically to close.

Fix: Raise minSdk in line with current platform security baselines for any app handling subscription billing or payment credentials.

H1: Zipline server-controlled dynamic JavaScript execution bypasses Play Store review

CRITICAL, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N, 9.2

Cash App's Zipline library is present, enabling server-controlled JavaScript that is loaded and executed at runtime, entirely outside the Google Play Store's app-review process.

RFI-IRFOS asked what server-side JS payloads are actually delivered to EU users via Zipline and how their data-protection compliance is assured without app-store review; this question was never answered. Scored conservatively (AC:H) since RFI-IRFOS's static analysis could not confirm the sandboxing boundary of the executed code, but the mechanism itself constitutes a persistent, unreviewed remote code-execution channel.

Impact: A production streaming app can have its runtime behavior altered server-side, for any user, without any app-store review checkpoint, at any time.

Fix: Document Zipline's sandboxing boundary and change-control process, or remove the mechanism in favor of standard, reviewable app-store release channels.

H3/H5: Nielsen, New Relic, and NPAW YouBora usage/session data sent to US infrastructure

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

Usage and session data is transmitted to Nielsen, New Relic, and NPAW YouBora, all US-based infrastructure, with no transfer mechanism disclosed in the app's own context.

Never addressed technically across eight notices.

Impact: Streaming usage and session data for RTL+'s user base is transferred to US third parties without a confirmed Art. 44-49 safeguard named where users can find it.

Fix: Name Nielsen, New Relic, and NPAW YouBora explicitly as processors with their applicable transfer mechanism in the privacy policy.

H4: Biometric permissions with no identifiable legal basis

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

USE_BIOMETRIC and USE_FINGERPRINT are declared with no identifiable Art. 9(2) GDPR legal basis for the associated biometric data processing.

Never addressed technically across eight notices.

Impact: Biometric authentication capability is present without a documented special-category-data legal basis for its use.

Fix: Document the Art. 9(2) legal basis for biometric authentication, or restrict the permission to device-local authentication with no server-side biometric data processing.

A Jurisdictional Deflection From the Regulator Itself

The only substantive reply this case produced came not from RTL/RTL+ but from LDI NRW, on 19 August 2026, and it was jurisdictional rather than technical: RTL Deutschland and SUPER RTL, as private broadcasters under § 49 Abs. 2 Landesmediengesetz NRW, fall under the data protection oversight of the Landesanstalt für Medien NRW's own data protection officer, 'soweit deren Programmtätigkeit betroffen ist.' RFI-IRFOS disputed this the same day and cc'd the Landesanstalt für Medien NRW directly: a hardcoded Firebase key, an eight-year-unpatched minimum Android version on a billing platform, and a server-controlled JavaScript execution channel are properties of an Android application, not broadcasting programme content, and LDI NRW's own phrasing left unresolved whether the media-law carve-out covers RTL Deutschland's entire activity or only content specifically related to programming. No further reply from either regulator or from RTL/RTL+ followed.

A Related, Jointly-Bundled Case: TOGGO

RTL+ and TOGGO are sibling platforms under RTL Group, marketed together in a joint 'TOGGO + RTL+' bundle, and operated respectively by RTL interactive GmbH and SUPER RTL Fernsehen GmbH. RFI-IRFOS disclosed TOGGO separately under its own reference and embargo date; that report likewise notes it was disclosed jointly with RTL+. Neither case received substantive technical engagement from the RTL Group side.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded Firebase key, unaddressed
C2	GDPR Art. 32, PSD2 RTS Art. 4	Eight-year-unpatched Android baseline on a billing platform
H1	GDPR Art. 32	Server-controlled JS execution outside app-store review
H3/H5	GDPR Art. 44-49	Usage/session data sent to US infrastructure, no disclosed transfer mechanism
H4	GDPR Art. 9(2)	Biometric permissions, no identifiable legal basis

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@rtl.de and privacy@rtl.de (bounced); C1, C2, H1, H3/H5, H4 disclosed; embargo stated as 2026-09-19
2026-06-28	Follow-up, 7 days no answer; automated ticket 03584638 received same day
2026-07-04	Follow-up #2, cc dsb@dsb.gv.at; automated ticket 03597130 received same day
2026-07-06	Non-substantive human reply (Jan Siewert, RTL+ support): 'cannot tell what you need'
2026-07-06	Follow-up #3, cc dsb@dsb.gv.at and poststelle@ldi.nrw.de from this point onward
2026-07-24	Follow-up, 18 days since last reply
2026-07-27	Follow-up, 21 days of automated replies only
2026-08-09	Follow-up, 49 days since first notice, six messages, two regulators cc'd
2026-08-12	Automated ticket update, no substantive content
2026-08-19	LDI NRW replies asserting Landesanstalt für Medien NRW jurisdiction over broadcaster programme activity
2026-08-19	RFI-IRFOS disputes the jurisdictional framing same day, cc datenschutzaufsicht@medienanstalt-nrw.de
2026-09-03	Follow-up, 74 days, seven messages, no substantive technical answer; embargo reaffirmed as 2026-09-19
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Rotate the exposed Firebase key and confirm App Check enforcement for the 'rtl-de' project.
- Raise minSdk in line with current platform security baselines for the subscription-billing and login flow.
- Document Zipline's sandboxing boundary and change-control process, or remove server-controlled runtime JavaScript execution.
- Name Nielsen, New Relic, and NPAW YouBora explicitly as US processors with their transfer mechanism in the privacy policy.
- Clarify, in writing, whether Landesanstalt für Medien NRW jurisdiction covers RTL Deutschland's entire activity or only programme-specific content, so future disclosures reach the correct regulator on the first attempt.

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, 9, 32, 33, 44-49. PSD2 RTS Art. 4. REF de.rtlplus.app.