Coordinated Security & Privacy Disclosure, Final Report

KFC UAE for Android (com.kfc.me, v10.56.1)

Nine written notices, ninety-one days, two identical procurement-deflection auto-replies, zero human replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED AFTER NINE NOTICES

Target	Americana Restaurants International / Americana Food Group (legal entity: Kuwait Food Company Americana)
Product audited	KFC UAE for Android, com.kfc.me, v10.56.1
Disclosure reference	REF KFCUAE-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C3 FLEDGE/Protected Audience ad-auction stack linking every food order to the Google Advertising ID via a hard-coded CleverTap flag, CVSS v4.0 8.7, unaddressed)

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 KFC UAE Android application and identified three CRITICAL and three HIGH findings: two Google/Firebase API keys hardcoded in the shipped APK, a Chucker HTTP debug interceptor active in the production build, storing the full local API call history, including authentication requests, order submissions, payment gateway calls, loyalty-program lookups, and delivery-address lookups, in a local SQLite database readable by any app with storage access or brief physical device access, a FLEDGE/Protected Audience ad-auction permission stack combined with a hardcoded CLEVERTAP_USE_GOOGLE_AD_ID manifest flag explicitly linking every food order to the Google Advertising ID for CleverTap marketing automation, Huawei HMS (1,835 smali classes) routing location and order data for Huawei device users through China-facing infrastructure subject to the PRC National Intelligence Law, continuous GPS collection via a foreground location service combined with an undisclosed third-party rider-tracking SDK during active orders, and a CleverTap and Facebook SDK combination transmitting meal-ordering behavior to marketing and advertising platforms.

Across nine written notices over ninety-one days, spanning four Gmail threads created by repeated address bounces, no human reply of any kind was ever received. The only inbound correspondence was an identical automated procurement-deflection auto-reply, 'thank you for reaching out to Americana Foods and expressing your interest in partnering with us,' sent twice, on 27 June and again on 16 September, confirming it as a canned CRM response entirely disconnected from the disclosure's actual content. None of RFI-IRFOS's five standing questions, on whether Chucker has been removed from the production build, the Art. 6(1) legal basis for the FLEDGE ad-auction pipeline, Art. 33 notification, DPO awareness, or the Art. 44-46 transfer mechanism governing data reaching China via Huawei HMS, ever received an answer.

Scope: Static analysis of the publicly downloaded production KFC UAE Android APK (v10.56.1), on an authorized test device, only. No Americana account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@americana-food.com (bounced), redelivered to digiteam@americana-food.com and, after a further bounce of privacy@amer.com, to info@americana-food.com, bcc/cc the Austrian Datenschutzbehoerde and CERT.at. Across nine written notices over ninety-one days, spanning four Gmail threads created by repeated address bounces, the only inbound correspondence was an identical automated 'thank you for your interest in partnering with us' procurement auto-reply, sent twice, on 27 June and again on 16 September after entirely different follow-up content, confirming it as a canned response rather than a human reading the disclosure.

ID	Severity	Title
C1	CRITICAL	Two Google/Firebase API keys hardcoded in the production APK

ID	Severity	Title
C2	CRITICAL	Chucker HTTP debug interceptor active in the production build
C3	CRITICAL	FLEDGE/Protected Audience ad-auction stack linking every food order to the Google Advertising ID
H1	HIGH	Huawei HMS routes location/order data through China-facing infrastructure
H2	HIGH	Continuous GPS via foreground location service plus an undisclosed rider-tracking SDK
H3	HIGH	CleverTap and Facebook SDK transmit order behavior to marketing/ad platforms

Subject & Operator Analysis

KFC UAE is operated by Americana Restaurants International / Americana Food Group, whose legal entity, per its own auto-reply footer, is Kuwait Food Company Americana.

Findings

C1: Two Google/Firebase API keys hardcoded in the production APK

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

Firebase key AIzaSyDJ-zNYxyLZfIH2tSMIswguUYx67Tcat1A (project kfc-uae-48842, App ID 1:395838544502:android:3f20f755abd62a7e155d57, storage bucket kfc-uae-48842.appspot.com) and a second Google key in the manifest, AIzaSyDkRWxO-3AFzXNd1i_tJupbFOTqorgZel8, both ship in the public Play Store binary.

No reply of any kind addressed this finding across nine notices.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Restrict both keys to the com.kfc.me package name and SHA-256 signing fingerprint, and rotate immediately.

C2: Chucker HTTP debug interceptor active in the production build

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 6.8

com.chuckerteam.chucker.internal.support.ClearDatabaseService and ChuckerFileProvider are present in the production Play Store APK, intercepting all HTTPS network calls and storing them in a local SQLite database, including authentication requests, order submissions, payment gateway calls, loyalty lookups, and delivery-address lookups.

Any app with storage read permission, or brief physical access to the device, can read the full API call history, including authentication tokens and payment instrument identifiers. No reply of any kind addressed whether Chucker has been removed from the production build or the CI/CD pipeline audited for release/debug separation.

Impact: Authentication tokens and payment-related identifiers are stored in an accessible local database on every user's device, readable by any party with storage access or momentary physical possession of the device.

Fix: Remove Chucker entirely from production release builds and audit the CI/CD pipeline to prevent debug tooling from reaching production.

C3: FLEDGE/Protected Audience ad-auction stack linking every food order to the Google Advertising ID

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

ACCESS_ADSERVICES_CUSTOM_AUDIENCE, ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_AD_ID permissions are present, and CLEVERTAP_USE_GOOGLE_AD_ID=1 is hardcoded in manifest metadata, explicitly linking every food order to the Google Advertising ID for CleverTap marketing automation.

No reply of any kind answered whether this is disclosed to users or what its Art. 6(1) legal basis is.

Impact: Individual food-order data is linked to a persistent advertising identifier for marketing-automation purposes with no confirmed disclosure of this specific linkage.

Fix: Disclose the CleverTap/Ad-ID linkage explicitly and confirm its Art. 6(1) legal basis, or remove the linkage.

H1: Huawei HMS routes location/order data through China-facing infrastructure

---

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

Huawei HMS (1,835 smali classes), including Location, Maps, and OAID advertising identifiers, is routed through Huawei's infrastructure in Shenzhen, China for Huawei device users, subject to China's National Intelligence Law Art. 7.

No reply of any kind answered which Art. 44-46 GDPR transfer mechanism governs this routing.

Impact: Location and order data for Huawei device users may be subject to PRC National Intelligence Law obligations with no confirmed GDPR transfer mechanism.

Fix: Cite the specific Art. 44-46 transfer mechanism covering Huawei HMS data routing, or restrict HMS integration to exclude the affected data categories.

H2: Continuous GPS via foreground location service plus an undisclosed rider-tracking SDK

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

FOREGROUND_SERVICE_LOCATION is declared alongside a third-party Rider Tracking SDK (571 smali classes) providing continuous GPS tracking during active orders. Data governance for the third-party tracking vendor is undisclosed.

No reply of any kind addressed this finding.

Impact: Continuous location tracking during active orders is transmitted to an undisclosed third-party vendor with no confirmed governance arrangement.

Fix: Name the rider-tracking vendor explicitly and disclose the applicable data-governance arrangement.

H3: CleverTap and Facebook SDK transmit order behavior to marketing/ad platforms

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

CleverTap (214 smali classes, Mumbai-based) and the Facebook SDK (355 smali classes, App ID 598651460889440) receive meal-ordering behavior data for marketing automation and Meta's advertising graph in the US.

No reply of any kind addressed this finding.

Impact: Meal-ordering behavior is transmitted to two named third-party advertising and marketing platforms with no confirmed matching disclosure.

Fix: Name CleverTap and Meta explicitly as recipients of order-behavior data in the privacy policy.

Nine Notices, Two Identical Procurement Deflections

Americana's only inbound correspondence in this case, across nine notices and four Gmail threads created by repeated address bounces, was an identical automated 'thank you for reaching out to Americana Foods and expressing your interest in partnering with us' reply, routed to a procurement team, sent on 27 June and again on 16 September after entirely different follow-up content. The identical wording across two unrelated sends confirms this as a canned CRM response, not a human reading the disclosure. No substantive reply of any kind was ever received.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Two hardcoded API keys in the production APK
C2	GDPR Art. 32(1)(a)	Debug HTTP interceptor storing auth tokens and payment data locally
C3	GDPR Art. 6(1), Art. 13(1)(e)	Undisclosed order-to-Ad-ID linkage for marketing automation
H1	GDPR Art. 44-46	Undocumented transfer mechanism for data routed through Chinese infrastructure
H2	GDPR Art. 13(1)(e)	Undisclosed third-party rider-tracking vendor
H3	GDPR Art. 13(1)(e)	Undisclosed order-behavior transfer to marketing/ad platforms

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@americana-food.com (bounced), redelivered to digiteam@americana-food.com; a EUR 18,000 enterprise-engagement figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-06-27	R1 resent to privacy@amer.com (bounced) and info@americana-food.com; automated procurement auto-reply received
2026-07-23	Follow-up names the procurement deflection explicitly, restates three questions
2026-09-04	Follow-up titled 'A Procurement Referral Is Not a Response to a GDPR Disclosure', deadline set 11 September
2026-09-16	Follow-up notes the 16 September deadline reached, stated as likely the last message before publication; identical procurement auto-reply received again
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning privacy contact distinct from the procurement/vendor-onboarding CRM pipeline.
- Remove Chucker entirely from production release builds and audit the CI/CD pipeline.
- Disclose the CleverTap/Advertising-ID order linkage explicitly, with its Art. 6(1) legal basis.
- Cite the Art. 44-46 transfer mechanism governing data routed via Huawei HMS.
- Rotate both exposed API keys and restrict them to the correct package and signing fingerprint.

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. GDPR Art. 6, 13, 25, 32, 44. REF KFCUAE-2026-R1.