Coordinated Privacy Disclosure, Final Report — Two Apps

McDonald’s Austria Loyalty (com.mcdonalds.mobileapp) and McDelivery (ph.mobext.mcdelivery)

McDonald’s Werbegesellschaft mbH, Brunn am Gebirge, Austria (NYSE: MCD)

JURISDICTIONAL DEFLECTION ON ONE APP, CORRECTED IN WRITING, THEN SILENT ON BOTH · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, FOUR DAYS AFTER THE EMBARGO

Target	Two related Android apps distributed to Austrian customers: the McDonald's Austria loyalty and ordering app, and McDelivery, a separately branded food-delivery app
Packages	com.mcdonalds.mobileapp (Loyalty) and ph.mobext.mcdelivery (McDelivery)
Operator	McDonald's Werbegesellschaft mbH, Campus 21, 2345 Brunn am Gebirge, Austria
Initial Disclosure	2026-06-23
Original Embargo	2026-09-21 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, four days after the embargo, an internal publishing gap, not a change in terms
Regulators	Austrian DSB (lead SA), CERT.at
Total Outbound Messages	6, across 73 days, to McDonald's Austria contacts (katrin.stockhammer@at.mcd.com, wilhelm.baldia@at.mcd.com, Arman.Manutscheri@at.mcd.com), cc'ing kundenservice@mcdonalds.at, the Austrian DSB, and CERT.at on later rounds. An initial attempt to security@mcdonalds.com and privacy@mcdonalds.com (McDonald's Corporation global addresses) bounced entirely before the Austrian entity's own contacts were used.
Inbound Replies	1 substantive reply, on 24 June 2026, from Arman Manutscheri (McDonald's Austria), stating that McDelivery "appears to be related to McDonald's Philippines," so Austria could not respond to that app. RFI-IRFOS corrected the record the same day, noting McDelivery's own Firebase project name confirms EU West infrastructure. No further reply of any kind was received on either app after that correction.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 23 June 2026, RFI-IRFOS disclosed to McDonald's Austria two related findings sets on two separate apps distributed to Austrian customers. The McDonald's Austria loyalty app hardcodes four Firebase API keys pointing to a production database named prd-euw-gmal-mcdonalds, prd for production, euw for Europe West, gmal for Global McDonald's App Loyalty, confirming this is the live EU loyalty backend embedded in every APK distributed to European customers. The same app declares ACCESS_ADSERVICES_CUSTOM_AUDIENCE, confirmed active via obfuscated CustomAudienceManager calls, feeding meal-ordering history, a dietary and behavioral profile, into Android's Protected Audience behavioral advertising auctions.

The second app, McDelivery, ships an empty network_security_config.xml, providing no cleartext protection and no certificate pinning across any endpoint handling order placement, delivery tracking, or account data, while its manifest reference to the file creates a false impression that security hardening exists. On 24 June 2026, McDonald's Austria's Arman Manutscheri replied that McDelivery "appears to be related to McDonald's Philippines," declining to respond to that app's findings on jurisdictional grounds. RFI-IRFOS corrected the record the same day: McDelivery's own Firebase project, mcdo-haku-2021, and its Google API keys are compiled directly into the app distributed to Austrian users through the Austrian Play Store listing, regardless of which regional entity nominally operates its backend.

Six messages were sent across 73 days. An initial attempt to McDonald's Corporation's global security and privacy addresses bounced entirely; McDonald's Austria's own named contacts accepted all subsequent messages. One substantive reply was received, the jurisdictional deflection on 24 June 2026, corrected the same day. No further reply of any kind was received on either app across two further follow-ups, on 4 August and 15 August 2026. The 90-day embargo, set at first contact, elapsed on 21 September 2026. This report and the accompanying closure notice publish four days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of two production Android applications distributed to Austrian customers: the McDonald's Austria loyalty app (com.mcdonalds.mobileapp, version 3.46.1) and McDelivery (ph.mobext.mcdelivery), both reviewed on 20-21 June 2026. No dynamic instrumentation, live traffic capture, or interaction with McDonald's, Kochava's, Braze's, mParticle's, Meta's, or Google's backend infrastructure was performed.

Disposition

Twelve findings across both apps were disclosed on 23 June 2026, re-scored under CVSS v4.0. Both apps ship an empty network_security_config, providing no cleartext protection and no certificate pinning while presenting a false signal of security hardening; both reach CRITICAL on the computed CVSS score alone. All remaining findings, hardcoded API keys, undisclosed US tracking stacks, a dietary-data behavioral-advertising pipeline, hardware-identifier permissions, and a redundant overlay permission, correct to MEDIUM or LOW. McDonald's Austria replied once, attempting to redirect the McDelivery disclosure to McDonald's Philippines as a jurisdictional matter; RFI-IRFOS corrected the record the same day by pointing to McDelivery's own EU-West-named Firebase project, and no further reply was received on either app.

ID	Severity	Title
L-C1	MEDIUM	[Loyalty App] Four Firebase Production Credentials Hardcoded, Confirming an EU Backend
L-C2	CRITICAL	[Loyalty App] Empty Network Security Configuration, No Certificate Pinning
L-H1	MEDIUM	[Loyalty App] A Purpose-Built Triple US Tracking Stack
L-H2	MEDIUM	[Loyalty App] Meal-Ordering History Feeds Behavioral Ad Auctions
L-H3	LOW	[Loyalty App] Three Audio Permissions Beyond What Camera-Based Features Require
L-H4	MEDIUM	[Loyalty App] A System-Level Phone-State Permission on a Consumer App
D-C1	CRITICAL	[McDelivery] Empty Network Security Configuration, a False Signal of Protection
D-C2	MEDIUM	[McDelivery] Two Google API Keys Hardcoded
D-H1	MEDIUM	[McDelivery] Facebook Conversions API Sends Order Value and Items to Meta
D-H2	MEDIUM	[McDelivery] IMEI and Phone Number Access With No Evident Functional Need
D-H3	MEDIUM	[McDelivery] A Full Ten-Service Firebase Stack Transmitting Order Behavior to Google
D-M1	LOW	[McDelivery] Redundant Legacy Overlay Permission

Subject & Operator Analysis

McDonald's Austria loyalty and ordering is operated by McDonald's Werbegesellschaft mbH, Brunn am Gebirge, Austria, a subsidiary of McDonald's Corporation (NYSE: MCD). McDelivery is developed under the ph.mobext namespace, associated with Mobext, a Havas Media Group agency; both apps are distributed to Austrian customers through the Austrian Play Store listing regardless of which regional entity nominally operates each backend.

Several genuine positives are worth naming. The loyalty app correctly targets Android 16, the current release, with no Chucker debug interceptor and no session-replay SDK found, correct baseline choices for a payment-handling app. McDelivery correctly sets allowBackup to false and has already adopted the modern HIDE_OVERLAY_WINDOWS permission alongside its legacy predecessor.

A Jurisdictional Deflection, Corrected the Same Day, Then Silence on Both Apps

This case's correspondence record includes a genuine reply, not silence from the outset. On 24 June 2026, one day after disclosure, McDonald's Austria's Arman Manutscheri replied that the McDelivery app "appears to be related to McDonald's Philippines," declining to respond on jurisdictional grounds. RFI-IRFOS corrected the record the same day, noting that McDelivery's own Firebase project name and hardcoded API keys are compiled directly into the exact APK distributed to Austrian users through the Austrian Play Store, independent of which regional entity nominally operates the backend, and that both apps remained in scope. No further reply of any kind was received on either app across two further follow-ups, on 4 August and 15 August 2026, both restating the correction and requesting a named EU data-protection contact for each app.

Findings

L-C1: [Loyalty App] Four Firebase Production Credentials Hardcoded, Confirming an EU Backend

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.

Four Firebase API keys are hardcoded in the production APK, pointing to a database at p rd-euw-gmal-mcdonalds.firebaseio.com, self-documenting as the production, Europe West, Global McDonald's App Loyalty backend. Four hardcoded keys is joint-highest across this audit series.

```
AIzaSyCahkwgCB2ErfAVpHSNxbcUbw8iFYRrDMw
AIzaSyDgmW4ZMvNblSXqMOgsbY8uRrTnfR3E7pY
AIzaSyDyXyb2NsmrUZypmZj4uPxqmSKD_dE3AqU
AIzaSyDzGQVpwZrKLwRhGSM_ApXFJ38e7hUPWmE
Firebase DB: prd-euw-gmal-mcdonalds.firebaseio.com
```

Impact: All four keys are trivially extractable, and depending on the security-rule configuration behind them, could enable unauthorized access to the live EU loyalty database or denial of service against legitimate users. The database naming itself independently confirms EU-West infrastructure.

Fix: Restrict all four Firebase keys by package name and SHA-256 certificate fingerprint, and rotate them. No confirmation that this has occurred was ever received.

L-C2: [Loyalty App] Empty Network Security Configuration, No Certificate Pinning

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3. This finding reaches CRITICAL on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

network_security_config.xml exists but is empty, no domain entries, no pin sets, across all API connections: the loyalty backend, Kochava, Braze, mParticle, and Firebase.

Impact: All traffic processing meal order data, loyalty point balances, and payment confirmations is susceptible to interception by any party with a system-trusted CA certificate.

Fix: Implement an explicit network security configuration with certificate pinning on all production API endpoints. No confirmation that this has occurred was ever received.

L-H1: [Loyalty App] A Purpose-Built Triple US Tracking Stack

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.

Kochava (317 classes), Braze (465 classes), and mParticle (334 classes) are all active, with a dedicated custom wrapper class, mcdonalds.core.tracking.KochavaTracking, architected specifically to serialize McDonald's proprietary event model into Kochava's measurement API, a deliberate pipeline, not an incidental dependency.

```
mcdonalds.core.tracking.KochavaTracking (custom wrapper, PersistDataTracker)
Kochava (317 classes), Braze (465 classes), mParticle (334 classes)
```

Impact: Restaurant visited, items ordered, order time and frequency, loyalty points, and GPS location at order time flow to three US-based processors, none with an EU adequacy decision.

Fix: Document Art. 44 transfer safeguards for all three processors and disclose mParticle's downstream recipients individually. No confirmation that this has occurred was ever received.

L-H2: [Loyalty App] Meal-Ordering History Feeds Behavioral Ad Auctions

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.

ACCESS_ADSERVICES_CUSTOM_AUDIENCE is declared and confirmed active via obfuscated CustomAudienceManager calls, alongside ACCESS_ADSERVICES_TOPICS and ACCESS_ADSERVICES_ATTRIBUTION, three separate ad-technology permissions on a food loyalty app. Meal-ordering data, which menu items, how frequently, which restaurants, and time-of-day patterns, feeds Android's Protected Audience API for cross-app behavioral ad targeting.

Impact: A user's dietary preferences and movement patterns become a targeting criterion usable in other apps entirely, with no granular consent observed at onboarding.

Fix: Document a specific legal basis for Custom Audience use or remove it. No confirmation that this has occurred was ever received.

L-H3: [Loyalty App] Three Audio Permissions Beyond What Camera-Based Features Require

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.

RECORD_AUDIO, MICROPHONE, and MODIFY_AUDIO_SETTINGS are all declared. Static analysis identified CameraX's VideoCapture API (AudioStreamImpl) as the explanation for RECORD_AUDIO and MICROPHONE, but MODIFY_AUDIO_SETTINGS, which allows changing device volume and audio routing, exceeds what QR-scanning or camera features require.

Impact: Microphone-adjacent access is present beyond documented feature need; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low.

Fix: Replace CameraX VideoCapture with image-only ImageCapture where audio is not intentionally used, and remove MODIFY_AUDIO_SETTINGS if unused. No confirmation that this has occurred was ever received.

L-H4: [Loyalty App] A System-Level Phone-State Permission on a Consumer App

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.

READ_PRIVILEGED_PHONE_STATE, normally restricted to system apps signed with the platform certificate, is declared in a consumer Play Store app. It grants IMEI/MEID and device serial access even on Android 10+, where standard READ_PHONE_STATE no longer returns hardware identifiers.

Impact: If active on any distribution channel, this permission would expose a permanent, non-resettable hardware identifier linked to a loyalty profile, a tracking capability that outlasts advertising ID resets.

Fix: Remove the permission if it serves no function, or fully document its purpose and distribution scope if it is intentionally granted on any device variant. No confirmation that this has occurred was ever received.

D-C1: [McDelivery] Empty Network Security Configuration, a False Signal of Protection

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3. This finding reaches CRITICAL on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

The manifest references @xml/network_security_config, but the referenced file contains only an empty <network-security-config /> element: no cleartext restriction, no pin-set, no certificate-transparency enforcement, no domain-config for any endpoint. An empty NSC file creates a false impression of security hardening to anyone reviewing the manifest reference alone.

```
<network-security-config />  (empty; referenced by manifest, provides no actual
    protection)
```

Impact: Order placement, delivery tracking, and account API traffic, including home delivery addresses and payment method data, is interceptable by any party holding a system-trusted CA certificate.

Fix: Replace the empty configuration with an explicit cleartext-disabled base-config and a pin-set for order and account endpoints. No confirmation that this has occurred was ever received.

D-C2: [McDelivery] Two Google API Keys Hardcoded

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 and a second Google API key are both hardcoded in the production binary, pointing to Firebase project mcdo-haku-2021, the same project that RFI-IRFOS cited when correcting McDonald's Austria's jurisdictional deflection.

```
AIzaSyDBhaGX9MvsqLP8baxv_qaQrG8EZ09sxjI (Firebase, project mcdo-haku-2021)
AIzaSyAOfCPpc3hAyv5uTVAybfPoJLTWzNUnseY
```

Impact: Both keys are trivially extractable, and depending on the security-rule configuration behind them, could enable unauthorized access to order and customer data or denial of service.

Fix: Restrict both keys by package name and certificate fingerprint, and rotate them. No confirmation that this has occurred was ever received.

D-H1: [McDelivery] Facebook Conversions API Sends Order Value and Items to Meta

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.

The Facebook SDK's Conversions API module (AppEventsConversionsAPITransformer and related classes) is integrated, transmitting purchase and behavioral events, order value, items, conversion timing, and optionally hashed contact details for advanced matching, directly to Meta's advertising infrastructure.

```
AppEventsConversionsAPITransformer, ConversionsAPIEventName,
    ConversionsAPICustomEventField
```

Impact: Order-level purchase data is sent to Meta's advertising infrastructure with no confirmed granular opt-in consent gate, and Meta is not confirmed as a disclosed recipient in the app's privacy documentation.

Fix: Gate Facebook SDK event logging and Conversions API calls behind explicit consent, and disclose Meta as an advertising recipient. No confirmation that this has occurred was ever received.

D-H2: [McDelivery] IMEI and Phone Number Access With No Evident Functional Need

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.

READ_PHONE_NUMBERS and READ_PHONE_STATE are both declared, granting access to the device IMEI, IMSI, and SIM-registered phone number, permanent hardware identifiers that cannot be reset, distinct from resettable advertising IDs.

```
android.permission.READ_PHONE_NUMBERS
android.permission.READ_PHONE_STATE
```

Impact: A food delivery app gains access to non-resettable hardware identifiers with no evident functional need beyond what a user already provides during registration.

Fix: Remove both permissions and collect the delivery contact number through a UI input field instead. No confirmation that this has occurred was ever received.

D-H3: [McDelivery] A Full Ten-Service Firebase Stack Transmitting Order Behavior to Google

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.

Ten Firebase services are confirmed active: Analytics, Crashlytics, Database, Dynamic Links, Auth, App Check, Remote Config, Messaging, Performance, and Sessions. Firebase Database being configured means real-time order data may flow through Google's infrastructure alongside the other nine services.

Impact: Order funnel events, crash state during active orders, and real-time order data all transit Google's US infrastructure across ten separate Firebase services.

Fix: Document each Firebase service individually under Art. 13(1)(e) and confirm SCCs cover the aggregate transfer. No confirmation that this has occurred was ever received.

D-M1: [McDelivery] Redundant Legacy Overlay Permission

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.

SYSTEM_ALERT_WINDOW is declared for legitimate tapjacking-detection purposes on payment screens, but the app also already declares the newer, less invasive HIDE_OVERLAY_WINDOWS permission, making the older, more powerful permission redundant.

Impact: A powerful, system-wide overlay permission remains declared alongside its modern replacement, an unnecessary residual attack surface, not an active exploit path.

Fix: Remove SYSTEM_ALERT_WINDOW now that HIDE_OVERLAY_WINDOWS covers the same legitimate use case. 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. 32(1)(b), Art. 25(1)	L-C1	Four hardcoded Firebase production credentials confirming an EU loyalty backend.
Art. 32(1)(a), Art. 5(1)(f)	L-C2 / D-C1	Empty network security configuration on both apps, no cleartext protection, no certificate pinning.
Art. 5(1)(b), Art. 13(1)(e)(f), Art. 44	L-H1	A purpose-built triple US tracking stack with a custom attribution wrapper.
Art. 5(1)(b), Art. 6, Art. 9(1)	L-H2	Meal-ordering history feeding behavioral ad auctions.
Art. 5(1)(c), Art. 13	L-H4 / D-H2	System-level or unjustified hardware-identifier permissions.
Art. 6(1)(a), Art. 13(1)(e), Art. 46	D-H1	Undisclosed order-level purchase data sent to Meta via Conversions API.
Art. 13(1)(e), Art. 46, Art. 28	D-H3	A full ten-service Firebase stack with no individually documented transfer basis.

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. In this report, L-C2 and D-C1 (the empty network security configuration on each app) reach CRITICAL on their computed CVSS v4.0 scores alone, no editorial escalation applied; L-C1, L-H1, L-H2, L-H4, D-C2, D-H1, D-H2, and D-H3 correct to MEDIUM to match their own computed bands; L-H3 and D-M1 correct to LOW on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: MCDONALDS-2026-R1.