Coordinated Security & Privacy Disclosure, Final Report

YouTube Kids for Android (com.google.android.apps.youtube.kids, v11.24.541)

Ten written notices, ninety days, one dead mailbox, one press-office auto-reply loop, zero human replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED AFTER TEN NOTICES

Target	Google Ireland Limited / Google LLC
Product audited	YouTube Kids for Android, com.google.android.apps.youtube.kids, v11.24.541
Disclosure reference	REF YTKIDS-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-18/19 (stated as 18 September in later follow-ups, 19 September in the original R1; this internal inconsistency in the sender's own drafting is disclosed here rather than silently resolved – both dates have passed as of publication)
Report published	2026-09-19
Severity	CRITICAL (C2 RECORD_AUDIO voice-data collection from children with no verifiable parental consent confirmed, 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

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production YouTube Kids Android application, a COPPA-designated children's product, and identified two CRITICAL and four HIGH findings: a Firebase API key carrying a development-environment project name hardcoded in the production binary, an active microphone pipeline (ten smali files reference it) capable of collecting children's voice recordings, which COPPA Sec. 312.2(b) classifies as personal information requiring verifiable parental consent, that consent was not confirmable from static analysis alone, a hardcoded IS_CHILD_ACCOUNT_OVER_13 string applying the US COPPA age-13 threshold to EU users instead of the applicable GDPR Art. 8 and national thresholds (14 in Austria, 16 in Germany and under the GDPR default), a bundled Google Cardboard VR SDK with camera-based QR scanning and no disclosed in-app age gate despite Google's own Daydream guidance recommending 13+ for VR, biometric-authentication permissions implicating Art. 9 special-category data on a children's platform, and a legacy broad storage permission inconsistent with the scoped-storage requirement in force since the app's declared minimum SDK level.

Across ten written notices over ninety days, privacy@google.com bounced on every attempt from the second notice onward, confirmed via five separate delivery-failure notifications, and correspondence was rerouted to press@google.com, which returned only an automated press-office acknowledgment four times and never routed to a person. No human reply of any kind was ever received from Google on this case. Neither of RFI-IRFOS's two standing questions, whether Google's DPO or legal team is aware that the COPPA threshold is being applied in place of applicable EU age thresholds, or whether the dev-named Firebase credential would be rotated before or after a supervisory authority raised it, ever received an answer.

Scope: Static analysis of the publicly downloaded production YouTube Kids Android APK (v11.24.541), on an authorized test device, only. No Google account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to privacy@google.com, cc press@google.com, the Austrian Datenschutzbehoerde, and the Irish Data Protection Commission. privacy@google.com bounced on every attempt from the second notice onward ('the group you tried to contact may not exist'), confirmed via five separate mailer-daemon bounce notifications, and correspondence was rerouted primarily to press@google.com from the seventh notice onward. Across ten written notices over ninety days, the only inbound messages were four identical automated press-office acknowledgments; no human reply of any kind was ever received.

ID	Severity	Title
C1	CRITICAL	Firebase API key with a development project name hardcoded in a production children's app
C2	CRITICAL	RECORD_AUDIO – voice data collected from children, verifiable parental consent not confirmed

ID	Severity	Title
H1	HIGH	IS_CHILD_ACCOUNT_OVER_13 applies the COPPA threshold to EU children instead of GDPR Art. 8 thresholds
H2	HIGH	Google Cardboard VR SDK (117 classes) – camera access, no disclosed in-app age gate
H3	HIGH	USE_BIOMETRIC and USE_FINGERPRINT – Art. 9 special-category data in a children's app
H4	HIGH	WRITE_EXTERNAL_STORAGE – legacy permission inconsistent with scoped storage

Subject & Operator Analysis

YouTube Kids is developed and operated by Google LLC, with Google Ireland Limited as the entity typically named for EU-directed correspondence. The Austrian Datenschutzbehoerde and Irish Data Protection Commission were informed from the original notice onward.

Findings

C1: Firebase API key with a development project name hardcoded in a production children's app

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 in the public Play Store APK contains a live Firebase key AIzaSyA9C_sRtHusuc4HsxtE57NOxBELMbSWB1w, database URL https://dev-inscriber-552.firebaseio.com, project dev-inscriber-552, App ID 1:548405466498:android:2070b46da7b771c4. A development-named credential ships inside a COPPA-designated children's production binary.

No reply of any kind addressed this finding across ten notices.

Impact: A production Firebase project's attack surface, apparently still carrying a development-stage naming convention, 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: RECORD_AUDIO – voice data collected from children, verifiable parental consent not confirmed

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

Ten smali files reference the microphone pipeline. COPPA Sec. 312.2(b) classifies children's voice recordings as personal information requiring verifiable parental consent before collection.

Static analysis alone cannot confirm whether verifiable parental consent is obtained before this pipeline activates. No reply of any kind answered this question across ten notices.

Impact: Children's voice data may be collected without the verifiable parental consent COPPA and, for EU users, GDPR Art. 8 both require.

Fix: Publish confirmation of the verifiable-parental-consent mechanism gating microphone activation, or disable the pipeline pending that confirmation.

H1: IS_CHILD_ACCOUNT_OVER_13 applies the COPPA threshold to EU children instead of GDPR Art. 8 thresholds

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

The string IS_CHILD_ACCOUNT_OVER_13 is present in the production APK. The Austrian DSG Sec. 4(4) sets the child-consent threshold at 14, the German BDSG Sec. 8 sets it at 16, and the GDPR Art. 8(1) default is 16, while the app applies the US COPPA cutoff of 13.

Effect: a 14-year-old in Vienna exits child-protective processing rules two years earlier than Austrian law provides for; a 15-year-old in Berlin, one year earlier than German law provides for. No reply of any kind addressed this finding.

Impact: EU children between ages 13 and their applicable national threshold may be processed under adult data-protection rules rather than the child-protective rules their own jurisdiction requires.

Fix: Apply the correct national or GDPR Art. 8 default age threshold for EU users instead of the US COPPA cutoff.

H2: Google Cardboard VR SDK (117 classes) – camera access, no disclosed in-app age gate

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

Full GL surface rendering, a QR headset scanner using the camera, and device-parameter reads are present via the bundled Cardboard VR SDK, with no disclosed in-app age gate found. Google's own Daydream guidance recommends VR for ages 13 and up; YouTube Kids targets users under 13.

No reply of any kind addressed this finding.

Impact: An immersive VR feature with camera access is available on a platform whose target users fall below the age range Google's own VR guidance recommends.

Fix: Gate the Cardboard VR feature behind an age check consistent with Google's own VR age guidance, or remove it from this app.

H3: USE_BIOMETRIC and USE_FINGERPRINT – Art. 9 special-category data in a children's app

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

USE_BIOMETRIC and USE_FINGERPRINT permissions are declared. Biometric data is GDPR Art. 9 special-category data; a parental-lock use case may be a legitimate purpose, but explicit disclosure under Art. 9(2) was not confirmed present from static analysis.

No reply of any kind addressed this finding.

Impact: Special-category biometric processing may be occurring on a children's platform without the explicit Art. 9(2) disclosure that processing requires.

Fix: Confirm and publish the specific Art. 9(2) legal basis and disclosure covering the biometric permissions' use case.

H4: WRITE_EXTERNAL_STORAGE – legacy permission inconsistent with scoped storage

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

WRITE_EXTERNAL_STORAGE is declared despite scoped storage having been mandatory since the app's declared minimum SDK level (Android 12).

No reply of any kind addressed this finding.

Impact: A broad legacy storage permission exceeds the data-minimization scoped storage was introduced to enforce, on a children's platform.

Fix: Remove the legacy storage permission and rely on scoped storage APIs consistent with the app's declared minimum SDK level.

A Dead Mailbox, an Auto-Reply Loop, and Ten Notices

privacy@google.com bounced on every attempt from the second notice onward, confirmed by five separate delivery-failure notifications stating the mailbox 'may not exist, or you may not have permission to post messages to the group.' From the seventh notice onward, correspondence was rerouted primarily to press@google.com, which replied only with an automated press-office acknowledgment, four times, and never routed the disclosure to a person. Across ten notices and ninety days, no human reply of any kind was ever received from Google on this case.

Finding	Provision	Concern

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded, dev-named Firebase key in a children's production app
C2	COPPA Sec. 312.2(b); GDPR Art. 8, Art. 9	Voice-data collection from children without confirmed verifiable consent
H1	GDPR Art. 8(1); Austrian DSG Sec. 4(4); German BDSG Sec. 8	US COPPA age threshold applied instead of EU/national thresholds
H2	GDPR Art. 5(1)(c), Art. 13	Camera-enabled VR feature with no disclosed age gate below Google's own guidance
H3	GDPR Art. 9(2)	Undisclosed biometric-permission use case on a children's platform
H4	GDPR Art. 5(1)(c)	Legacy storage permission inconsistent with scoped storage requirements

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@google.com; C1 and H1 first raised; Austrian DSB and Irish DPC informed
2026-06-27 to 2026-07-27	Five follow-ups to privacy@google.com; every message bounces, confirmed via mailer-daemon
2026-08-09	First message routed primarily to press@google.com after the bounce pattern is confirmed

Date	Event
2026-08-31	Follow-up, twenty-two days since the prior message, no reply of any kind; embargo restated as 18 September
2026-09-12	Follow-up, two direct yes/no questions posed with a deadline of 16 September
2026-09-16	Final follow-up, deadline day, no answer to either question, stated as likely the last message before publication
2026-09-19	Embargo, as stated (with the internal 18/19 September inconsistency disclosed above), closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning privacy contact address for EU GDPR disclosures distinct from the press office.
- Apply the correct national or GDPR Art. 8 default age threshold for EU users instead of the US COPPA cutoff.
- Publish confirmation of the `verifiable-parental-consent` mechanism gating the RECORD_AUDIO pipeline.
- Rotate the exposed, development-named Firebase key.
- Confirm the Art. 9(2) legal basis and disclosure covering the app's biometric permissions.

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, 9, 13, 25, 32. COPPA Sec. 312.2(b). REF YTKIDS-2026-R1.