Coordinated Security & Privacy Disclosure, Final Report

TOGGO for Android (de.toggo)

Five written notices, ninety-one days, four identical ticket auto-replies, one off-topic regulator jurisdiction dispute, zero substantive replies from SUPER RTL

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SEVEN FINDINGS UNADDRESSED AFTER FIVE NOTICES

Target	SUPER RTL Fernsehen GmbH, Cologne, Germany, part of the Bertelsmann/RTL Group family
Product audited	TOGGO for Android, de.toggo
Disclosure reference	REF TOGGO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Privacy Sandbox Topics API active on a dedicated children's platform, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Findings 4

3.1 C1: Firebase API key hardcoded in the publicly distributed APK 4

3.2 C2: Privacy Sandbox Topics API active on a dedicated children's platform . . . 5

3.3 H1: Adobe Experience Cloud (15 modules) – cross-channel identity resolution and personalization on children's data 5

3.4 H2: GfK SUI Connector – audience research data collection from children . . . 6

3.5 H3: CleverPush (563 classes) – marketing stack aimed at children as young as three 6

3.6 H4: RECORD_AUDIO, CAMERA, and video-capture permissions declared together with no confirmed consent gate 6

3.7 H5: minSdk 26 (Android 8.0, 2017) – devices unpatched since 2022 supported 7

4 Four Auto-Replies, One Jurisdiction Dispute, Zero Substance From SUPER RTL 7

5 A Joint Disclosure, Reported Separately: RTL+ 7

6 Data Protection, Article by Article 8

7 Disclosure Timeline & Outcome 9

8 Residual Risk & Recommendations 10

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production TOGGO Android application, a streaming platform aimed at children aged 3 and up, and identified two CRITICAL and five HIGH findings: a Firebase project key hardcoded in the shipped APK, a Privacy Sandbox Topics API implementation (68 smali files) actively profiling users for ad topics while running simultaneously with an internal flag suppressing Ads Storage cookies, an internal contradiction rather than a coherent privacy posture, a 15-module Adobe Experience Cloud integration performing cross-channel identity resolution and A/B personalization with real-time streaming of children's behavioral data to Adobe's US Edge Network, a GfK SUI Connector feeding children's viewing behavior into commercial audience-ratings panels, a 563-class CleverPush marketing stack running push notifications, in-app chat, and banner campaigns aimed at children as young as three, RECORD_AUDIO, CAMERA, and video-capture permissions declared together with no confirmed consent gate for the COPPA-relevant under-13 audience, and a minimum supported Android version last patched in 2022.

Across five written notices over ninety-one days, TOGGO's own ticket system returned four identical automated acknowledgments and never routed to a human. The case's only substantive reply came from LDI NRW on 19 August, disputing its own jurisdiction over the joint RTL+/TOGGO disclosure rather than addressing any finding; RFI-IRFOS replied the same day pointing out an internal contradiction in LDI NRW's own jurisdictional reasoning and requested clarification by 26 August, which was never received. No member of SUPER RTL's privacy or security team replied in substance at any point, and none of RFI-IRFOS's three standing questions, on DPO awareness of the Topics API, an Art. 28 DPA with Adobe, or a remediation timeline, ever received an answer.

Scope: Static analysis of the publicly downloaded production TOGGO Android APK, on an authorized test device, only. No SUPER RTL account, backend, or infrastructure was accessed or tested. RTL+ (de.rtli.tvnow), disclosed jointly in the original R1, is reported separately under its own reference.

Disposition

R1 sent 20 June 2026 jointly covering TOGGO and its sibling platform RTL+ (reported separately under its own reference), to no-reply@toggo.de, with TOGGO-specific follow-ups then routed to kommunikation@superrtl.de and Datenschutz@toggo.de, cc/bcc the Austrian Datenschutzbehoerde, LDI NRW, the German BfDI, CERT.at, and, from 19 August, the Landesanstalt fuer Medien NRW. Across five written notices over ninety-one days, TOGGO's ticket system sent four identical automated acknowledgments; the only substantive reply in the case came from LDI NRW disputing its own jurisdiction, not from SUPER RTL. No member of SUPER RTL's privacy or security team ever replied in substance.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the publicly distributed APK

ID	Severity	Title
C2	CRITICAL	Privacy Sandbox Topics API active on a dedicated children's platform
H1	HIGH	Adobe Experience Cloud (15 modules) – cross-channel identity resolution and personalization on children's data
H2	HIGH	GfK SUI Connector – audience research data collection from children
H3	HIGH	CleverPush (563 classes) – marketing stack aimed at children as young as three
H4	HIGH	RECORD_AUDIO, CAMERA, and video-capture permissions declared together with no confirmed consent gate
H5	HIGH	minSdk 26 (Android 8.0, 2017) – devices unpatched since 2022 supported

Subject & Operator Analysis

SUPER RTL Fernsehen GmbH, based in Cologne, Germany, operates TOGGO as part of the Bertelsmann/RTL Group family, alongside sibling platform RTL+. LDI NRW's own jurisdiction reply refers jointly to 'RTL interactive GmbH und SUPER RTL Fernsehen GmbH.'

Findings

C1: Firebase API key hardcoded in the publicly distributed APK

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

res/values/strings.xml contains verbatim API key AIzaSyB0CD8BcCBtQ_ADTgsGySpyM50yIAsfSH0, database URL https://srtl-toggo.firebaseio.com, project srtl-toggo, App ID 1:878017703711:android:5ca3e4c05ec0134777ca2a, extractable from the public APK in under 60 seconds.

No reply of any kind, substantive or otherwise, addressed this finding across five notices.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm Firestore/RTDB security rules are deny-by-default, and enforce App Check for this project.

C2: Privacy Sandbox Topics API active on a dedicated children's platform

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

ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_AD_ID, and ACCESS_ADSERVICES_ATTRIBUTION permissions are declared, and TopicsManagerFutures/TopicsManagerImplCommon (68 smali files) actively calls getTopicsAsync(). This runs simultaneously with an internal flag, gads:tfcd_deny_ad_storage:enabled, which suppresses Ads Storage cookies but does not disable the separate Topics profiling pipeline.

The coexistence of a child-directed-treatment flag with an active ad-topics profiling call is an internal contradiction rather than a coherent privacy posture. No reply of any kind addressed this finding.

Impact: Ad-topic profiling continues to operate on a platform whose entire audience is children, despite an internal flag apparently intended to suppress ad-related data collection for that same audience.

Fix: Disable the Topics API call entirely on a platform serving a child-only audience, consistent with the intent already expressed by the tfcd_deny_ad_storage flag.

H1: Adobe Experience Cloud (15 modules) – cross-channel identity resolution and personalization on children's data

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

com.adobe.marketing.mobile analytics, edge, identity, optimize, launch, lifecycle, signal, and rulesengine modules are present, performing cross-channel identity resolution and A/B personalization with real-time streaming of behavioral data to Adobe's US Edge Network.

No reply of any kind addressed this finding.

Impact: Children's cross-channel behavioral profiles may be constructed and streamed to a US vendor with no confirmed Art. 28/44 coverage for this specific data class.

Fix: Confirm and publish an Art. 28 DPA and Art. 44 transfer mechanism with Adobe covering this specific real-time data stream, or discontinue it for this audience.

H2: GfK SUI Connector – audience research data collection from children

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

28 smali files (SUIConnector, collector, transmitter, http) feed children's viewing behavior into GfK commercial audience-ratings panels.

No reply of any kind addressed this finding.

Impact: Children's viewing behavior is shared with a third-party commercial ratings panel with no confirmed disclosure matching that specific recipient.

Fix: Disclose GfK explicitly as a recipient of viewing-behavior data and confirm the applicable legal basis for this specific audience.

H3: CleverPush (563 classes) – marketing stack aimed at children as young as three

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

A full commercial marketing campaign stack, push banners, in-app chat, stories, and inbox management, is present via the CleverPush SDK, targeting an audience aged three and up.

No reply of any kind addressed this finding.

Impact: A commercial marketing and engagement stack of this scope operates on an audience below the age at which most jurisdictions consider marketing consent meaningful.

Fix: Scope CleverPush's marketing features down to age-appropriate, non-targeted engagement for this audience.

H4: RECORD_AUDIO, CAMERA, and video-capture permissions declared together with no confirmed consent gate

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

RECORD_AUDIO, CAMERA, and video-capture capability are declared together. COPPA Sec. 312.2(b) classifies voice recordings from under-13 users as personal information requiring verifiable parental consent; no confirmed consent gate was found in static analysis.

No reply of any kind addressed this finding.

Impact: Audio, camera, and video capture capability may be exercised on a children's platform without the verifiable parental consent COPPA and GDPR Art. 8 both require.

Fix: Publish confirmation of the verifiable-parental-consent mechanism gating these capture permissions, or remove the permissions if unused.

H5: minSdk 26 (Android 8.0, 2017) – devices unpatched since 2022 supported

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

The app's minimum supported Android version, 8.0, stopped receiving security updates in 2022; the app remains connected to a live Firebase backend on such devices.

No reply of any kind addressed this finding.

Impact: A children's streaming platform with live backend connectivity supports devices carrying four years of unpatched platform-level vulnerabilities.

Fix: Raise the minimum supported Android version to one still receiving security updates.

Four Auto-Replies, One Jurisdiction Dispute, Zero Substance From SUPER RTL

TOGGO's ticket system returned four identical automated acknowledgments across the case and never routed to a human. The only substantive reply this case produced came not from SUPER RTL but from LDI NRW on 19 August, disputing its own jurisdiction over the joint RTL+/TOGGO disclosure and redirecting toward the Landesanstalt fuer Medien NRW's own data protection officer. RFI-IRFOS replied the same day identifying an internal contradiction in LDI NRW's cited standard and requested clarification by 26 August; none arrived. No member of SUPER RTL's own privacy or security team ever replied in substance.

A Joint Disclosure, Reported Separately: RTL+

TOGGO was disclosed jointly with its sibling platform RTL+ (de.rtli.tvnow) in the original R1, reflecting their shared Bertelsmann/RTL Group ownership. Each platform's specific findings and follow-up correspondence were then run separately, and each is reported here on its own terms; RTL+'s findings are covered in its own report under its own reference.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key in the production APK
C2	GDPR Art. 8, Art. 5(1)(a)(b)	Ad-topics profiling active on a child-only platform
H1	GDPR Art. 8, Art. 28, Art. 44	Cross-channel identity resolution and US data streaming on children's data
H2	GDPR Art. 13(1)(e)(f)	Undisclosed third-party sharing of children's viewing behavior
H3	GDPR Art. 8	Commercial marketing stack targeting an under-consent-age audience
H4	COPPA Sec. 312.2(b); GDPR Art. 8	Audio/camera/video capture permissions with no confirmed consent gate
H5	GDPR Art. 32	Unpatched minimum supported Android version

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent jointly for TOGGO and RTL+ to no-reply@toggo.de; a EUR 120,000 combined remediation figure was referenced under the R1 policy then in force – historical record only, not a currently open offer; automated ticket ack same day
2026-06-28	TOGGO-specific R2 sent to kommunikation@superrtl.de, three questions posed, regulators bcc'd
2026-08-09	Follow-up moves regulators from bcc to visible cc; second automated ticket ack received
2026-08-19	LDI NRW replies disputing its own jurisdiction; RFI-IRFOS responds same day requesting clarification by 26 August
2026-09-04	Follow-up, sixty-eight days since the full findings notice, three automated replies, zero substantive reaction
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Disable the Topics API on a platform serving a child-only audience.
- Confirm and publish an Art. 28 DPA and Art. 44 transfer mechanism with Adobe for the real-time behavioral data stream.
- Disclose GfK explicitly as a recipient of children's viewing-behavior data.
- Rotate the exposed Firebase key and confirm deny-by-default security rules with App Check enforced.
- Publish confirmation of the `verifiable-parental-consent` mechanism gating audio/camera/video capture.

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. GDPR Art. 5, 8, 13, 25, 28, 32, 44. COPPA Sec. 312.2(b). REF TOGGO-2026-R1.