



Security & Privacy Disclosure, Final Report

KICK for Android (com.kick.mobile)

Fingerprint biometric collection with no Art. 9 basis, a formal legal denial letter that contradicted itself and the binary on three separate points, and gambling-style prediction mechanics running inside a livestreaming app, unresolved through 112 days and a 21-day-overdue embargo

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26
SEPTEMBER 2026, SIX FINDINGS REMAIN UNADDRESSED**

Target	Kick Streaming Pty Ltd (Australia), operator of Stake.com-affiliated livestreaming platform KICK
Package	com.kick.mobile
Platform Audited	Android · v40.23.0, static analysis of the production APK and JS/Hermes bundle
Initial Disclosure (R1)	2026-06-27 (REF com.kick.mobile)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	6 (2 Critical, 3 High, 1 Medium)
Correspondence	9 messages sent by RFI-IRFOS across two threads, 1 formal denial letter received from Kick's legal department on 2026-07-01, 0 further replies since
Authorities BCC'd / CC'd	Austrian Datenschutzbehörde (DSB) · CERT.at · German BfDI · European Data Protection Supervisor (EDPS)

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	6
4.1	C1: Biometric data (USE_BIOMETRIC, USE_FINGERPRINT) collected in a livestreaming app with no Art. 9 legal basis	6
4.2	C2: Firestore integration and a hardcoded Firebase key initialize pre-consent, directly contradicting Kick's own written denial	7
4.3	H1: Expo PedometerModule and DeviceMotionModule track step count and motion in a streaming app, contradicting the operator's own stated justification	7
4.4	H2: SYSTEM_ALERT_WINDOW and RECEIVE_BOOT_COMPLETED grant persistent overlay and boot-launch capability, justified by a technically backwards claim	8
4.5	H3: Pusher and Datadog receive undisclosed US data transfers, alongside undisclosed personalised-advertising profiling	8
4.6	M1: Gambling-style prediction mechanics with a channel-point balance system, and Storybook development tooling left active in production	9
5	Impact Analysis	9
6	The Complete Chain: From a Written Denial to Three Independently Falsified Points	10
7	Data Protection — Article by Article	11
8	Regulatory & Legal Landscape	11
9	Indicators of Compromise	12
10	Disclosure Timeline & Outcome	12
11	Residual Risk & Recommendations	13

Executive Summary

Kick Streaming Pty Ltd operates KICK, a livestreaming platform affiliated with the online gambling brand Stake.com. The Android application (com.kick.mobile, v40.23.0) collects fingerprint biometric data, tracks step count and device motion, and runs a built-in channel-point prediction-and-wagering mechanic structurally similar to a gambling product, inside what presents itself to users as a video-streaming app.

Static analysis identified six findings. The app declares `USE_BIOMETRIC` and `USE_FINGERPRINT` with no documented GDPR Art. 9 legal basis for collecting biometric data in a streaming context. `FirebaseInitProvider` initializes, and a hardcoded Firebase API key sits in the binary, before any consent mechanism can act; the app also integrates Google Firestore, which Kick's own legal department later denied in writing. Expo's `PedometerModule` and `DeviceMotionModule`, tied to the `ACTIVITY_RECOGNITION` permission, track step count and device motion inside a streaming app. `SYSTEM_ALERT_WINDOW` and `RECEIVE_BOOT_COMPLETED` give the app persistent overlay and boot-triggered launch capability. Pusher and Datadog receive user data in undisclosed transfers to US infrastructure, alongside undisclosed personalised-advertising profiling. A built-in gambling-style prediction mechanic with a channel-point balance system runs without the consumer-protection disclosures a gambling-adjacent feature would ordinarily require, and Storybook development tooling was left active in the production binary.

RFI-IRFOS disclosed these findings to privacy@kick.com, security@kick.com, and legal@kick.com on 27 June 2026, BCC the Austrian DSB, CERT.at, and the German BfDI, and followed up with a 72-hour silence sweep on 30 June 2026. On 1 July 2026, Kick's legal department replied with a formal eight-point written denial, asserting the findings were inaccurate or not made out on the facts, with no technical evidence attached. RFI-IRFOS re-verified the production binary directly against the denial rather than accepting it at face value, and found three of the eight points broke on fresh inspection: the letter flatly denied any Firestore use, while a fresh grep of the JS/Hermes bundle found `FirestoreDocumentReference`, `FirestorePersistentCacheIndexManager`, `FirestoreFieldValue`, and `generateFirestoreId` present by name; the letter stated the biometric permission was 'not used' and in the same paragraph described 'reviewing whether the permission can be removed... as a housekeeping measure', a direct self-contradiction; and the letter cited picture-in-picture video as the justification for `SYSTEM_ALERT_WINDOW`, when Android's own PiP API has required no such permission since Android 8. RFI-IRFOS sent this rebuttal the same day, 1 July 2026, naming the pattern and presenting the three confirmed contradictions alongside the weaker remaining points. Kick never replied again. Three further follow-ups, 23 July, 25 August (twice, the second a same-day correction), and 6 September 2026, restated the findings and a set of still-open questions. The stated embargo of 26 September 2026 passed three weeks ago with the case in exactly this state: one formal denial letter, three of its eight points independently falsified against the binary within hours, and silence since.

ID	Severity	Title
C1	CRITICAL	Biometric data (<code>USE_BIOMETRIC</code> , <code>USE_FINGERPRINT</code>) collected in a livestreaming app with no Art. 9 legal basis
C2	CRITICAL	Firestore integration and a hardcoded Firebase key initialize pre-consent, directly contradicting Kick's own written denial

ID	Severity	Title
H1	HIGH	Expo PedometerModule and DeviceMotionModule track step count and motion in a streaming app, contradicting the operator's own stated justification
H2	HIGH	SYSTEM_ALERT_WINDOW and RECEIVE_BOOT_COMPLETED grant persistent overlay and boot-launch capability, justified by a technically backwards claim
H3	HIGH	Pusher and Datadog receive undisclosed US data transfers, alongside undisclosed personalised-advertising profiling
M1	MEDIUM	Gambling-style prediction mechanics with a channel-point balance system, and Storybook development tooling left active in production

Subject & Operator Context

Kick Streaming Pty Ltd (Australia) operates KICK, a livestreaming platform built around gaming, gambling, and general content streaming, affiliated with the online gambling operator Stake.com. The audited application, com.kick.mobile (v40.23.0), is the platform's Android client.

A livestreaming platform affiliated with a gambling operator occupies a position that invites specific scrutiny: biometric authentication, device-motion sensing, and persistent background capability are not features a video-streaming app inherently requires, and a built-in prediction-and-wagering mechanic sitting inside the same app as livestreamed content raises consumer-protection questions that a pure entertainment platform would not. The findings in this report, and the correspondence history around them, concern exactly that combination.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 27 June 2026 to privacy@kick.com, security@kick.com, and legal@kick.com, BCC the Austrian DSB, CERT.at, and the German BfDI. A 72-hour silence sweep followed on 30 June 2026, BCC the DSB and the EDPS.

On 1 July 2026, legal@kick.com sent a formal written reply: an eight-point denial letter, confident in register ('inaccurate', 'not made out on the facts'), with no technical evidence attached to any of the eight points. RFI-IRFOS re-verified the current production binary and JS bundle directly against each point rather than trusting the letter or prior notes, and found three confirmed, independently falsifiable contradictions: Firestore, flatly denied, is present by class name in the bundle; the biometric permission, said to be 'not used', is in the same letter described as under review for 'housekeeping' removal, which does not happen to something genuinely inert; and the `SYSTEM_ALERT_WINDOW` permission, justified by the letter as required for picture-in-picture video, is in fact not required for PiP by Android's own API, which has supported PiP without that permission since Android 8. RFI-IRFOS sent a full technical rebuttal the same day, 1 July 2026, naming this pattern, presenting the three hard contradictions with fresh evidence, and addressing the four weaker points rather than conceding them by silence. Kick's claim that RFI-IRFOS should 'refrain from publishing' was also addressed directly: the KICK ledger entry had been public on rfi-irfos.com since 27 June 2026, before Kick's letter existed.

Kick never replied again. RFI-IRFOS followed up on 23 July 2026 (23 days since the acknowledgment that never continued), 25 August 2026 (twice, the second message a same-day correction to the first), and 6 September 2026 (71 days since the original disclosure, three questions still unanswered). No further message of any kind was received from Kick after the single 1 July denial letter. The stated embargo of 26 September 2026 passed 21 days before this report's publication date.

Findings

C1: Biometric data (USE_BIOMETRIC, USE_FINGERPRINT) collected in a livestreaming app with no Art. 9 legal basis

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — special-category biometric data, blast-radius escalated from HIGH

```
android.permission.USE_BIOMETRIC
android.permission.USE_FINGERPRINT
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL because fingerprint biometric data, Art. 9(1) special-category data, is being collected inside a livestreaming application with no shopping, banking, or security context that would ordinarily justify biometric authentication, with no documented Art. 9(2)(a) consent basis identified during this audit. Kick's own 1 July 2026 denial letter stated the permission was 'not used' while in the same paragraph describing it under review for removal 'as a housekeeping measure', a self-contradiction that does not describe something genuinely inert in the binary.

C2: Firestore integration and a hardcoded Firebase key initialize pre-consent, directly contradicting Kick's own written denial

CRITICAL (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, 5.4) — universal pre-consent data collection the operator denied in writing, blast-radius escalated from MEDIUM

```
assets/index.android.bundle:
  FirestoreDocumentReference, FirestorePersistentCacheIndexManager,
  FirestoreFieldValue, generateFirestoreId
```

Hardcoded key: AIzaSyBt03MQfMaVa2QNnADsIUgT1LB00x7SET0 (Firebase)

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.4 to CRITICAL for two compounding reasons. First, FirebaseInitProvider starts before any consent mechanism can act, meaning Firestore-backed data collection and the hardcoded Firebase key both apply to every single install, unconditionally, the same universal-scope reasoning that applies to pre-consent SDK findings throughout this disclosure series. Second, Kick's legal department flatly denied using Firestore at all in its 1 July 2026 letter; a fresh grep of assets/index.android.bundle the same day found FirestoreDocumentReference, FirestorePersistentCacheIndexManager, FirestoreFieldValue, and generateFirestoreId present by name, a direct factual contradiction of a formal written denial, not an interpretation dispute.

H1: Expo PedometerModule and DeviceMotionModule track step count and motion in a streaming app, contradicting the operator's own stated justification

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1) — motion-sensor tracking the operator's own letter misdescribed, blast-radius escalated from MEDIUM

```
android.permission.ACTIVITY_RECOGNITION
PedometerModule.kt -- step-count tracking, Expo
DeviceMotionModule -- device motion tracking, Expo
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because Kick's 1 July 2026 denial letter specifically claimed the ACTIVITY_RECOGNITION-linked functionality served 'device-orientation purposes only'. A dedicated PedometerModule.kt class and a separate DeviceMotionModule are both present in the production binary; orientation sensing alone never requires ACTIVITY_RECOGNITION or step-count tracking. The written misdescription of a specific, checkable technical fact to a disclosure recipient is treated here as materially more serious than the underlying sensor access alone would be.

H2: SYSTEM_ALERT_WINDOW and RECEIVE_BOOT_COMPLETED grant persistent overlay and boot-launch capability, justified by a technically backwards claim

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 5.5)
 — overlay and persistence permissions the operator's own PiP justification does not require, blast-radius escalated from MEDIUM

```
android.permission.SYSTEM_ALERT_WINDOW
android.permission.RECEIVE_BOOT_COMPLETED
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.5 to HIGH because Kick's 1 July 2026 denial letter cited picture-in-picture video playback as the justification for SYSTEM_ALERT_WINDOW. Android's native PiP API, `enterPictureInPictureMode()`, has not required SYSTEM_ALERT_WINDOW since Android 8; the API was built specifically so apps do not need that permission. The stated justification is backwards, and combined with RECEIVE_BOOT_COMPLETED, the app retains the technical capability for a persistent, boot-triggered overlay beyond what any disclosed feature requires.

H3: Pusher and Datadog receive undisclosed US data transfers, alongside undisclosed personalised-advertising profiling

HIGH (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, 7.0)
 — undisclosed third-party data recipients and cross-border transfers

```
Pusher    -- real-time data transfer, US infrastructure
Datadog   -- application monitoring/telemetry, US infrastructure
```

Impact: Pusher and Datadog, both US-based infrastructure providers, receive user data from the application in transfers not identified as disclosed Art. 13(1)(e) data recipients in Kick's available privacy documentation, engaging Art. 44 cross-border transfer requirements. Undisclosed personalised-advertising profiling was identified alongside these transfers during this audit, compounding the transparency gap rather than standing as an isolated finding.

M1: Gambling-style prediction mechanics with a channel-point balance system, and Storybook development tooling left active in production

MEDIUM (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0) — undisclosed gambling-adjacent mechanic and residual dev tooling

```
Channel-point balance / prediction mechanic -- gambling-adjacent,
no consumer-protection disclosure identified
Storybook -- development/component-preview tooling present in
production binary
```

Impact: A built-in prediction mechanic with a channel-point balance system, structurally similar to a wagering feature, runs inside the application without the kind of consumer-protection framing a gambling-adjacent feature on a platform affiliated with Stake.com would ordinarily carry. Separately, Storybook development and component-preview tooling was identified active in the production binary, residual dev infrastructure that should not ship to end users. Neither finding reaches the severity of C1, C2, or the HIGH findings above; both are included because they were confirmed present and not addressed in any of Kick's correspondence.

Impact Analysis

C1 and C2 describe an application that collects special-category biometric data with no documented basis and runs a cloud-backed data pipeline (Firestore, Firebase) before any consent mechanism can act, both findings on an app with no functional need for either. What sets this case apart from most others in this disclosure series is not the underlying technical findings alone but Kick's own response to them: a formal legal denial letter that, on fresh re-inspection the same day, contradicted itself on the biometric point and was independently falsified on the Firestore and SYSTEM_ALERT_WINDOW points by direct evidence from the production binary and Android's own public API documentation.

H1 through H3 each have the same shape: either a written claim from Kick that the binary does not support (H1, H2), or a data flow absent from Kick's own disclosures entirely (H3). M1 is the weakest finding, a consumer-protection and hygiene gap rather than a GDPR Art. 9/Art. 32 issue, but it is included because it, too, went unaddressed across every message in this correspondence.

The Complete Chain: From a Written Denial to Three Independently Falsified Points

Step 1 — Disclosure: RFI-IRFOS sends the original findings (C1-C2, H1-H3, M1) to privacy@kick.com, security@kick.com, and legal@kick.com on 27 June 2026.

Step 2 — Silence, then a formal denial: After a 72-hour silence sweep on 30 June 2026, Kick's legal department replies on 1 July 2026 with an eight-point denial letter, confident in register, no evidence attached.

Step 3 — Re-verification, not acceptance: Rather than treat a confident legal-register denial as authoritative, RFI-IRFOS re-pulls the current production APK and re-runs static analysis against the binary the same day.

Step 4 — Three contradictions surface: The Firestore denial is contradicted by four Firestore class names present in `assets/index.android.bundle`. The biometric 'not used' claim is contradicted by the same letter's own description of a pending 'housekeeping' removal. The `SYSTEM_ALERT_WINDOW` PiP justification is contradicted by Android's own public API documentation, which has not required that permission for PiP since Android 8.

Step 5 — Rebuttal, same day: RFI-IRFOS sends a full technical rebuttal on 1 July 2026 naming the pattern and presenting all three contradictions with fresh evidence, alongside the four weaker points addressed rather than conceded.

Step 6 — Silence resumes: Kick never replies again. Three further follow-ups (23 July, 25 August twice, 6 September 2026) restate the findings and the still-open questions. The embargo of 26 September 2026 passes with the case in exactly this state.

The chain illustrates a pattern distinct from simple non-response: an operator did engage, in writing, through counsel, and the engagement did not survive contact with the operator's own production binary.

Data Protection — Article by Article

Art. 9(1)/Art. 9(2)(a) GDPR — Special categories of data: C1's fingerprint biometric collection in a livestreaming context lacks a documented Art. 9(2)(a) consent basis.

Art. 7(1) GDPR — Conditions for consent: C2's Firestore and Firebase initialization via FirebaseInitProvider starts before any consent mechanism can act, for every install.

Art. 32 GDPR — Security of processing: C2's hardcoded Firebase key and H2's unjustified SYSTEM_ALERT_WINDOW/RECEIVE_BOOT_COMPLETED combination both fall short of the technical security measures Art. 32 requires.

Art. 5(1)(b)/(c) GDPR — Purpose limitation and data minimisation: H1's step-count and motion tracking in a streaming app, and H2's overlay/boot-persistence capability, both exceed what streaming functionality requires.

Art. 13(1)(e) GDPR — Transparency, recipients of data: H3's Pusher and Datadog data transfers were not identified as disclosed recipients in Kick's available privacy documentation.

Art. 44 GDPR — Transfers to third countries: H3's transfers to Pusher and Datadog, both US infrastructure, engage Art. 44 transfer-mechanism requirements.

Art. 13(1)(c) GDPR — Transparency, purpose of processing: M1's gambling-adjacent prediction mechanic is not accompanied by a stated purpose or consumer-protection framing in documentation reviewed for this audit.

Regulatory & Legal Landscape

Kick Streaming Pty Ltd is an Australian company; RFI-IRFOS BCC'd and later openly CC'd the Austrian DSB, CERT.at, the German BfDI, and the European Data Protection Supervisor throughout this correspondence as the relevant authorities under Art. 3(2) extraterritorial scope for Kick's EU-resident users, given Kick's EU-facing livestreaming and Stake.com-affiliated operations.

Fine exposure under GDPR, to the extent EU-resident users are processed under Art. 3(2): Art. 83(5) applies to the Art. 9 special-category violation in C1, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 5, 7, 13, 32, and 44 issues in C2 and H1-H3, up to EUR 10,000,000 or 2% of total worldwide annual turnover. A formal written denial that does not survive same-day technical re-verification is, separately from the fine exposure itself, a material fact relevant to any regulator assessing Kick's good faith in this correspondence.

Indicators of Compromise

The following identifiers and class names were extracted from the production APK and JS/Hermes bundle (v40.23.0) via static analysis only, including a same-day re-verification pass on 1 July 2026 against Kick's own written denial. No Kick servers, accounts, or infrastructure were probed.

```
C1 -- android.permission.USE_BIOMETRIC, USE_FINGERPRINT

C2 -- assets/index.android.bundle: FirestoreDocumentReference,
    FirestorePersistentCacheIndexManager, FirestoreFieldValue,
    generateFirestoreId
    Hardcoded key: AIzaSyBt03MQfMaVa2QNnADsIUgTILB00x7SET0

H1 -- android.permission.ACTIVITY_RECOGNITION
    PedometerModule.kt, DeviceMotionModule

H2 -- android.permission.SYSTEM_ALERT_WINDOW, RECEIVE_BOOT_COMPLETED

H3 -- Pusher, Datadog (US infrastructure, undisclosed recipients)
```

Disclosure Timeline & Outcome

2026-06-27 Initial disclosure sent to privacy@kick.com, security@kick.com, legal@kick.com. BCC: Austrian DSB, CERT.at, German BfDI.

2026-06-30 72-hour silence sweep sent to the same three recipients, BCC DSB and EDPS.

2026-07-01 12:24 UTC legal@kick.com sends a formal eight-point written denial letter, no technical evidence attached.

2026-07-01 12:42-12:53 UTC RFI-IRFOS re-verifies the production binary directly against the denial, finds three confirmed contradictions (Firestore, biometric self-contradiction, PiP justification), and sends a full technical rebuttal the same day.

2026-07-23 Follow-up, 23 days since the acknowledgment that never continued.

2026-08-25 Two follow-ups (the second a same-day correction to the first), restating the unanswered contradictions.

2026-09-06 Follow-up, 71 days since the original disclosure, three questions still open.

2026-09-26 Stated embargo date reached. No further message of any kind received from Kick since the single 1 July 2026 denial letter.

2026-10-17 This report published, 21 days after the embargo date. All six findings confirmed unaddressed on the basis of the correspondence record; no re-verification download was performed beyond the 1 July 2026 pass for this report.

Residual Risk & Recommendations

C1 — Immediate: Document a specific, proportionate purpose and an Art. 9(2)(a) consent basis for biometric data collection in a livestreaming context, or remove the USE_BIOMETRIC/USE_FINGERPRINT permissions if no such purpose exists.

C2 — Immediate: Rotate the hardcoded Firebase key. Reorder Firestore and Firebase initialization to occur after a consent signal, not before. Correct the public record: the 1 July 2026 denial letter's Firestore claim does not match the current production binary and should be formally corrected with Kick's own regulator contacts.

H1 — Governance: Scope ACTIVITY_RECOGNITION-linked functionality to an actual disclosed feature, or remove it; correct the prior written claim that it serves 'device-orientation purposes only.'

H2 — Governance: Remove SYSTEM_ALERT_WINDOW if picture-in-picture is the only intended use case, since Android's native PiP API does not require it; audit RECEIVE_BOOT_COMPLETED for the same question.

H3 — Transparency: Disclose Pusher and Datadog as named Art. 13(1)(e) data recipients, document the Art. 44 transfer mechanism relied on for both, and disclose the personalised-advertising profiling identified during this audit.

M1 — Consumer protection: Apply responsible-gambling-style disclosure framing to the channel-point prediction mechanic consistent with Kick's affiliation with a licensed gambling operator. Remove Storybook development tooling from the production build pipeline.

Across all findings: when a disclosure recipient's legal counsel issues a formal written denial, verify it does not contain internally self-contradictory language and does not conflict with the recipient's own public API documentation before relying on it, the same standard RFI-IRFOS applied in reverse when it re-verified Kick's own denial within hours of receiving it.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis of

the published application and its JS/Hermes bundle using publicly available tooling, including a same-day re-verification pass on 2026-07-01 against Kick's own written denial letter. No Kick servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF KICK-2026.