



Coordinated Privacy Disclosure, Final Report

ElePant "Einfache Lernspiele für Kinder" Android
(com.gamesforkids.toddlers.baby.games.girls.learning.coloring.easy)

GunjanApps Studios LLP, India; PEGI 3, Google "Teacher Approved" badge

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, FOUR MESSAGES, ZERO REPLY OF ANY KIND

Target	ElePant, a PEGI 3-rated, Google "Teacher Approved"-badged toddler learning app
Package	com.gamesforkids.toddlers.baby.games.girls.learning.coloring.easy, version 20
Operator	GunjanApps Studios LLP, India
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Austrian DSB, CERT.at, EDPS
Total Outbound Messages	4, across 32 days: privacy@ele-pant.com bounced outright on the first attempt, support@gunjanappstudios.com and info@gunjanappstudios.com accepted delivery for the remaining messages.
Inbound Replies	0. No reply, automated or human, was ever received.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Analysis	5
3	Four Messages, Zero Reply	5
4	Findings	6
4.1	C1: Seventeen Advertising SDKs, Including Two Chinese Networks, in a Toddler App	6
4.2	C2: Three-Way Monetization of Children Presented Under an Educational-Trust Badge	7
4.3	H1: Advertising Identifier Collected Directly From a Child-Directed App	7
5	Data Protection, Article by Article	8

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to GunjanApps Studios LLP that ElePant, a PEGI 3-rated toddler learning app carrying Google's "Teacher Approved" badge, ships seventeen advertising and tracking SDKs in a single binary: ByteDance/Pangle, Mintegral, Meta, AppLovin, ironSource/Supersonic, Vungle, InMobi, Chartboost, Fyber, Tapjoy, Unity Ads, Google Ads, and Firebase among them. Two of these, ByteDance/Pangle and Mintegral, are Chinese-origin networks, meaning children's advertising data routes to infrastructure legally compellable by PRC state authorities, layered on top of the underlying Art. 8 problem that no child in this app's audience can give valid consent to any of it in the first place. RFI-IRFOS holds this finding at HIGH under an explicit blast-radius escalation beyond its computed MEDIUM band.

A second finding names the monetization structure directly: the same toddler audience is monetized three ways simultaneously, in-app purchases ranging from EUR 1.29 to EUR 11.99, the seventeen-network advertising stack, and advertising-identifier collection, all presented under a "Von Pädagogen empfohlen" (Teacher Approved) badge and a PEGI 3 rating that signal safety to a purchasing parent while the underlying code does the opposite. This combination raises an unfair commercial practice question under UCPD 2005/29/EC on top of the data-protection findings.

A third finding names the specific mechanism: ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_TOPICS are all declared, collecting the advertising identifier directly from a child-directed app, the exact practice Art. 8 GDPR and child-data enforcement exist to prevent. Four messages were sent across 32 days; privacy@ele-pant.com bounced outright on the first attempt, and support@gunjanappstudios.com and info@gunjanappstudios.com accepted delivery for the remaining messages, cc'ing the Austrian DSB and CERT.at throughout. Not one reply of any kind was ever received. The 90-day embargo, stated directly to the target in the initial disclosure, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production ElePant Android application (com.gamesforkids.toddlers.baby.games.girls.learning.coloring.easy, version 20, SHA-256 ff1d5c7f054e6148bb6b4756e7d20d2ec0facf223a78b554e9ef1133e568c375), pulled from Google Play and reviewed on 25 June 2026. No account was created and no interaction with any of the seventeen advertising SDKs' backend infrastructure was performed.

Disposition

Three findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Seventeen advertising and tracking SDKs, including two Chinese-origin networks (ByteDance/Pangle, Mintegral), compute to MEDIUM/6.9 on CVSS alone and are held at HIGH under an explicit RFI-IRFOS blast-radius escalation: no child in the app's target audience can give valid consent, and two of the seventeen networks route data to PRC-subject infrastructure. Three-way monetization (paid purchases, advertising SDKs, advertising-ID collection) presented under an educational-trust badge, and advertising-identifier collection from children, both correct to MEDIUM. Four messages were sent across 32 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	Seventeen Advertising SDKs, Including Two Chinese Networks, in a Toddler App
C2	MEDIUM	Three-Way Monetization of Children Presented Under an Educational-Trust Badge
H1	MEDIUM	Advertising Identifier Collected Directly From a Child-Directed App

Subject & Operator Analysis

ElePant is published by GunjanApps Studios LLP, India, and carries both a PEGI 3 rating and Google's "Von Pädagogen empfohlen" (Teacher Approved) badge, both signals of institutional trust presented directly to purchasing parents.

Four Messages, Zero Reply

This case's correspondence record involved one address failure before a working channel was found. `privacy@ele-pant.com` bounced outright on the first attempt. `support@gunjanappstudios.com` and `info@gunjanappstudios.com` accepted delivery for the remaining messages across the following 32 days, cc'ing the Austrian DSB and CERT.at throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Seventeen Advertising SDKs, Including Two Chinese Networks, in a Toddler App

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.

Seventeen advertising and tracking SDKs are present in the binary: ByteDance/Pangle, Mintegral (both Chinese-origin), Meta, AppLovin, ironSource/Supersonic, Vungle, InMobi, Chartboost, Fyber, Tapjoy, Unity Ads, Google Ads, and Firebase. Firebase's auto-init provider runs before any consent screen. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because no child in this app's PEGI 3 target audience can give valid consent under any circumstance, and two of the seventeen networks route data to PRC-subject infrastructure, adding an Art. 44 transfer dimension on top of the underlying Art. 8 problem.

ByteDance/Pangle, Mintegral (mbridge) - Chinese-origin networks
Facebook (Meta), AppLovin, ironSource/Supersonic, Vungle, InMobi
Chartboost, Fyber, Tapjoy, Unity Ads, Google Ads, Firebase (17 total)

Impact: A child using a PEGI 3-rated, Teacher Approved-badged learning app has behavioral advertising data collected by seventeen separate networks, two of which route that data to infrastructure legally compellable by PRC state authorities, with no possibility of valid consent from the data subject.

Fix: Remove the advertising stack entirely for child-directed builds, or implement verifiable parental consent under Art. 8 before any SDK initializes. No confirmation that this has occurred was ever received.

C2: Three-Way Monetization of Children Presented Under an Educational-Trust Badge

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

The same toddler audience is monetized three ways simultaneously: paid in-app purchases (EUR 1.29 to EUR 11.99 per the Play listing), the seventeen-network advertising stack (C1), and advertising-identifier collection (H1), all presented under Google's "Von Pädagogen empfohlen" (Teacher Approved) badge and a PEGI 3 rating.

In-app purchases: EUR 1.29 - EUR 11.99

Badge: "Von Pädagogen empfohlen" (Teacher Approved), Rating: PEGI 3

Impact: A badge and rating that signal safety to a purchasing parent sit directly on top of code that monetizes the same child three separate ways, an unfair commercial practice question under UCPD 2005/29/EC layered on the data-protection findings.

Fix: Either substantiate the Teacher Approved designation by removing the advertising and attribution stack, or remove the badge. No confirmation that this has occurred was ever received.

H1: Advertising Identifier Collected Directly From a Child-Directed App

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.

ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_TOPICS are all declared, collecting the advertising identifier directly from a PEGI 3-rated app.

Impact: Collecting the advertising identifier from a child-directed app is the specific practice Art. 8 GDPR and child-data enforcement priorities exist to address.

Fix: Remove all three Privacy Sandbox advertising permissions unless verifiable parental consent gates their use. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR and consumer-protection provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 8, Art. 6(1), Art. 7, Art. 44	C1	Seventeen advertising SDKs, two Chinese-origin, in a child-directed app.
Art. 8, UCPD 2005/29/EC	C2	Three-way monetization presented under an educational-trust badge.
Art. 8, Art. 5(1)(c)	H1	Advertising identifier collected directly from children.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a

ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1 is held at HIGH under an explicit, stated blast-radius escalation beyond its computed MEDIUM/6.9 band. C2 and H1 correct to MEDIUM on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: ELEPANT-R1.