Coordinated Privacy Disclosure, Final Report

Subway Surfers (com.kiloo.subwaysurf)

SYBO Games ApS, Copenhagen, Denmark; owned by Miniclip SA (Geneva) and Krafton Inc. (South Korea)

TICKET-SYSTEM DEFLECT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 92 DAYS AFTER DISCLOSURE, THIRTEEN MESSAGES, SIX IDENTICAL AUTO-REPLIES, ZERO SUBSTANTIVE REPLY

Target	Subway Surfers, over 3.5 billion downloads, one of the most-downloaded mobile games in history
Package	com.kiloo.subwaysurf
Operator	SYBO Games ApS, Copenhagen, Denmark; owned by Miniclip SA (Geneva, Switzerland), ultimately Krafton Inc. (South Korea)
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Danish Datatilsynet (lead SA), Austrian DSB, CERT.at
Total Outbound Messages	13, across 92 days, primarily to privacy@sybogames.com
Inbound Replies	6, every one the identical automated ticket-system acknowledgment (”Hey Surfer, this is just to let you know that we’ve received your request”), each issued under a new, unrelated conversation ID, not a continuation of the existing thread. Zero substantive replies were ever received.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to SYBO Games ApS that Subway Surfers, downloaded more than 3.5 billion times, ships six advertising and analytics SDK ContentProviders that all initialize before any consent screen can appear, the largest such stack RFI-IRFOS has documented across this audit series. The Moloco SDK's AndroidX Startup initOrder is set to 2147483648, Java's Integer.MAX_VALUE, a deliberate engineering choice to guarantee it fires in absolute first position ahead of every other ContentProvider in the binary, including AppLovin's own consent-management-platform state machine, which is present in the app but initializes too late to gate anything.

The mediation stack includes Mintegral/MBridge, a subsidiary of Mobvista Inc., operationally headquartered in Guangzhou and subject to compelled-disclosure obligations under China's National Security Law Art. 7, alongside nine further ad networks, ten-plus independent processors in total. Separately, the binary bundles SuperAwesome, the leading COPPA-compliant kids advertising platform, as a mediation adapter, evidence that SYBO's own infrastructure is configured with awareness of a child audience, while the same binary simultaneously applies a full adult behavioral-targeting stack, including all four Android Privacy Sandbox permissions, to that same audience.

Thirteen messages were sent to privacy@sybogames.com across 92 days, cc'ing press@sybogames.com and press@miniclip.com. Six drew the identical automated ticket-system acknowledgment, 'Hey Surfer, this is just to let you know that we've received your request,' each one issued under a new, unrelated conversation ID, not a continuation of the existing thread. Not one substantive reply was ever received. The 90-day embargo, set at first contact, 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 Subway Surfers Android application (com.kiloo.subwaysurf, version 3.65.0, versionCode 92515, 216.6 MB, Unity engine), as pulled via ADB and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with SYBO's or any mediation partner's backend infrastructure was performed.

Disposition

Six findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Six simultaneous pre-consent advertising and analytics SDK initializations, the largest such stack RFI-IRFOS has recorded in this audit series, with the Moloco SDK's initOrder literally set to Java's Integer.MAX_VALUE to guarantee it fires before every other component in the binary, is held at HIGH under an explicit, stated blast-radius escalation given the game's 3.5 billion-plus download base and confirmed evidence of a substantial underage audience. All four Android Privacy Sandbox permissions, including cross-app behavioral cohort targeting, are held at HIGH for the same reason. An undisclosed PRC-NSL-exposed ad network, a hardcoded Firebase key, and a ten-plus-network mediation stack correct to MEDIUM. A structural contradiction, a COPPA-compliant kids ad adapter present alongside a full adult behavioral targeting stack, is classified OBSERVATIONAL. Thirteen messages were sent across 92 days; six drew the identical ticket-acknowledgment auto-reply, and not one substantive reply was ever received.

ID	Severity	Title
C1	HIGH	Six Pre-Consent Ad and Analytics SDK Content-Providers, One Set to Fire at the Absolute Maximum Priority Android Allows
H1	MEDIUM	Mintegral/MBridge, a PRC-NSL-Exposed Ad Network, Bundled With a Full Video Playback Stack
H2	MEDIUM	Firebase API Key Hardcoded in the Distributed Binary
H3	HIGH	All Four Privacy Sandbox Permissions, Including Cross-App Behavioral Cohort Targeting, on a 3.5 Billion-Download Game With a Confirmed Child Audience
H4	OBSERVATIONAL	A COPPA-Compliant Kids Ad Adapter Ships Alongside a Full Adult Behavioral Targeting Stack
M1	MEDIUM	Ten-Plus Independent Ad Network Mediation Stack
M2	MEDIUM	Cleartext Traffic Permitted at the Manifest Level

Subject & Operator Analysis

Subway Surfers is operated by SYBO Games ApS of Copenhagen, owned by Miniclip SA (Geneva, Switzerland), ultimately controlled by Krafton Inc. (South Korea). With more than 3.5 billion downloads, it is one of the most-downloaded mobile games in history.

Several genuine positives are worth naming. allowBackup is correctly set to false. A network security configuration is present in the manifest. The app requests no camera, microphone, location, or contacts permissions, an unusually clean permission profile for a game of this scale. A real AppLovin consent-management-platform configuration file exists in the binary, genuine engineering investment, even though it cannot gate the SDKs that initialize ahead of it. The privacy policy URL is hardcoded and accessible in-app.

Six Identical Ticket Acknowledgments, Zero Substantive Replies

This case's correspondence pattern is a clean instance of automated ticket-system deflection: six of thirteen messages drew the identical acknowledgment, 'Hey Surfer, this is just to let you know that we've received your request. One of our agents will reach out to you as soon as possible,' each issued under a new, unrelated conversation ID, not a continuation of the existing thread, meaning no continuity of context was ever established on SYBO's side. No agent ever did reach out. Not one substantive reply was received across 92 days.

Findings

C1: Six Pre-Consent Ad and Analytics SDK ContentProviders, One Set to Fire at the Absolute Maximum Priority Android Allows

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 this is the largest pre-consent ContentProvider stack RFI-IRFOS has recorded in this audit series, on an application downloaded more than 3.5 billion times with confirmed evidence of a substantial underage audience.

Six ContentProviders, Moloco, Vungle, AppLovin, Google AdMob, Firebase, and BidMachine, all initialize at process creation, before MainActivity and before any consent dialog. Moloco's initOrder is set to 2147483648, Integer.MAX_VALUE, guaranteeing it fires before every other ContentProvider in the entire APK, including Vungle's already-aggressive initOrder=102. AppLovin ships a real consent-management-platform configuration file in the binary, but AppLovinInitProvider itself fires before that CMP can load, meaning the consent infrastructure exists but cannot gate the SDK it belongs to. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because this is the largest pre-consent ContentProvider stack RFI-IRFOS has recorded in this audit series, on an application with more than 3.5 billion downloads and confirmed evidence of a substantial underage audience.

```
com.moloco.sdk...StartupComponentInitialization: initOrder=2147483648 (Integer.
    MAX_VALUE)
VungleProvider: initOrder=102
AppLovinInitProvider: initOrder=101 (fires before its own bundled CMP can load)
MobileAdsInitProvider / FirebaseInitProvider / BidMachineInitProvider: initOrder=100 (
    tied)
PlayGamesInitProvider: initOrder=99
```

Impact: Six independent third parties begin collecting device and behavioral signals before a player, plausibly a child given the game's confirmed underage audience, has seen a single consent screen, with the highest-priority SDK engineered specifically to guarantee it fires first.

Fix: Gate all six ContentProviders behind the existing AppLovin CMP or an equivalent app-native consent flow, reordering initialization so the CMP fires first. No confirmation that this has occurred was ever received.

H1: Mintegral/MBridge, a PRC-NSL-Exposed Ad Network, Bundled With a Full Video Playback Stack

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

Mintegral (formerly MBridge), operationally headquartered in Guangzhou and a subsidiary of Mobvista Inc. (HKEX: 1860), is bundled with a full ExoPlayer fork for native video ad rendering. As a PRC-incorporated group, Mobvista is subject to National Security Law Art. 7 compelled-disclosure obligations. No EU adequacy decision covers this transfer.

Impact: EU players' device identifiers and ad-interaction behavior flow through a PRC-NSL-exposed processor with no disclosed transfer mechanism.

Fix: Document an Art. 44-49 transfer mechanism for the Mintegral relationship, or remove it from the EU-distributed build. No confirmation that this has occurred was ever received.

H2: Firebase API Key Hardcoded in the Distributed Binary

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

The Firebase API key, app ID, and project URL are present verbatim in the APK's assets, extractable in under a minute. This is an availability finding, quota exhaustion and potential Firebase Rules misconfiguration exposure, not a confidentiality one.

```
google_api_key:  AIzaSyAIrgHn1QjOvdtW6AjpMUytqrLOCJN9al8
project:         api-project-1055792361676
app_id:          1:1055792361676:android:94e1faead5ee4c7281d269
```

Impact: A party holding the exposed key can attempt quota exhaustion or exploit any Firebase Rules misconfiguration against the project.

Fix: Rotate the exposed key and apply Firebase App Check and key restrictions. No confirmation that this has occurred was ever received.

H3: All Four Privacy Sandbox Permissions, Including Cross-App Behavioral Cohort Targeting, on a 3.5 Billion-Download Game With a Confirmed Child Audience

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 ACCESS_ADSERVICES_CUSTOM_AUDIENCE enables cross-app behavioral cohort targeting on a game with more than 3.5 billion downloads and confirmed evidence of a substantial underage audience.

ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS, and ACCESS_ADSERVICES_CUSTOM_AUDIENCE are all declared. Custom Audience specifically enables SYBO to build behavioral cohorts from Subway Surfers play data and target those cohorts with ads in unrelated apps. A player of a running game has no reason to expect their play behavior is used to target them elsewhere. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because this cross-app cohort-targeting capability sits on a game with more than 3.5 billion downloads and confirmed evidence of a substantial underage audience, evidenced by the SuperAwesome kids-ad adapter documented in H4.

```
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

Impact: Behavioral cohorts built from a child-audience runner game's play data can be used to target the same players with advertising in apps that have nothing to do with Subway Surfers.

Fix: Remove ACCESS_ADSERVICES_CUSTOM_AUDIENCE or restrict cross-app cohort participation for any session context consistent with a minor user, and document the legal basis for the remaining three permissions individually. No confirmation that this has occurred was ever received.

H4: A COPPA-Compliant Kids Ad Adapter Ships Alongside a Full Adult Behavioral Targeting Stack

OBSERVATIONAL — not independently CVSS-scored; a structural transparency contradiction, not a demonstrated technical attack path on its own.

SuperAwesome, the leading COPPA/GDPR-K compliant kids advertising platform, is present as a bidding adapter within the IronSource/LevelPlay mediation stack, evidence that SYBO's own infrastructure is configured with awareness of a child audience in at least some contexts. The same binary simultaneously initializes six pre-consent behavioral ad SDKs (C1), including a PRC-NSL-exposed network (H1), and declares all four Privacy Sandbox permissions (H3). A partial, context-dependent compliance measure does not remediate pre-consent tracking of the same user base.

Impact: The presence of a child-safe ad adapter alongside a full adult behavioral-targetin g stack demonstrates the operator's own awareness of a child audience, while providing no evidence that the adult-targeting infrastructure is actually excluded from reaching that same audience.

Fix: Document explicitly which sessions are routed through the SuperAwesome child-safe path versus the standard adult behavioral stack, and how that determination is made. No confirmation that this has occurred was ever received.

M1: Ten-Plus Independent Ad Network Mediation Stack

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

In addition to Mintegral (H1), the binary integrates Moloco, AppLovin MAX, Google AdMob, Vungle/Liftoff, IronSource/LevelPlay, Fyber/Digital Turbine, InMobi, Unity Ads, BidMachine, and Facebook Audience Network, ten-plus independent networks each with their own device fingerprinting, audience modeling, and data-retention pipeline.

Impact: Ten or more separate third parties each independently profile the same player, with the cumulative surface exceeding what any single processor relationship would suggest.

Fix: Name each network individually as a data recipient with a stated Art. 28 processing basis. No confirmation that this has occurred was ever received.

M2: Cleartext Traffic Permitted at the Manifest Level

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3.

android:usesCleartextTraffic="true" is set at the manifest level. A network security configuration is present, which may restrict cleartext to specific domains, but its exact scope was not independently verifiable without decoding resources.arsc in this pass. In the context of a ten-plus network ad stack, cleartext capability increases the attack surface for ad injection or traffic interception.

Impact: The manifest-level cleartext permission increases the theoretical attack surface for ad-traffic interception or injection across a stack of ten-plus ad networks, though the network security configuration's actual restriction scope was not independently confirmed.

Fix: Set usesCleartextTraffic to false and confirm the network security configuration enforces HTTPS across all ad-network endpoints. No confirmation that this has occurred was ever received.

Article	Finding	Basis

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. 7, Art. 25	C1	Six-provider pre-consent SDK bootstrap, one engineered to fire at maximum priority.
Art. 44-49, Art. 13(1)(e)	H1	Undisclosed PRC-NSL-exposed ad network, no adequacy decision.
Art. 32	H2	Hardcoded Firebase credential, availability exposure.
Art. 5(1)(b), Art. 6(1), Art. 8	H3	Cross-app behavioral cohort targeting reaching a confirmed underage audience.
Art. 8	H4	Structural contradiction between a child-safe ad adapter and a full adult targeting stack.
Art. 13(1)(e), Art. 28	M1	Ten-plus undisclosed ad-network processor relationships.
Art. 32	M2	Manifest-level cleartext traffic permission.

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. In this report, C1 and H3 are escalated from MEDIUM/6.9 to HIGH specifically because of the game's 3.5 billion-plus download base and confirmed evidence of a substantial underage audience, real-world circumstances CVSS's technical vector does not capture; H1, H2, M1, and M2 correct to MEDIUM to match their own computed bands; H4 is classified OBSERVATIONAL because it is a structural transparency contradiction without a demonstrated technical

attack path to score. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF #SUBWAYSURF-001.