Coordinated Security & Privacy Disclosure, Final Report

King Portfolio, 12 apps (com.king.*)

King.com Ltd, a subsidiary of Activision Blizzard, ultimately controlled by Microsoft Corporation (NASDAQ: MSFT)

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 92 DAYS AFTER DISCLOSURE, TEN AUTOMATED REPLIES, ZERO FINDINGS EVER NAMED

Target	King portfolio, 12 Android game apps under com.king.* and com.midasplayer.*, all PEGI 3, collectively over 3 billion downloads
Package	com.king.candycrushsaga and 11 further titles
Operator	King.com Ltd, subsidiary of Activision Blizzard, ultimate controller Microsoft Corporation (NASDAQ: MSFT) since the October 2023 acquisition
Initial Disclosure	2026-06-24
Original Embargo	2026-09-20 (90 days from disclosure)
Report Published	2026-09-24, four days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Austrian DSB, German BfDI, UK ICO (delivery to ICO blocked by a Microsoft-side mail flow rule)
Total Outbound Messages	8, across 92 days
Inbound Replies	10, all identical automated Player Support acknowledgments from replyto.kcare@king.com. Zero human reply from privacy, legal, or DPO at any point.

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 disclosed to King.com that its entire 12-title Android portfolio, all rated PEGI 3 and collectively downloaded over 3 billion times, ships AppLovin MAX behavioral ad mediation with the SDK's own purpose-built age-restriction signal, setIsAgeRestrictedUser(), declared in the binary but never invoked with the value true anywhere in the application. 235 separate COPPA-related string references in the same binary confirm King's own codebase already documents its awareness of the child audience. The same portfolio ships a proprietary cross-app identifier SDK that fires at every device boot and aggregates a child's behavioral activity across all 12 games into one unified profile, undisclosed in any of the twelve apps' privacy notices, and an IAB Open Measurement SDK carrying the literal string "Microsoft Corporation CMP," identifying Microsoft's own consent-management platform as the entity presenting a consent dialog to children as young as three, a mechanism that cannot meet GDPR Art. 8's requirement of parental authorization.

Three further HIGH findings: Braze behavioral-marketing infrastructure (1,607 smali classes, including a geofence manager present in the binary though its own string literals indicate it is not currently active), twelve separately hardcoded Firebase API keys, one per app, and a legacy cleartext-HTTP exception for King's original midasplayer.com domain, still present in the network security configuration of every current app.

Across 92 days and eight outbound messages, King's Player Support inbox returned the identical automated acknowledgment ten separate times, the same template, word for word, regardless of escalation to legal@king.com, dpo@king.com, and privacy@activision.com. No human respondent from privacy, legal, or the DPO function ever replied. No finding, of the six disclosed, was ever named, disputed, or confirmed fixed.

All six findings were re-scored under CVSS v4.0 for this closure report, not carried forward with the original hand-assigned labels. C1, the AppLovin age-restriction finding, independently carries a CVSS v4.0 base of MEDIUM, 6.9, and is held at CRITICAL in this report under an explicit blast-radius escalation, documented in the finding itself, for a documented, deliberate choice affecting a PEGI 3 child audience at a scale of over 3 billion downloads. C2 and C3 are held at HIGH under the same reasoning. H1, H2, and H3 are corrected down to MEDIUM, matching their own CVSS v4.0 bands honestly.

Scope: Root-level static analysis of the production King Android applications (com.king.* and com.midasplayer.*, 12 titles, representative sampling against com.king.candycrushsaga), covering the AndroidManifest, resource strings, and decompiled dex, as pulled and reviewed on 24 June 2026. No dynamic instrumentation, live traffic capture, or interaction with King's, Activision's, or Microsoft's backend infrastructure was performed. RFI-IRFOS was unable to pull a fresh production build for this closure report and does not claim to know whether the six findings still hold against the current Google Play builds, that gap is stated here explicitly, it is not assumed either way.

Disposition

Six findings were disclosed on 24 June 2026 covering all 12 King titles: three CRITICAL (AppLovin MAX behavioral ad profiling running unrestricted on PEGI 3 children's games because a purpose-built age-restriction API exists in the binary and is deliberately never invoked with true, a cross-app behavioral graph unifying a child's activity across all 12 games via a boot-triggered ContentProvider, and a Microsoft-operated consent management platform collecting purported consent from children as young as three) and three HIGH (undisclosed Braze behavioral marketing infrastructure, twelve separately hardcoded Firebase API keys, and a legacy cleartext domain exception). Eight messages were sent across 92 days. Every one of the ten inbound replies was the identical automated Player Support template. No human at King, Activision, or Microsoft ever engaged with a single finding. This report closes and publishes the case on the terms disclosed from the first message.

ID	Severity	Title
C1	CRITICAL	AppLovin MAX Behavioral Ad Profiling Runs Unrestricted on PEGI 3 Children's Games, a Documented Choice, Not an Oversight
C2	HIGH	Cross-App Behavioral Graph Unifies a Child's Profile Across All 12 Games, Undisclosed
C3	HIGH	A Microsoft-Operated Consent Management Platform Collects Purported Consent From Three-Year-Olds
H1	MEDIUM	Braze Behavioral Marketing Infrastructure on Children's Games, Including a Deployed Geofence Manager
H2	MEDIUM	Twelve Separately Hardcoded Firebase API Keys, One Per App
H3	MEDIUM	Legacy Cleartext Exception for midasplayer.com, No TLS Enforcement

Subject & Operator Analysis

The King portfolio, 12 Android titles including Candy Crush Saga (over 3 billion downloads alone), is operated by King.com Ltd, a subsidiary of Activision Blizzard, ultimately controlled by Microsoft Corporation since the October 2023, $68.7 billion acquisition. All 12 apps are rated PEGI 3. King maintains a Player Support intake (replyto.kcare@king.com) that responded to every message in this case with the identical automated acknowledgment template, regardless of the content, escalation, or CC list of the message it was replying to.

Several genuine positives are worth naming: the games are technically polished and reliably performant, with no PRC SDK dependencies, no cleartext global network configuration, and no biometric processors identified. The issues documented here sit at the ad-mediation and analytics layer, not in the game engine, and are fixable without touching gameplay code.

Architecture & Data Flow

All 12 King apps compile AppLovin MAX with its child-safety signal left uninvoked, a proprietary cross-app identifier SDK that fires at device boot and aggregates behavioral data across the entire portfolio, and an IAB Open Measurement SDK operating Microsoft's own consent-management platform for an audience below the age GDPR requires parental authorization for. Braze behavioral-marketing infrastructure, twelve separately hardcoded Firebase keys, and a legacy cleartext domain exception sit alongside these three core findings.

Findings

C1: AppLovin MAX Behavioral Ad Profiling Runs Unrestricted on PEGI 3 Children's Games, a Documented Choice, Not an Oversight

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because this is a documented, deliberate choice, the age-restriction API exists in the binary and is simply never invoked, affecting a PEGI 3 child audience at a scale of over 3 billion downloads across the portfolio.

Every King app ships AppLovin MAX, a full ad-mediation platform aggregating multiple ad networks and building behavioral profiles. AppLovin's SDK exposes setIsAgeRestrictedUser(), purpose-built to signal a child audience and disable behavioral profiling. Across the King portfolio this method is declared as an interface but never called with the value true anywhere in the application. AppLovin MAX therefore runs in default, full behavioral-profiling mode on games whose own Play Store rating designates them appropriate for children aged 3 and above. 235 separate COPPA-related string references in the same binary confirm King's own codebase already documents its awareness of the child audience, the presence of the API alongside its non-invocation is not an oversight. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because this is a documented, deliberate choice affecting a PEGI 3 child audience at a scale of over 3 billion downloads across the portfolio.

```
com.king.candycrushsaga (representative sample):
1,278 AppLovin smali classes
com/applovin/mediation, com/applovin/adview, com/applovin/sdk,
com/applovin/impl/privacy/consentFlow/TermsAndPrivacyPolicyFlowSettingsImpl

.method public abstract isAgeRestrictedUser()Ljava/lang/Boolean;
# No call to setIsAgeRestrictedUser(true) found anywhere in the binary.
# 235 COPPA references present in smali.
```

Impact: Behavioral advertising profiles are built on children as young as three, at a scale of over 3 billion downloads across the twelve-app portfolio, using a mechanism the SDK vendor built specifically to prevent this, left unused.

Fix: Call setIsAgeRestrictedUser(true) across all 12 apps, or migrate to a child-directed ad configuration verified by AppLovin. No confirmation that this has occurred was ever received.

C2: Cross-App Behavioral Graph Unifies a Child's Profile Across All 12 Games, Undisclosed

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the mechanism fires at every device boot, before any app is opened, and aggregates a child's behavioral data across all 12 titles into one profile with no disclosure in any of the twelve apps' privacy notices.

Every King app ships com.king.usdk.kdid, King's proprietary cross-device identifier SDK, registering a signature-level ContentProvider (com.king.cross.kingapp.provider.ACCESS) that lets all 12 King apps on a device share behavioral data with each other. Three intent actions are registered, including com.king.analytics.BOOT_COMPLETED, which fires at every device reboot, before any user opens any King app. A child who plays several King titles on the same device has their activity aggregated into a single cross-game profile. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the mechanism fires at every device boot and aggregates a child's behavioral data across all 12 titles into one profile with no disclosure in any privacy notice.

```
AndroidManifest.xml, present in all 12 com.king.* apps:
<permission android:name="com.king.cross.kingapp.provider.ACCESS" android:
    protectionLevel="signature"/>
<action android:name="com.king.analytics.BOOT_COMPLETED"/>
<action android:name="com.king.analytics.REQUEST_VALUE"/>
<action android:name="com.king.analytics.RECEIVE_VALUE"/>
```

Impact: A child's activity across multiple games becomes one unified behavioral profile without any user, or parent, ever being told this cross-app aggregation happens.

Fix: Disclose the cross-app identifier mechanism explicitly in each app's privacy notice, and gate BOOT_COMPLETED-triggered profile aggregation behind a documented, opt-in consent mechanism. No confirmation that this has occurred was ever received.

C3: A Microsoft-Operated Consent Management Platform Collects Purported Consent From Three-Year-Olds

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the entity operating the mechanism is Microsoft Corporation, the ultimate controller of the portfolio, and the population affected is PEGI 3 children below the age GDPR Art. 8 requires parental authorization for.

The binary ships the IAB Open Measurement SDK under the namespace com.iab.omid.library.activision and contains the literal string "Microsoft Corporation CMP", identifying Microsoft's own consent-management platform as the entity controlling consent collection. GDPR Art. 8 requires that consent for processing a child's data be given or authorized by the holder of parental responsibility, a CMP dialog presented directly to a three-year-old does not meet that standard. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the entity operating the mechanism is Microsoft Corporation, the ultimate controller of the portfolio, and the population affected is PEGI 3 children below the age GDPR Art. 8 requires parental authorization for.

```
const-string p0, "Microsoft Corporation CMP"
.class public final Lcom/iab/omid/library/activision/utils/b;
# IAB Open Measurement SDK registered under the Activision namespace
```

Impact: Microsoft, as the ultimate controller of the King portfolio, operates a consent-collection mechanism for a population that cannot legally provide the consent it purports to collect.

Fix: Replace the direct-to-child consent flow with a verified parental-authorization mechanism meeting GDPR Art. 8, across the full portfolio. No confirmation that this has occurred was ever received.

H1: Braze Behavioral Marketing Infrastructure on Children's Games, Including a Deployed Geofence Manager

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. Corrected from the original HIGH label under CVSS v4.0.

Braze is present across the King portfolio, 1,607 smali classes in com.king.candycrushsaga alone, including BrazeGeofenceManager. Braze builds individual behavioral profiles for push notification targeting and engagement optimization. Its own string literals in the binary indicate the geofence capability is present but not currently enabled, the infrastructure is deployed and could be activated remotely without a Play Store update, but is not demonstrated as active today.

Impact: Behavioral marketing infrastructure, including a remotely activatable geofencing capability, is present on a children's platform without documented parental consent, though not confirmed active.

Fix: Disclose the Braze integration explicitly, including the dormant geofence capability, and require a consent gate before any future remote activation. No confirmation that this has occurred was ever received.

H2: Twelve Separately Hardcoded Firebase API Keys, One Per App

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9. Corrected from the original HIGH label under CVSS v4.0.

Every King app ships a unique hardcoded Firebase API key. "It's just a public key" is an incomplete answer in three specific ways: a key is only safe if the project's Security Rules are correctly configured, and misconfiguration is the most common cause of real Firebase data breaches; the same key drives FCM push delivery, so twelve hardcoded keys represent twelve separate unauthenticated push-spoofing vectors directed at a child audience; and Firebase Remote Config, if not scope-restricted, allows server-side behavior changes, potentially including the same AppLovin age-restriction flag from C1, without any Play Store review.

```
12 unique Firebase API keys, one per King app, e.g.:
com.king.candycrushsaga: AIzaSyBVVfgVyT0ic2T82BM1Rub6BCs3Cekj5rU
com.king.farmheroessaga: AIzaSyBHnsVrBQHcpFaPXgxavpbzQq1gEsnZ7eY
+ 10 further keys, one per remaining title
```

Impact: Twelve independent Firebase projects each carry the standard hardcoded-key risk class, quota exhaustion, unauthenticated push notification spoofing to a child audience, and potential Remote Config manipulation, none individually confirmed exploited.

Fix: Confirm Security Rules and App Check enforcement individually across all twelve projects, or rotate and restrict each key. No confirmation that this has occurred was ever received.

H3: Legacy Cleartext Exception for midasplayer.com, No TLS Enforcement

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.3. Corrected from the original HIGH label under CVSS v4.0, exploitation requires network-adjacent position, not a remote path.

The network security configuration permits cleartext HTTP to midasplayer.com and midasplayer.cloud, King's original domain name from before its 2011 rebrand, present as a cleartext exception in every current app. Traffic to these endpoints travels without TLS protection, a network-adjacent interception surface on a children's platform.

```
res/xml/network_security_config.xml (com.king.candycrushsaga):
<domain-config cleartextTrafficPermitted="true">
  <domain includeSubdomains="true">midasplayer.com</domain>
  <domain includeSubdomains="true">midasplayer.cloud</domain>
</domain-config>
```

Impact: A legacy domain exception leaves a real, if network-adjacent, interception surface open on every current King app, over a decade after the underlying rebrand.

Fix: Remove the cleartext exception for midasplayer.com and midasplayer.cloud, or migrate any remaining traffic to those endpoints to TLS. No confirmation that this has occurred was ever received.

Impact Analysis

C1 through C3 compound, they do not sit side by side as isolated issues: C1 establishes that behavioral profiling runs unrestricted on a PEGI 3 audience by deliberate design, C2 shows that profile is not confined to a single app but unified across the entire portfolio a child might play on one device, and C3 shows the consent mechanism meant to authorize any of this is operated by the ultimate parent company, Microsoft, in a form that cannot legally authorize it for the age group actually playing.

Ten Identical Replies, Pattern P-01 Family

This case's correspondence pattern is a clean instance of the automated-support-deflectio n family documented in the RFI-IRFOS Corporate Response Pattern Atlas v0.1: ten inbound replies across the case, every one the identical Player Support template ("Thanks for your message.. We've received it and will get back in touch soon"), regardless of whether the outbound message was the original disclosure, an escalation naming legal@king.com and dpo@king.com directly, or a message stating plainly that the automated acknowledgment does not constitute engagement. No human respondent from privacy, legal, or the DPO function replied at any point across 92 days.

Data Protection, Article by Article

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

Article	Finding	Basis
Art. 6, Art. 8	C1	Behavioral advertising processing on children's data with no valid legal basis, the vendor's own age-restriction signal left uninvoked.
Art. 5(1)(b), Art. 13	C2	Cross-app data aggregation constitutes a new processing purpose, undisclosed in any privacy notice.
Art. 8	C3	Consent for processing a child's data requires parental authorization; a CMP dialog to a three-year-old does not meet this standard.
Art. 6, Art. 8	H1	Deployed behavioral-marketing infrastructure targeting children without documented consent.
Art. 32	H2	Security of processing for twelve hardcoded, unrotated project credentials.
Art. 32	H3	Security of processing, cleartext transport on a legacy domain exception.

Regulatory & Legal Landscape

Microsoft Corporation is the ultimate data controller of the King portfolio via the Activision Blizzard acquisition, and GDPR Art. 3(2) applies to it as a US entity offering services to EU data subjects. Art. 83(4) penalties for Art. 8 violations reach EUR 10 million or 2% of global annual turnover, against Microsoft's scale that places the upper penalty ceiling in the billions of euros. The Austrian DSB and German BfDI were held in BCC across this case's correspondence; delivery to the UK ICO's casework address was blocked outright by a Microsoft-side mail flow rule (indigoffice.onmicrosoft.com), an organizational block on the regulator's own inbox receiving a formal disclosure addressed to it.

IOC / Reproducible Evidence

```
Representative package: com.king.candycrushsaga
C1: com.applovin.* (1,278 smali classes), setIsAgeRestrictedUser() never invoked with
    true
C2: com.king.usdk.kdid, com.king.cross.kingapp.provider.ACCESS, BOOT_COMPLETED
C3: com.iab.omid.library.activision, string "Microsoft Corporation CMP"
H1: com.braze.* (1,607 smali classes), BrazeGeofenceManager
H2: 12 unique Firebase API keys, one per app (res/values/strings.xml)
H3: network_security_config.xml, cleartextTrafficPermitted for midasplayer.com/.cloud
```

No fresh production build was pulled for this closure report. RFI-IRFOS does not claim to know whether the current Google Play builds still match the build reviewed on 24 June 2026, and states that gap explicitly instead of assuming continuity.

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to privacy@king.com, cc privacy@activision.com, bcc DSB/BfDI/ICO (ICO delivery blocked). Six findings, 90-day embargo set for 2026-09-20.
2026-06-24 through 2026-09-06	Seven further outbound messages, escalating to legal@king.com and dpo@king.com directly. Every inbound reply, ten in total, was the identical automated Player Support template.
2026-09-20	Original 90-day embargo elapses. No human reply had ever been received.
2026-09-24	Case closed and published, four days after embargo, on the terms stated from the first message.

Eight outbound messages, ten identical automated acknowledgments, zero human replies, zero findings named, across 92 days.

Residual Risk & Recommendations

All six findings remain unconfirmed as fixed at the time of publication, because no human at King, Activision, or Microsoft ever engaged with any of them. RFI-IRFOS recommends, in order of urgency: invoke setIsAgeRestrictedUser(true) across the portfolio (C1); disclose and consent-gate the cross-app identifier mechanism (C2); replace the direct-to-child CMP flow with verified parental authorization (C3); consent-gate the Braze geofence capability before any activation (H1); confirm Security Rules and App Check across all twelve Firebase projects (H2); and remove the legacy cleartext domain exception (H3). Weekly monitoring of the public builds continues after this publication; any change to any of the six findings will be documented and added to the public record.

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 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, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. Any such escalation is always stated explicitly in the finding itself, never left implicit, as C1, C2, and C3 are escalated and H1, H2, and H3 are corrected down in this report. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF RFI-2026-KI-001.