



Coordinated Security & Privacy Disclosure, Final Report

StoryToys ten-app children's portfolio for Android (LEGO Bluey plus a nine-app licensed portfolio)

One reply covering one of ten licensed children's apps, then eleven weeks of silence on the other nine

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ONE FINDING, TEN APPS, ONE PARTIAL REPLY

Target	StoryToys Limited, Dublin, Ireland
Products audited	LEGO Bluey plus a nine-app licensed children's portfolio (Peppa Pig, Thomas & Friends, Sesame Street Mecha Builders, LEGO DUPLO World, Barbie Coloring, Marvel HQ, Disney Coloring, Hungry Caterpillar Play School, Mother Goose Club)
Disclosure reference	REF STORYTOYS-2026-R1
R1 sent	2026-06-25
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (advertising-identifier collection and pre-consent Firebase initialization on children's apps for under-5s, CVSS v4.0 8.7, portfolio-wide)

Contents

1	Executive Summary	4
2	Subject & Operator Analysis	5
3	Findings	5
3.1	H1: Advertising identifier and ad SDKs, pre-consent Firebase initialization, present across a ten-app children's portfolio	5
4	One Reply Covering One of Ten Apps	6
5	Data Protection, Article by Article	6
6	Disclosure Timeline & Outcome	6
7	Residual Risk & Recommendations	7

Executive Summary

On 25 June 2026, RFI-IRFOS performed static analysis of LEGO Bluey, a StoryToys children's app, and identified a HIGH finding: the ACCESS_AD SERVICES_AD_ID and ACCESS_AD SERVICES_ATTRIBUTION permissions are declared alongside active Google Ads and Unity ad SDKs, and Firebase auto-initializes before any consent screen is reachable, on an app aimed at children under five. StoryToys Support replied once, on 26 June 2026, stating its engineering team could not reproduce the behavior and found no evidence the advertising identifier is collected before consent, and asked RFI-IRFOS to supply runtime network captures as proof.

RFI-IRFOS's position, stated the same day: a manifest permission declaration and an SDK's presence in the compiled binary are static facts that do not require dynamic reproduction to establish, and RFI-IRFOS does not supply the runtime-instrumentation methodology that a paid engagement would cover for free. On 17 July 2026, RFI-IRFOS restated the identical technical pattern as present across a nine-app licensed portfolio spanning LEGO, Mattel, Disney, Sesame Workshop, Marvel, and the Eric Carle estate, all children's titles aimed at under-fives.

Across twelve written notices over eleven weeks, cc'ing the Austrian DSB and the European Data Protection Supervisor, no reply of any kind addressed the nine-app portfolio restatement. The only reply StoryToys ever sent, on 26 June 2026, covered one of ten apps in this case. Three standing questions, whether the pattern is confirmed across all nine portfolio apps, whether each licensor has been notified that their branded app carries this finding, and whether a fix will be made before or after Ireland's Data Protection Commission makes direct contact, were never answered.

Scope: Static analysis of the publicly downloaded production StoryToys Android APKs, on an authorized test device, only. No StoryToys account, backend, or infrastructure was accessed or tested.

Disposition

R1 was sent 25 June 2026 for LEGO Bluey to dataprotection@storytoys.com and support@storytoys.com, bcc the Austrian DSB, CERT.at, and Ireland's DPC. StoryToys Support replied once, the only substantive reply in the entire case, dismissing the finding for that single app as unreproducible. On 17 July 2026, RFI-IRFOS restated the identical finding as present across a nine-app licensed portfolio, Peppa Pig, Thomas & Friends, Sesame Street Mecha Builders, LEGO DUPLO World, Barbie Coloring, Marvel HQ, Disney Coloring, Hungry Caterpillar Play School, and Mother Goose Club. Across twelve written notices over eleven weeks, no reply of any kind addressed the nine-app portfolio.

ID	Severity	Title
H1	HIGH	Advertising identifier and ad SDKs, pre-consent Firebase initialization, present across a ten-app children's portfolio

Subject & Operator Analysis

StoryToys Limited is headquartered in Dublin, Ireland, whose Data Protection Commission is the lead supervisory authority for this case, named throughout the correspondence though not visibly cc'd after the second message.

Findings

H1: Advertising identifier and ad SDKs, pre-consent Firebase initialization, present across a ten-app children's portfolio

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_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION are declared alongside active Google Ads and Unity SDKs. FirebaseInitProvider auto-initializes before any consent screen is reachable. The identical pattern was found in LEGO Bluey and restated as present across nine further licensed titles: Peppa Pig, Thomas & Friends, Sesame Street Mecha Builders, LEGO DUPLO World, Barbie Coloring, Marvel HQ, Disney Coloring, Hungry Caterpillar Play School, and Mother Goose Club, all aimed at children under five.

StoryToys Support's only reply, verbatim, 26 June 2026: "Based on our review, we have not been able to reproduce the reported behaviour. In particular, we found no evidence that the Advertising ID is collected or transmitted prior to user consent. If you have runtime evidence demonstrating collection ... we'd appreciate it if you could share it." This reply addressed LEGO Bluey alone. RFI-IRFOS's rebuttal the same day: a manifest permission declaration and a compiled SDK's presence are static, binary-level facts, not claims requiring dynamic runtime reproduction, and full network-capture methodology is reserved for a paid engagement. No reply of any kind ever addressed the nine-app portfolio restatement sent three weeks later, nor the three standing questions repeated in every subsequent notice.

Impact: An advertising identifier and third-party ad SDKs operate before any consent gate on ten children's apps aimed at under-fives, each carrying a major licensed brand.

Fix: Gate Firebase and all ad-SDK initialization behind a verified parental-consent flow before any network call, across every app in the portfolio, and confirm this fix for each app individually.

One Reply Covering One of Ten Apps

The only substantive reply StoryToys ever sent addressed a single app, LEGO Bluey, and asked for runtime proof of a finding that is verifiable statically. The nine-app portfolio restatement, sent three weeks later and covering major licensed brands including LEGO, Mattel's Barbie, Disney, Sesame Workshop, Marvel, and the Eric Carle estate's Hungry Caterpillar, received no reply of any kind across twelve written notices and eleven weeks. dataprotection@storytoys.com, the primary recipient on every message in this case, never replied at all; the sole reply came from the separate support@storytoys.com address.

Data Protection, Article by Article

Finding	Provision	Concern
H1	GDPR Art. 5(1)(a), Art. 6(1), Art. 7, Art. 8	Advertising-identifier and ad-SDK activity before consent, on children's apps for under-fives

Disclosure Timeline & Outcome

Date	Event
2026-06-25	R1 sent for LEGO Bluey, bcc Austrian DSB/CERT.at/Ireland DPC
2026-06-26	StoryToys Support's only reply, covering LEGO Bluey alone, asks for runtime proof; RFI-IRFOS rebuts the same day
2026-07-17	RFI-IRFOS restates the finding as present across a nine-app portfolio, cc DSB/EDPS visibly
2026-08-05 through 2026-08-31	Four further follow-ups restate the three standing questions; no reply
2026-09-04	Follow-up notes the cc channel to support@storytoys.com now bounces as a policy rejection; primary recipient delivery unaffected
2026-09-12	Final follow-ups restate the chronology and set a sub-deadline for the three questions; no reply
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Confirm, app by app, whether the advertising-identifier and pre-consent Firebase pattern is present in each of the nine portfolio titles.
 - Notify each licensor (LEGO, Mattel, Disney, Sesame Workshop, Marvel, the Eric Carle estate) that their branded app carries this finding.
 - Restore a functioning support@storytoys.com delivery channel; it began rejecting mail from RFI-IRFOS's domain on 4 September 2026.
-

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, 6, 7, 8, 33, 35. REF STORYTOYS-2026-R1.