Coordinated Privacy Disclosure, Final Report

FIFA Panini Digital Collection Android (it.panini.fifacollection)

Panini S.p.A., Modena, Italy

DEFLECTED VIA IDENTITY CHALLENGE, NO TECHNICAL RESPONSE · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, TWO DAYS AFTER THE EMBARGO

Target	FIFA Panini Digital Collection, a licensed FIFA/EA Sports FC digital sticker collection app
Package	it.panini.fifacollection
Operator	Panini S.p.A., Via Nilde Iotti 1, 41100 Modena, Italy
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators	Garante per la protezione dei dati personali (Italy, lead SA), Austrian DSB, CERT.at
Total Outbound Messages	6, across 92 days: five to Panini's privacy and press addresses plus one immediate same-day reply declining an identity-verification demand, cc'ing Italy's Garante and CERT.at on later rounds.
Inbound Replies	1, received 6 July 2026 via rfi-irfos.com's own contact form, eleven days after disclosure: Panini's Data Protection Committee demanded written proof that rfi.irfos@gmail.com was an authorized RFI-IRFOS channel before any further exchange, stated the report was treated as unvalidated pending that proof, and formally requested that publication be withheld until the matter was validated through Panini's own process. RFI-IRFOS replied the same day, declining the demand and confirming the embargo unchanged. No technical rebuttal of any specific finding was ever received, before or after.

---

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 Panini S.p.A. that its then-recently-launched FIFA Panini Digital Collection Android app, a licensed FIFA/EA Sports FC digital sticker collection product, initializes both FirebaseInitProvider (initOrder=100) and a custom MlKitInitProvider (initOrder=99) at process creation, both directBootAware, before any Activity or consent dialog can appear.

A second finding names an unusual SDK architecture, not a single tracking flow: AppsFlyer is integrated via both a Unity plugin wrapper and a React Native module simultaneously, an atypical combination for a Unity-engine app, alongside advertising-attribution permissions in a licensed sticker product with no advertised free or ad-supported tier. A third finding notes allowBackup is left at its true default, meaning sticker-collection state, album completion, and purchase history are all eligible for unencrypted Google Cloud backup with no observed exclusion rules.

Six messages were sent across 92 days. The first, to dpo@panini.it, bounced outright; subsequent messages to privacy@panini.it, press@panini.it, and webprivacy@panini.it were all accepted, cc'ing Italy's Garante and CERT.at on later rounds. On 6 July 2026, eleven days after disclosure, Panini's Data Protection Committee replied via rfi-irfos.com's own contact form, demanding written proof that rfi.irfos@gmail.com was an authorized RFI-IRFOS channel, stating the report would otherwise be treated as unvalidated, and formally requesting that publication be withheld pending that validation. RFI-IRFOS replied the same day, declining the identity-verification precondition and confirming the embargo remained unchanged. No technical rebuttal of any specific finding was ever received, before or after. The 90-day embargo, set at first contact, elapsed on 23 September 2026. This report and the accompanying closure notice publish two 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 FIFA Panini Digital Collection Android application (it.panini.fifacollection, version 1.2.0, 148.3 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Panini's or AppsFlyer's backend infrastructure was performed.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All five correct to MEDIUM or LOW on their computed bands. Pre-consent Firebase and ML Kit initialization, a hardcoded Firebase API key, and an atypical mixed Unity/React Native AppsFlyer architecture correct to MEDIUM. allowBackup=true, eligible sticker-collection and purchase-history state for Google Cloud backup, and a cluster of phone-state and storage permissions both correct to LOW. Eleven days after disclosure, Panini's Data Protection Committee replied demanding proof of RFI-IRFOS's identity before any further exchange and asking that publication be withheld pending validation; RFI-IRFOS declined the demand the same day and confirmed the embargo unchanged. No technical rebuttal of any specific finding was ever received.

ID	Severity	Title
C1	MEDIUM	Firebase and ML Kit Both Initialize Before Any Consent Screen
H1	MEDIUM	Firebase API Key Hardcoded and Extractable
H2	MEDIUM	AppsFlyer Runs a Mixed Unity/React Native SDK Architecture With Undisclosed Attribution
H3	LOW	allowBackup Left at True: Sticker Collection and Purchase History Eligible for Cloud Backup
M1	LOW	READ_PHONE_STATE and Broad Storage Permissions in a Sticker Collection App

Subject & Operator Analysis

FIFA Panini Digital Collection is a licensed FIFA/EA Sports FC digital sticker collection app, operated by Panini S.p.A. of Modena, Italy, and was recently launched (v1.2.0) at the time of review.

Several genuine positives are worth naming. No advertising networks beyond attribution tracking are present, no AdMob, no AppLovin, no Mintegral. CAMERA access is justified by a confirmed ML Kit barcode scanner used to scan physical Panini stickers. No location or microphone permissions are declared. The Firebase project name (fifa-panini-digital-collection) is correctly scoped to the product. As an early-stage app at the time of review, a fix window remained genuinely open before the user base grew.

Six Messages, One Identity Challenge, Zero Technical Response

This case's correspondence record involved one address failure before a working channel was confirmed. The first message, to dpo@panini.it, bounced outright on 25 June 2026. Subsequent messages to privacy@panini.it, press@panini.it, and later webprivacy@panini.it were all accepted for delivery. On 6 July 2026, eleven days after disclosure, Panini's Data Protection Committee replied via rfi-irfos.com's own contact form, requiring written confirmation that rfi.irfos@gmail.com was an authorized RFI-IRFOS channel before engaging further, stating the report was treated as unvalidated until then, and formally requesting that publication be withheld pending Panini's own validation process. RFI-IRFOS replied the same day, declining the precondition and confirming the embargo unchanged. Four further messages followed through 6 September 2026, restating the same technical questions; none drew a further reply, and no specific finding was ever technically rebutted.

Findings

C1: Firebase and ML Kit Both Initialize Before Any Consent Screen

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.

FirebaseInitProvider (initOrder=100) and a custom MlKitInitProvider (initOrder=99) are both declared directBootAware="true", both firing at process creation, before any Activity and therefore before any consent screen, and potentially before device unlock.

```
com.google.firebase.provider.FirebaseInitProvider    initOrder=100, directBootAware=
    true
it.panini.fifacollection.mlkitinitprovider           initOrder=99,  directBootAware=
    true
```

Impact: Two separate SDK bootstraps begin before a user has seen a single consent notice, in a licensed product marketed to a broad, general-audience fanbase.

Fix: Defer both providers' initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

H1: Firebase API Key Hardcoded and Extractable

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.

A Firebase API key, project ID, app ID, and storage bucket are all extractable from a bundled google-services-desktop.json asset file. Depending on the project's security-rule configuration, this enables unauthorized database access or quota-exhaustion denial of service.

```
Firebase API key:  AIzaSyDdLFrS41ZOQUKMCT8FempPeN14zzoJyus
Firebase project:  fifa-panini-digital-collection
Firebase App ID:   1:749957597071:android:dbc723fad479b08586adfa
Storage bucket:    fifa-panini-digital-collection.firebasestorage.app
```

Impact: The key and associated project identifiers are trivially extractable, and depending on the security-rule configuration behind them, could enable unauthorized access or denial of service against legitimate users.

Fix: Restrict the Firebase API key by package name and SHA-1 certificate fingerprint, and audit the project's security rules. No confirmation that this has occurred was ever received.

H2: AppsFlyer Runs a Mixed Unity/React Native SDK Architecture With Undisclosed Attribution

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.

AppsFlyer is integrated via both a Unity plugin wrapper and a React Native module simultaneously, an atypical combination for a Unity-engine game, tracking install sources, in-app sticker-pack purchase events, and conversion funnels. ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION are both declared in a licensed product with no advertised free or ad-supported tier.

```
com.appsflyer.unity.AppsFlyerAndroidWrapper    -- Unity plugin wrapper
com.appsflyer.reactnative.RNAppsFlyerModule   -- React Native module
appsflyer_backup_rules.xml
appsflyer_data_extraction_rules.xml
```

Impact: Install and purchase-attribution tracking runs through an unusually broad, dual-framework SDK footprint in a licensed sticker product with no disclosed advertising purpose.

Fix: Document AppsFlyer's attribution purpose under Art. 13(1)(e) and remove the unused framework wrapper. No confirmation that this has occurred was ever received.

H3: allowBackup Left at True: Sticker Collection and Purchase History Eligible for Cloud Backup

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

android:allowBackup is left at its true default, with no observed backup exclusion rules, meaning sticker-collection state (owned stickers, album completion, trade history) and in-app purchase history are all eligible for Google Cloud backup.

```
android:allowBackup=true (no exclusion rules observed)
```

Impact: Collection and purchase state can end up in a user's Google Cloud backup; the practical exposure depends on the backup destination's own security and is not directly network-reachable, which keeps the computed score low.

Fix: Set allowBackup=false, or define explicit backup exclusion rules for sensitive collection and purchase data. No confirmation that this has occurred was ever received.

M1: READ_PHONE_STATE and Broad Storage Permissions in a Sticker Collection App

LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0.

READ_PHONE_STATE (IMSI/device ID access), READ_EXTERNAL_STORAGE, and WRITE_EXTERNAL_STORAGE are all declared, alongside Huawei HMS and Samsung-specific data-access permissions, none with a documented purpose for a sticker-collection product.

```
android.permission.READ_PHONE_STATE
android.permission.READ_EXTERNAL_STORAGE
android.permission.WRITE_EXTERNAL_STORAGE
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA
com.samsung.android.mapsagent.permission.READ_APP_INFO
```

Impact: Device identifier and broad storage access are declared without a documented purpose; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low.

Fix: Remove unused permissions and migrate to scoped storage on modern Android. No confirmation that this has occurred was ever received.

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	Pre-consent SDK initialization via direct-BootAware ContentProviders.
Art. 32	H1	Hardcoded, trivially extractable Firebase API key.
Art. 5(1)(b), Art. 13(1)(e)	H2	Undisclosed dual-framework attribution SDK in a non-advertising product.
Art. 5(1)(c), Art. 32, Art. 13(1)(e)	H3	Collection and purchase data eligible for unrestricted cloud backup.
Art. 5(1)(c), Art. 13(1)(c)	M1	Undocumented device-identifier and broad storage permissions.

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, H1, and H2 correct to MEDIUM to match their own computed bands; H3 and M1 correct to LOW on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: FIFAPANINI-2026-R1.