# Coordinated Security & Privacy Disclosure, Final Report

## Roma and Diana Show for Android (com.epicrondigital.romadianashow, v2.8.3)

Thirteen written notices, eighty-eight days, one misdirected regulator bounce, zero replies of any kind, a children's app tied to a 130 million-plus subscriber channel

**PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED AFTER THIRTEEN NOTICES, ZERO REPLIES**

| | |
|---|---|
| **Target** | Epicron Digital, Garut, West Java, Indonesia |
| **Product audited** | Roma and Diana Show for Android, com.epicrondigital.romadianashow, v2.8.3 (companion app to the Roma and Diana Show children's YouTube channel, 130 million-plus subscribers) |
| **Disclosure reference** | REF RFI-2026-EP-001 |
| **R1 sent** | 2026-06-24 |
| **Disclosure / embargo date** | 2026-09-19 |
| **Report published** | 2026-09-19 |
| **Severity** | CRITICAL (C1 a hardcoded YouTube Data API key and three hardcoded Firebase/Google Cloud API keys, enabling quota exhaustion or redirection at the target's cost, CVSS v4.0 8.8, unaddressed) |

rfi.irfos@gmail.com • rfi-irfos.com

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

## Contents

## Executive Summary

On 24 June 2026, RFI-IRFOS performed static analysis of the production Roma and Diana Show Android application, the companion app to a children's YouTube channel with over 130 million subscribers and a target audience aged 2 to 8, and identified one CRITICAL and three HIGH findings: a YouTube Data API key embedded directly in a request URL string plus three additional hardcoded Firebase and Google Cloud API keys in the binary, extractable by anyone downloading the APK and sufficient to exhaust the project's API quota, redirect requests, or query YouTube data at the target's cost, the complete absence of an Art. 27 EU representative despite Epicron Digital, based in Indonesia, offering this app to EU data subjects including children, a reCAPTCHA implementation routed through a PRC-hosted CDN endpoint (gstatic.cn) subject to Chinese law regardless of Google's own jurisdiction, constituting an undisclosed third-country transfer with no adequacy decision on a child-directed app, and a complete absence of GDPR-compliant privacy infrastructure for a child-directed application, no DPO, no Art. 13 disclosure of data processors, no parental consent mechanism, and no age verification, with the sole privacy contact being a personal Gmail address.

Across thirteen written notices over eighty-eight days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, the German BfDI, the EDPS, and CERT.at, not one reply of any kind was ever received from Epicron Digital or any address associated with it. The only inbound message in the entire thread was an automated Gmail delivery-failure bounce for a mistyped regulator address, unrelated to the target itself. None of RFI-IRFOS's standing questions, on awareness of the four hardcoded credentials, designation of an Art. 27 EU representative, credential rotation, or Art. 33/35 regulatory notification and DPIA status, ever received an answer.

**Scope:** Static analysis of the publicly downloaded production Roma and Diana Show Android APK (v2.8.3), on an authorized test device, only. No Epicron Digital account, backend, or infrastructure was accessed or tested.

**Disposition**

R1 sent 24 June 2026 to epicrondigital@gmail.com, cc a second Epicron-linked address, bcc the Austrian Datenschutzbehoerde and the German BfDI. Across thirteen written notices over eighty-eight days, not one reply of any kind was ever received from Epicron Digital or any address associated with it; the only inbound message in the entire thread was an automated bounce for a mistyped regulator address, unrelated to the target.

| ID | Severity | Title |
|---|---|---|
| C1 | CRITICAL | YouTube API key hardcoded in a request URL plus three hardcoded Firebase/Google Cloud API keys |
| H1 | HIGH | No Art. 27 EU representative for a non-EU developer serving EU children |
| H2 | HIGH | reCAPTCHA routed through a PRC-hosted CDN endpoint |

| ID | Severity | Title |
|---|---|---|
| H3 | HIGH | No GDPR-compliant privacy infrastructure for a child-directed application |

## Subject & Operator Analysis

Epicron Digital, based in Garut, West Java, Indonesia, operates the companion app for the Roma and Diana Show children's YouTube channel, one of the largest children's media properties on the platform with over 130 million subscribers.

## Findings

### C1: YouTube API key hardcoded in a request URL plus three hardcoded Firebase/Google Cloud API keys

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

A YouTube Data API key is embedded directly in a request URL string (https://youtubei.googleapis.com/youtubei/v1/player?key=AIzaSyDCU8hByM-4DrUqRUYnGn-3lIEO78bcxq8&t=). Three additional hardcoded keys are present in the binary: a Google API key (AIzaSyA-11MrOJ1bSJjvVzBGCPx9SxGRnWfxLho), a second YouTube Data API key from a separate project (AIzaSyDCU8hByM-4DrUqRUYnGn-3lIEO78bcxq8), and a further project key (AIzaSyDyT5W0Jh49F30Pqqtyfdf7pDLFKLJoAnw).

Anyone extracting these keys from the APK can exhaust the associated projects' API quotas, redirect requests, or query YouTube data at the target's cost. No reply of any kind, across thirteen notices, addressed whether any of these four credentials have been rotated or revoked.

**Impact:** Four separate Google Cloud/YouTube API projects' quotas and billing are exposed to abuse by any party extracting these keys from the public APK.

**Fix:** Rotate and revoke all four exposed keys, restrict each to the correct package name and SHA-256 signing fingerprint, and route API calls through an authenticated backend rather than embedded client-side keys.

### H1: No Art. 27 EU representative for a non-EU developer serving EU children

**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**

Epicron Digital is based in Garut, West Java, Indonesia, and distributes this app via Google Play to EU users, including children. GDPR Art. 27(1) requires a non-EU controller offering services to EU data subjects to designate a written EU representative. No such representative is identified anywhere in the app, the Play Store listing, or the privacy policy.

No reply of any kind addressed this finding.

**Impact:** EU data subjects, including parents acting on behalf of children, have no designated EU point of contact for exercising their rights against this non-EU controller.

**Fix:** Designate and publish a written Art. 27 EU representative.

### H2: reCAPTCHA routed through a PRC-hosted CDN endpoint

**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**

The binary references www.gstatic.cn/recaptcha, meaning Google's reCAPTCHA is served via a PRC-hosted CDN endpoint, subject to Chinese law (the Data Security Law and PIPL) regardless of the origin service's own jurisdiction.

This constitutes an undisclosed third-country transfer with no adequacy decision, on a child-directed app. No reply of any kind addressed this finding.

**Impact:** Interaction data from a child-directed app may pass through PRC-jurisdiction infrastructure with no disclosed transfer mechanism.

**Fix:** Route reCAPTCHA and related components through a non-PRC CDN endpoint, or disclose the transfer explicitly with an Art. 46 mechanism.

### H3: No GDPR-compliant privacy infrastructure for a child-directed application

**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**

The app serves content from the Roma and Diana Show YouTube channel (130 million-plus subscribers), targeting children aged 2-8. The privacy contact is a personal Gmail address; there is no DPO, no Art. 13 disclosure listing data processors (Firebase, the YouTube API), no parental consent mechanism, and no age verification.

No reply of any kind addressed this finding.

**Impact:** A children's app with a very large audience operates with no functional privacy infrastructure, no consent mechanism, and no way for parents to identify or contact a responsible data controller.

**Fix:** Implement a parental-consent mechanism, publish an Art. 13 disclosure naming all data processors, and establish a functional privacy contact beyond a personal Gmail address.

## Thirteen Notices, One Misdirected Bounce, Zero Replies

Across thirteen written notices sent over eighty-eight days on a single continuous thread, not one reply of any kind was ever received from Epicron Digital or any address associated with it. The only inbound message in the entire thread was an automated Gmail delivery-failure bounce for a mistyped regulator address (edps@europa.eu instead of edps@edps.europa.eu), unrelated to the target itself.

## Data Protection, Article by Article

| Finding | Provision | Concern |
|---|---|---|
| C1 | GDPR Art. 32(1) | Four hardcoded API keys enabling quota exhaustion/redirection |
| H1 | GDPR Art. 27(1) | No designated EU representative for a non-EU controller serving EU children |
| H2 | GDPR Art. 46 | Undisclosed transfer via a PRC-hosted CDN endpoint |
| H3 | GDPR Art. 8, Art. 13 | No functional privacy infrastructure for a children's app |

## Disclosure Timeline & Outcome

| Date | Event |
|---|---|
| 2026-06-24 | R1 sent; 1 CRITICAL + 3 HIGH findings; bcc Austrian DSB/German BfDI; remediation tiers of EUR 4,500/9,000/18,000 referenced under the R1 policy then in force – historical record only, not a currently open offer |
| 2026-06-30 | Two follow-ups sent minutes apart ('72h-Sweep'), Austrian DSB and EDPS moved to open cc |
| 2026-08-01 | Follow-up sent; automated bounce received for a mistyped regulator address |
| 2026-08-29 | Follow-up, sixty-six days, six messages, zero replies |
| 2026-09-11 | Follow-up, seventy-nine days since disclosure, zero replies, embargo in eight days |
| 2026-09-16 | Follow-up, day 84, zero replies to six substantive messages, embargo in three days, all four findings restated |
| 2026-09-19 | Embargo, as stated identically throughout the correspondence, closes and this report publishes |

## Residual Risk & Recommendations

- Rotate and revoke all four exposed API keys immediately.
- Designate and publish a written Art. 27 EU representative.
- Route reCAPTCHA through a non-PRC CDN endpoint or disclose the transfer explicitly.
- Implement a parental-consent mechanism and publish an Art. 13 disclosure naming all data processors.
- Establish a functional privacy contact beyond a personal Gmail address.

**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. 8, 13, 27, 32, 46. REF RFI-2026-EP-001.