Coordinated Security & Privacy Disclosure, Final Report

ZARA for Android (com.inditex.zara)

Cleartext checkout traffic on twenty production domains, an AR try-on feature uploading body images, eleven notices, zero replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ZERO REPLIES OF ANY KIND

Target	Industria de Diseno Textil, S.A. (Inditex), Arteixo, A Coruna, Spain
Product audited	ZARA for Android, com.inditex.zara, v18.10.1
Disclosure reference	REF ZARA-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase/Maps keys, C2 cleartext production traffic, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Positive Observations 4

4 Findings 4
- 4.1 C1: Hardcoded Firebase and Google Maps API keys in the production APK . . 4
- 4.2 C2: Cleartext HTTP permitted on twenty production domains, including the main storefront 5
- 4.3 H1: Microsoft Clarity: dual-layer session recording including checkout-adjacent screens 5
- 4.4 H2: AR Try-On feature: body images uploaded to Inditex servers, potential undisclosed Art. 9 biometric processing 6
- 4.5 H3: GeofenceBroadcastReceiver: undisclosed in-store physical proximity tracking 6
- 4.6 H4: Privacy Sandbox: five ad-tracking and attribution permission registrations 7

5 Data Protection, Article by Article 7

6 Disclosure Timeline & Outcome 8

7 Residual Risk & Recommendations 9

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production ZARA Android application and identified six findings, two CRITICAL, four HIGH. The most significant: the network security configuration permits cleartext HTTP on 20 production domains, including the main shopping website, the Inditex REST API, and the Inditex CDN, not legacy or test endpoints but the live domains handling product browsing, search, wish lists, authentication sessions, and purchase-adjacent API calls.

Two hardcoded API keys, Firebase and Google Maps, were also extracted from the production binary. Four further findings raise separate concerns: Microsoft Clarity's dual-layer session recording, including session replay of checkout-adjacent screens; an AR Try-On feature uploading body images to Inditex servers with a server-side avatar-generation pipeline, potentially constituting Art. 9 biometric processing; an undisclosed in-store geofencing receiver; and five Privacy Sandbox ad-attribution permissions enabling cross-channel tracking from ad exposure to physical store visit.

Eleven written notices were sent over 90 days. privacy@inditex.com never bounced once and never once replied. All six findings stand exactly as originally reported, with three specific yes/no questions restated nine times across the correspondence and never answered.

Scope: Static analysis of the publicly downloaded production ZARA Android APK, on an authorized test device, only. No Inditex account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@inditex.com, bcc the Austrian DSB and CERT.at. Ten further written notices followed through 16 September 2026, with the Spanish AEPD added to CC as Inditex's home supervisory authority. privacy@inditex.com never bounced once across the entire correspondence, and never once replied.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase and Google Maps API keys in the production APK
C2	CRITICAL	Cleartext HTTP permitted on twenty production domains, including the main storefront
H1	HIGH	Microsoft Clarity: dual-layer session recording including checkout-adjacent screens
H2	HIGH	AR Try-On feature: body images uploaded to Inditex servers, potential undisclosed Art. 9 biometric processing
H3	HIGH	GeofenceBroadcastReceiver: undisclosed in-store physical proximity tracking
H4	HIGH	Privacy Sandbox: five ad-tracking and attribution permission registrations

Subject & Operator Analysis

Industria de Diseno Textil, S.A. (Inditex), headquartered in Arteixo, Spain, operates the ZARA Android application for its global retail customer base.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Hardcoded Firebase and Google Maps API keys in the production APK

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

A complete Firebase project configuration and a Google Maps key are extracted verbatim from the production binary. The Firebase project name, zara-prod, confirms the live production instance.

```
Firebase API Key: AIzaSyAj_8SEZKsHjBcvM2d3kCM-AlJAC713N4o
Firebase Project:  zara-prod
Firebase App ID:   1:250129606065:android:7cc234649a1debc3840990
Storage bucket:    zara-prod.appspot.com
Google Maps Key:   AIzaSyBbwEMIOaQ99StS1vL6Ocd5OnQ7j9k6FFE
```

No response was received naming this finding. The keys enable probing of the project and reading remote config, accessing Firebase Storage, and, if security rules have gaps, reading or writing user-attributed data, plus unrestricted Google Maps API calls billed to Inditex's own cloud account.

Impact: Publicly extractable production credentials enable configuration probing, potential further backend access, and billing abuse.

Fix: Rotate both keys, restrict them to the production certificate fingerprint, and audit Firebase security rules.

C2: Cleartext HTTP permitted on twenty production domains, including the main storefront

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

cleartextTrafficPermitted="true" is set for 20 domains including www.zara.com, itxrest.inditex.com, ws.inditex.com, static.zara.net, static.inditex.com, and Alipay/Chinese-market and Taiwan payment-partner endpoints.

```
www.zara.com          <- main shopping website
itxrest.inditex.com   <- Inditex REST API
ws.inditex.com        <- Inditex WebSocket endpoint
static.zara.net       <- ZARA CDN
static.inditex.com    <- Inditex CDN
alipayobjects.com     <- Alipay, China market
+ 14 further domains (Taiwan payment partners, China-market endpoints)
```

No response was received naming this finding, including the three-part standing question of whether these were fixed at all, and if so, before or after any regulator contact. These are live production endpoints handling product browsing, search queries, wish lists, authentication sessions, and purchase-adjacent API calls, not legacy or test domains. On HTTP fallback, whether from misconfiguration, a proxy, or a TLS-downgrade attempt, session tokens, shopping cart contents, search terms, and address lookups transit unencrypted.

Impact: Twenty production domains, including the primary storefront and checkout-adjacent infrastructure, permit unencrypted fallback for session, cart, and address data.

Fix: Remove all cleartextTrafficPermitted="true" entries and enforce HTTPS with HSTS across all listed domains.

H1: Microsoft Clarity: dual-layer session recording including checkout-adjacent screens

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

711 native Microsoft Clarity smali classes plus a bundled 56.1KB clarity.js in the app's WebView layer together capture all native app interactions and everything inside the shopping catalog, product pages, search, and checkout-adjacent flows, including session replay.

No response was received naming this finding, including whether Clarity is disclosed as a processor. clarity.js transmits via the Beacon API with session and user ID attribution; session replay includes visual playback of full sessions, including payment-adjacent and address-entry screens. All data routes to Microsoft Azure in the US.

Impact: Full-session visual replay, including near-payment and address-entry screens, is transmitted to a US processor with no confirmed gating behind explicit analytics consent.

Fix: Gate Clarity initialization behind explicit analytics consent, disable session replay for checkout and address-entry screens specifically, and name Microsoft in the privacy notice.

H2: AR Try-On feature: body images uploaded to Inditex servers, potential undisclosed Art. 9 biometric processing

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

com.inditex.cfatryon, 1,230 smali classes, includes TROAvatarImage (body image upload), TROPollingData (server-side processing poll), and TROLook (try-on result), indicating body or silhouette images are uploaded to Inditex servers, which generate a virtual avatar via a polling loop.

No response was received naming this finding, including whether an Art. 9(2)(a) legal basis exists. If this pipeline involves body-shape measurement, pose estimation, or facial feature extraction, it constitutes Art. 9(1) biometric data requiring explicit consent. Even limited to 2D overlay, transmission of body photos for commercial fitting requires disclosure of the processing chain and a retention policy for avatar images under Art. 13(1)(c).

Impact: Body images processed through a server-side avatar-generation pipeline may constitute undisclosed special-category biometric data with no confirmed consent basis or retention policy.

Fix: Disclose the full AR Try-On processing chain, document whether measurements or feature vectors are extracted or retained, publish the avatar retention policy, and implement on-device processing where feasible.

H3: GeofenceBroadcastReceiver: undisclosed in-store physical proximity tracking

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

com.inditex.zara.receivers.GeofenceBroadcastReceiver registers ZARA store perimeters and fires callbacks on user enter/exit.

No response was received naming this finding. Combined with purchase history and Microsoft Clarity session data, geofence events create a physical-visit attribution layer linking digital browsing to actual store visits, dwell time, and visit frequency, not disclosed as a named processing activity.

Impact: Physical store visits are attributed to digital browsing behavior through undisclosed geofencing, with no named third-party recipients documented.

Fix: Disclose geofencing explicitly, gate registration behind explicit location consent, and document third-party recipients of geofence event data.

H4: Privacy Sandbox: five ad-tracking and attribution permission registrations

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_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, AD_ID, AD_SERVICES_CONFIG, and android.ext.adservices are all declared.

No response was received naming this finding. Combined with Clarity recording and geofencing, this constructs a cross-channel attribution model: ad exposure to app session recording to physical store visit to purchase, with no disclosed unified consent basis.

Impact: Cross-app advertising attribution linking ad exposure to purchase and physical store visits operates with no disclosed unified consent basis.

Fix: Disclose the cross-channel attribution model explicitly and obtain specific consent for combining ad-attribution, session-recording, and geofence data.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Hardcoded, publicly extractable production credentials
C2	GDPR Art. 32(1)(a), Art. 25, Art. 5(1)(f)	Cleartext HTTP on twenty production domains
H1	GDPR Art. 6(1), Art. 13(1)(e), Art. 46, Art. 25	Undisclosed US session-replay processor
H2	GDPR Art. 9(1)/(2)(a), Art. 13(1)(c), Art. 5(1)(e)	Potential undisclosed biometric processing, body images
H3	GDPR Art. 6(1)(a), Art. 13(1)(c)	Undisclosed in-store geofencing
H4	GDPR Art. 6(1)(a), Art. 5(1)(b)	Undisclosed cross-channel ad attribution

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@inditex.com, bcc Austrian DSB/CERT.at, 6 findings
2026-06-27 / 06-28 / 07-17 / 07-27	Follow-ups; comunicacion@inditex.com added to cc; zero reply
2026-08-09	Follow-up, Austrian DSB and Spanish AEPD added to cc as home/lead supervisory authorities
2026-08-15 / 08-24	Follow-ups restate cleartext finding and three standing yes/no questions
2026-08-31	Weekly SHA-256 binary-diff monitoring instituted for the remainder of the embargo
2026-09-12	Follow-up, day 83, three questions restated for the eighth time
2026-09-16	Final pre-embargo message, zero reply across eight messages confirmed, privacy@inditex.com never bounced once
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Eleven written notices across 90 days produced zero replies of any kind. privacy@inditex.com never bounced once across the entire correspondence, and never once replied. All six findings, including cleartext exposure on twenty live production domains, stand exactly as originally reported.

Residual Risk & Recommendations

- Remove cleartextTrafficPermitted="true" from all twenty listed domains and enforce HTTPS with HSTS; this is the single highest-priority item given the storefront and checkout-adjacent exposure.
- Rotate the Firebase and Google Maps keys and restrict both to the production certificate fingerprint.
- Disclose the AR Try-On processing chain and confirm whether it constitutes Art. 9 biometric processing.
- Gate Microsoft Clarity behind explicit consent and disable session replay on checkout and address-entry screens.
- Disclose in-store geofencing and cross-channel ad attribution as named processing activities with their own consent 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 Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 9, 13, 25, 32, 46. REF ZARA-2026-R1.