Coordinated Security & Privacy Disclosure, Final Report

Canva for Android (com.canva.editor)

Cannot-reproduce, disagreement-without-specifics, and a bug-bounty redirect, followed by four written questions about child users' advertising identifiers that a named security contact closed twice without answering

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNRESOLVED, CHILD AD-ID QUESTION NEVER ANSWERED

Target	Canva Pty Ltd, Australia
Product audited	Canva for Android, com.canva.editor, v2.365.0
Disclosure reference	REF CANVA-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C2 Sentry session replay of design canvases, C3 undisclosed Facebook/Segment data pipeline, CVSS v4.0 8.7, both unresolved)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Canva Android application and identified three CRITICAL and three HIGH findings: a hardcoded, never-rotated Firebase API key; Sentry's session-replay module recording and transmitting screen captures of users' in-progress creative work, pitch decks, business plans, client proposals, unreleased mockups, to Sentry's US infrastructure, alongside a hardcoded Sentry auth token giving read access to Canva's own Sentry organization; the complete seven-permission Android Privacy Sandbox stack including Protected Audience (formerly FLEDGE) on-device ad auctions with no identified consent basis; an AppsFlyer local purchase-tracking database whose own backup-exclusion rules are AppsFlyer-controlled rather than Canva's; Braze-based paywall and subscription behavioral profiling timing upgrade offers to individual users; and a Facebook SDK and Segment pipeline routing behavioral events to Meta and Twilio US infrastructure.

Peter, a named Canva Security contact, replied substantively within the first nine days: acknowledging receipt, then stating the findings could not be reproduced, then closing the ticket after RFI-IRFOS supplied three specific grep-verifiable artifacts (the Sentry replay strings, the hardcoded Sentry auth token, and the allowBackup=true manifest flag), stating only 'we do not agree with your assessment of these matters' without naming which artifact was disputed or why, and redirecting RFI-IRFOS to Canva's Bugcrowd bug-bounty program.

From 30 June 2026 onward, RFI-IRFOS made four written requests for a Data Protection Officer or Head of Privacy to respond substantively; none ever did, and the dpo@canva.com address bounced on both occasions it was used. From 15 August 2026 onward, RFI-IRFOS asked three specific yes/no questions concerning advertising-identifier handling for child users, repeated in four separate written notices; Canva's only response was to close the ticket a second time on 19 August, stating 'we have no further feedback on this matter,' without answering any of the three questions. Separately, every delivery attempt to Australia's OAIC, cc'd on this disclosure from 30 June onward, bounced with a recipient-not-found error; RFI-IRFOS records this honestly rather than asserting the regulator was notified.

Scope: Static analysis of the publicly downloaded production Canva Android APK (v2.365.0), on an authorized test device, only. No Canva account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@canva.com, cc security@canva.com and strategic-partnerships@canva.com, bcc the Austrian DSB and CERT.at. A named contact, Peter of Canva Security, replied substantively within the first nine days, disputed the findings without naming a specific artifact, and redirected RFI-IRFOS to Canva's Bugcrowd program. Four written escalations over the following ten weeks, explicitly requesting a Data Protection Officer, never received one. A three-question, four-times-repeated inquiry about advertising-identifier handling for child users was never answered.

ID	Severity	Title
CRITICAL-1	CRITICAL	Hardcoded, never-rotated Firebase API key
CRITICAL-2	CRITICAL	Sentry session replay records users' in-progress creative work; hardcoded Sentry auth token
CRITICAL-3	CRITICAL	Complete Privacy Sandbox / Protected Audience (FLEDGE) permission stack
HIGH-1	HIGH	AppsFlyer local purchase database with AppsFlyer-controlled backup exclusion
HIGH-2	HIGH	Braze paywall and subscription behavioral profiling
HIGH-3	HIGH	Facebook SDK and Segment pipeline route behavioral events to Meta and Twilio

Subject & Operator Analysis

Canva Pty Ltd is headquartered in Australia; the Office of the Australian Information Commissioner (OAIC) is the relevant national regulator. Every delivery attempt to OAIC's enquiries address bounced throughout this case, recorded honestly in the timeline below rather than asserted as a completed notification.

Positive Observations

- A named Canva Security contact, Peter, replied substantively and quickly within the first nine days, faster than the majority of targets in this research series.

Findings

CRITICAL-1: Hardcoded, never-rotated Firebase API key

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

google_api_key AIzaSyDMm3GTaTSqvdV1wBXI2azofQZW6MVfcHs, Firebase project api-72714182225299754 55-514310, ships in the public Play Store binary. The auto-generated project ID suggests the credential was never rotated after initial provisioning.

Peter's 30 June reply stated the findings could not be reproduced; RFI-IRFOS's follow-up supplied the exact strings and asked Canva to "name one artifact, one string, one class, one line" in rebuttal. None was named, for this finding or any other.

Impact: The key allows probing Canva's Firebase project, reading remote configuration such as feature flags and paywall A/B parameters, and potentially exfiltrating push-targeting data.

Fix: Restrict the key to the app's package name and SHA-256 signing fingerprint, rotate it, and audit Firebase Security Rules.

CRITICAL-2: Sentry session replay records users' in-progress creative work; hardcoded Sentry auth token

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

io.sentry.android.replay and io.sentry.android.core.ScreenshotEventProcessor (151 combined smali files) capture visual screen state, in-progress pitch decks, business plans, client proposals, unreleased mockups, and transmit it periodically to Sentry's US infrastructure. A Sentry auth token is separately hardcoded in res/values/strings.xml, granting read access to Canva's own Sentry organization.

This was one of the three specific, named artifacts RFI-IRFOS supplied in its 30 June rebuttal after Peter's "cannot reproduce" reply. Peter's next reply closed the ticket without naming which part of this artifact was disputed.

Impact: Confidential creative work in progress is captured as screen recordings and transmitted to a US third party with no stated legal basis, and a live credential exposes Canva's own crash-reporting organization to read access.

Fix: Disable ScreenshotEventProcessor and the Sentry replay module entirely, or gate it behind explicit consent; remove the hardcoded auth token and rotate it.

CRITICAL-3: Complete Privacy Sandbox / Protected Audience (FLEDGE) permission stack

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

All seven Privacy Sandbox permissions are present, including ACCESS_ADSERVICES_CUSTOM_AUDIENCE (Protected Audience, formerly FLEDGE), which places users into on-device interest groups based on in-app behavior and runs on-device ad auctions using those groups.

No consent basis for Custom Audience membership or on-device auction participation was identified in the binary. Unaddressed by any Canva reply.

Impact: A design tool used for confidential business and creative work runs the full on-device ad-auction stack with no demonstrable consent gate.

Fix: Remove ACCESS_ADSERVICES_CUSTOM_AUDIENCE, and document the legal basis for any remaining Ad Services permissions actually in use.

HIGH-1: AppsFlyer local purchase database with AppsFlyer-controlled backup exclusion

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

res/xml/appsflyer_data_extraction_rules.xml excludes afpurchases.db and AppsFlyer-branded shared preferences from device backup; AppsFlyer itself, not Canva, controls this exclusion rule. Subscription events are routed to AppsFlyer's US attribution infrastructure.

Unaddressed by any Canva reply.

Impact: A third-party attribution vendor controls which of its own local data stores are excluded from backup, and purchase events are exposed to a US processor not named in the privacy policy.

Fix: Audit afpurchases.db retention and consider SKAdNetwork or Privacy Sandbox Attribution as a lower-footprint alternative.

HIGH-2: Braze paywall and subscription behavioral profiling

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

39 of 828 Braze-related smali files reference subscription, premium, paywall, and trial terms. Every paywall encounter, which Pro-only template was blocked, how often the user hits the paywall, trial start and end, is logged to the user's Braze profile to time upgrade offers.

Unaddressed by any Canva reply.

Impact: Differential upgrade offers are timed against individually profiled paywall-friction behavior with no disclosed automated-decision safeguard.

Fix: Gate Braze initialization behind explicit analytics consent, and document the minimum necessary event set collected.

HIGH-3: Facebook SDK and Segment pipeline route behavioral events to Meta and Twilio

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 Facebook SDK (App ID 525265914179580) feeds Meta's advertising graph; Segment acts as a central customer-data pipeline routing behavioral events through Twilio's US infrastructure to downstream destinations including Braze and AppsFlyer.

Unaddressed by any Canva reply.

Impact: Behavioral events from a creative-work platform are routed through two undisclosed US processors to Meta's advertising graph.

Fix: Name Meta Platforms Inc. and Twilio Inc. explicitly as processors in the privacy policy, and document the legal basis for Facebook App Events on this platform.

A Named Contact, Three Deflection Patterns, Two Ticket Closures

Peter's first reply acknowledged the report. His second stated the findings "could not be reproduced," a claim RFI-IRFOS addressed by supplying three specific, grep-verifiable static artifacts, exact strings and file paths for the Sentry replay module, the hardcoded Sentry auth token, and the allowBackup manifest flag, since static findings do not require dynamic reproduction. His third reply disputed the assessment without naming which artifact was wrong, and redirected RFI-IRFOS to Canva's Bugcrowd bug-bounty program. Ten weeks later, after four written requests for a Data Protection Officer and four repetitions of a specific child-advertising-identifier question, Peter closed the ticket a second time: "Canva provided our response to your disclosure on 30 June. We have no further feedback on this matter." The three yes/no questions were never answered in either closure.

The Unanswered Question: Advertising Identifiers and Child Users

From 15 August 2026, RFI-IRFOS asked three specific questions in writing, four separate times: whether the advertising identifier is read for users Canva classifies as children; whether Firebase, Unity, or Google Ads initialize before verifiable parental consent for a child user; and whether Canva will confirm or correct this handling before or after the Australian regulator is in contact about this disclosure. None of the three was ever answered.

Data Protection, Article by Article

Finding	Provision	Concern
CRITICAL-1	GDPR Art. 32(1)	Hardcoded, unrotated credential
CRITICAL-2	GDPR Art. 6(1), Art. 13(1)(e), Art. 46	Undisclosed US screen-recording transfer, exposed org credential
CRITICAL-3	GDPR Art. 6(1)(a), Art. 5(1)(b); TTDSG §25	On-device ad auctions without identified consent basis
HIGH-1	GDPR Art. 13(1)(e), Art. 46	Undisclosed US attribution processor
HIGH-2	GDPR Art. 6(1), Art. 5(1)(c), Art. 22	Individualized paywall-timing profiling
HIGH-3	GDPR Art. 13(1)(e), Art. 46	Undisclosed US advertising and pipeline processors

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@canva.com, cc security@canva.com/strategic-partnerships@canva.com, bcc Austrian DSB/CERT.at, 3 CRITICAL + 3 HIGH findings
2026-06-28/29	Peter (Canva Security) acknowledges, then states the findings cannot be reproduced
2026-06-30	RFI-IRFOS supplies three specific verifiable artifacts; Peter disputes without naming one, redirects to Bugcrowd, closes the ticket
2026-06-30	RFI-IRFOS formally escalates for a DPO reply; delivery to OAIC bounces (first of at least four confirmed bounces)
2026-08-15	RFI-IRFOS first states the three child-advertising-ID questions explicitly
2026-08-19	Peter closes the ticket a second time without answering any of the three questions; cc to dpo@canva.com bounces
2026-09-04	Final follow-up restates chronology and questions; cc to dpo@canva.com bounces again
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Answer the three child-advertising-identifier questions directly, in writing.
- Publish a functioning Data Protection Officer contact address; dpo@canva.com bounced on both occasions it was used.
- Name one specific artifact if any of the six findings is genuinely disputed, rather than a general statement of disagreement.

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, 13, 22, 32, 46; TTDSG §25. REF CANVA-2026-R1.