Coordinated Security & Privacy Disclosure, Final Report

Marionnaud Android app, v4.22.3 (package name disputed between correspondence's own subject lines and body text – see Scope)

Nine written notices, ninety-one days, one permanently rejecting mailbox, two silent mailboxes, zero replies of any kind

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

Target	Marionnaud Austria, Austria's largest perfumery chain, part of A.S. Watson Group / CK Hutchison Holdings
Product audited	Marionnaud Android app, v4.22.3 (Firebase project mat-android-app)
Disclosure reference	REF AT-MARIONNAUD-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 ContentSquare session-replay capturing a user's face during an AR makeup try-on session with no matching consent, 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 Marionnaud Android application and identified three CRITICAL and three HIGH findings: three hardcoded API keys (Firebase, Google Maps, and Fritz AI) in the shipped APK, a ContentSquare session-replay integration (2,348 smali classes, initializing automatically before the first screen renders) that, during an AR-camera makeup try-on session, captures the user's face in real time and transmits it to ContentSquare SAS in France, a use the user consented to for the try-on feature itself but not for session-replay capture, a ModiFace facial-recognition model (459 smali classes) using a 65-point facial landmark bundle that constitutes a biometric profile under GDPR Art. 9(1), a Network Security Configuration whose cleartextTrafficPermitted attribute is set to a string reference rather than the boolean literal the attribute requires, causing the parser to potentially fail silently and fall back to a platform default, a Criteo retargeting integration (128 smali classes) tracking browsed-but-unpurchased beauty products that could combine with ModiFace try-on data to form a linked beauty-preference profile, and a missing data_extraction_rules.xml leaving loyalty, purchase, and cached AR session data without an explicit device-to-device backup exclusion.

Across nine written notices over ninety-one days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde and CERT.at, no message from any @marionnaud.at address was ever received. datenschutz@marionnaud.at rejected mail outright on every one of four separate attempts spanning five weeks, and office@marionnaud.at and presse@marionnaud.at, while never bouncing, never responded either. None of RFI-IRFOS's standing questions, on whether ModiFace's facial landmark data leaves the device, whether Criteo receives AR try-on interaction data, whether the three exposed API keys were rotated, or whether datenschutz@marionnaud.at is a dead mailbox or an intentional non-response, ever received an answer.

Scope: Static analysis of the publicly downloaded production Marionnaud Android APK (v4.22.3), on an authorized test device, only. No Marionnaud account, backend, or infrastructure was accessed or tested. A package-name discrepancy in RFI-IRFOS's own correspondence is disclosed rather than silently resolved: every email subject line across this case refers to the app as com.marionnaud.android, while the R1 body text and all technical findings consistently reference at.marionnaud.customer as the analyzed package. Both names are reported here as they appear in the record.

Disposition

R1 sent 21 June 2026 to datenschutz@marionnaud.at (rejected on every one of four attempts: 06-21, 06-27, 06-28, 07-28, '550 5.4.1 Recipient address rejected') and forwarded the same day to office@marionnaud.at requesting internal routing to the DPO, cc presse@marionnaud.at, bcc/cc the Austrian Datenschutzbehoerde and CERT.at. Across nine written notices over ninety-one days, no message from any @marionnaud.at address was ever received; the only inbound mail was repeated mailer-daemon rejections for the datenschutz@ mailbox.

ID	Severity	Title
C1	CRITICAL	Three hardcoded API keys in the public Play Store APK
C2	CRITICAL	ContentSquare session-replay capturing a user's face during an AR makeup try-on session
C3	CRITICAL	ModiFace 65-point facial landmark model constitutes biometric processing under Art. 9
H1	HIGH	Network Security Config: cleartextTrafficPermitted set to a string reference instead of a boolean literal
H2	HIGH	Criteo retargeting based on browsed-but-unpurchased beauty products
H3	HIGH	Missing data_extraction_rules despite WRITE_EXTERNAL_STORAGE permission

Subject & Operator Analysis

Marionnaud Austria is Austria's largest perfumery chain, part of the A.S. Watson Group, whose parent is CK Hutchison Holdings.

Findings

C1: Three hardcoded API keys in the public Play Store 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

A Firebase API key (AIzaSyDxCGNat1FrmBz0LCZ9kJuBOWQqizvQIac, project mat-android-app, App ID 1:756146699911:android:fc1ea9a8973224cf), a Google Maps key (AIzaSyAIDoODGD6vorVCK77fl_Dw0r6hcPULu3s), and a Fritz AI key (f2cb44d6e1a84b bd827d50245b0e162a) are all hardcoded in the shipped APK. The Firebase key alone allows probing the mat-android-app project, reading Remote Config (loyalty parameters, promo flags, pricing experiments), accessing Firebase Storage, and, if security rules have gaps, reading or writing customer data.

No reply of any kind, from any of three separate mailboxes, addressed this finding across nine notices.

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

Fix: Rotate all three exposed keys, restrict each to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default Firebase security rules.

C2: ContentSquare session-replay capturing a user's face during an AR makeup try-on session

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

CSQInitializer starts automatically via AndroidX Startup before the first screen renders, and an OverlayService captures the visual screen state. During an AR-camera makeup try-on session, this overlay contains the user's face in real time.

The user consented to use her camera to test a lipstick shade. She did not consent to her face being captured in a session replay and transmitted to ContentSquare SAS's servers in France. No reply of any kind addressed this finding.

Impact: A user's face may be captured and transmitted to a third-party session-replay processor under a consent that covered only the camera-based try-on feature itself, not screen-replay capture of that same camera feed.

Fix: Exclude AR camera try-on screens from ContentSquare's session-replay capture entirely, or obtain a separate, specific consent covering that capture.

C3: ModiFace 65-point facial landmark model constitutes biometric processing under Art. 9

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

assets/MFEFaceTrackerBundle/ contains RoIFANV2Optimized.bin (696KB, a neural network for face alignment), face_detector.bin (459KB), face_contour_65pts.dat (50.8KB, 65 facial landmark points), and Mask_Classifier.bin (60.6KB). These 65 landmark coordinates constitute a biometric profile within the meaning of GDPR Art. 9(1). ModiFace is L'Oreal's AR beauty technology, acting here as a processor.

Whether these landmark coordinates are transmitted off-device to ModiFace/L'Oreal servers or processed purely on-device was explicitly asked and never answered. No reply of any kind addressed this finding.

Impact: Special-category biometric data may be generated, and possibly transmitted off-device, with no confirmed Art. 9(2)(a) explicit consent specific to that processing.

Fix: Confirm and publish whether facial landmark data ever leaves the device, and if so, obtain explicit Art. 9(2)(a) consent specific to that transmission.

H1: Network Security Config: cleartextTrafficPermitted set to a string reference instead of a boolean literal

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

The base configuration reads cleartextTrafficPermitted="@string/clear_text_config". This is a boolean attribute that accepts only true or false; the NSC parser may fail to resolve the reference correctly, causing the attribute to fail silently and fall back to the platform default.

No reply of any kind addressed this finding, including RFI-IRFOS's request to confirm which value the platform actually resolves to at runtime.

Impact: The app's actual cleartext-traffic policy at runtime cannot be confirmed from the manifest alone due to this configuration error.

Fix: Replace the string reference with an explicit boolean literal (true or false) for cleartextTrafficPermitted.

H2: Criteo retargeting based on browsed-but-unpurchased beauty products

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

Criteo (128 smali classes, Paris) tracks which products, foundation shades, perfumes, skincare, a user views without purchasing. Combined with ModiFace try-on data, this could form a linked beauty-preference profile tied to the advertising identifier.

Whether AR try-on interaction data is actually shared with Criteo for retargeting was explicitly asked and never answered.

Impact: Browsing and possibly try-on interaction data may be combined into a beauty-preference profile shared with a third-party retargeting vendor without a confirmed matching disclosure.

Fix: Confirm and disclose whether Criteo receives AR try-on interaction data, not only page-view data.

H3: Missing data_extraction_rules despite WRITE_EXTERNAL_STORAGE permission

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

allowBackup="false" prevents Google Cloud Backup, but data_extraction_rules.xml, which controls device-to-device transfer, is missing. Beauty-loyalty data, purchase history, and locally cached AR session data have no explicit device-to-device backup exclusion.

No reply of any kind addressed this finding.

Impact: Locally cached loyalty, purchase, and AR session data may be included in device-to-device transfers with no explicit exclusion.

Fix: Add a data_extraction_rules.xml excluding loyalty, purchase, and AR session cache data from device-to-device transfer.

One Rejecting Mailbox, Two Silent Mailboxes, Nine Notices

datenschutz@marionnaud.at rejected mail outright on every one of four separate attempts across five weeks (21 June, 27 June, 28 June, 28 July), each time with '550 5.4.1 Recipient address rejected: Access denied.' office@marionnaud.at and presse@marionnaud.at never bounced, but also never responded across nine notices and ninety-one days. Whether either address was ever monitored or forwarded internally remains unconfirmed.

Finding	Provision	Concern

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Three hardcoded API keys, including a Firebase key exposing customer-data risk
C2	GDPR Art. 9(1)/(2)(a), Art. 6(1), Art. 13(1)(e), Art. 25	Session-replay capture of a user's face during AR try-on without matching consent
C3	GDPR Art. 9(1)/(2)(a), Art. 13(1)(c), Art. 5(1)(e)	Biometric facial-landmark processing without confirmed transmission disclosure
H1	GDPR Art. 32(1)(a)	Misconfigured cleartext-traffic attribute, actual runtime value unconfirmable
H2	GDPR Art. 6(1)(a), Art. 13(1)(e)	Undisclosed retargeting combination of browsing and try-on data
H3	GDPR Art. 32	Missing device-to-device backup exclusion for loyalty and purchase data

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@marionnaud.at (rejected) and forwarded to office@marionnaud.at; bcc Austrian DSB and CERT.at
2026-06-27	Follow-up, six days, no reply; datenschutz@ copy bounces again
2026-07-23	Follow-up, twenty-eight days since disclosure, no reply
2026-08-04	Follow-up, forty-five days since disclosure, no reply
2026-08-15	Follow-up, fifty-five days since disclosure, references a three-questions deadline of 12 September
2026-09-06	Final follow-up on file, seventy-seven days, six messages sent, embargo reaffirmed unchanged at 19 September
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Repair the datenschutz@marionnaud.at mailbox so it can receive external GDPR correspondence at all.
- Exclude AR camera try-on screens from ContentSquare’s session-replay capture, or obtain a specific consent covering that capture.
- Confirm and publish whether ModiFace facial landmark data ever leaves the device.
- Replace the string-reference cleartextTrafficPermitted attribute with an explicit boolean literal.
- Rotate all three exposed API keys and restrict them to the correct package name 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. 5, 6, 9, 13, 25, 32. REF AT-MARIONNAUD-2026-R1.