Coordinated Privacy Disclosure, Final Report

TK Maxx Android (com.tjx.tkmaxx)

TJX Companies, Inc. (NYSE: TJX), Framingham, Massachusetts, USA

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 92 DAYS AFTER DISCLOSURE, SIXTEEN MESSAGES, MULTIPLE BOUNCES, ZERO REPLY OF ANY KIND

Target	TK Maxx, a European discount retail chain (DE, AT, NL, PL, CZ), Android shopping app
Package	com.tjx.tkmaxx
Operator	TJX Companies, Inc. (NYSE: TJX), Framingham, Massachusetts, USA; TJX European operations for TK Maxx
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	German BfDI, Austrian DSB, CERT.at, EDPS
Total Outbound Messages	16, across 92 days, cycling through five different contact addresses (privacy@tkmaxx.com, privacy@tjx.com, gdpr@tkmaxx.co.uk, data_protection@tjxeurope.com) after repeated bounces before settling on the last.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

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 TJX Companies, Inc. that its TK Maxx Android shopping app ships Dynatrace OneAgent configured to record touch interactions, replay crash sessions including the touch events leading up to them, identify users by linking sessions to account identity, and log business events, purchase flow behavior in a retail checkout context, none of it disclosed as session recording in the app's privacy documentation as reviewed.

A second finding names a structural transparency gap, not a single data flow: Google Tag Manager is integrated, meaning TJX can inject new tracking tags, analytics scripts, conversion pixels, remarketing code, into the running app at any time without submitting an app update through the Play Store's review process. A user who reviewed the app's data-collection practices at install time consented to the binary as it existed then, not to whatever tracking configuration is pushed into it afterward, and any such change is invisible to the user and outside app-store review.

Sixteen messages were sent across 92 days, cycling through four different contact addresses after repeated bounces (privacy@tkmaxx.com, privacy@tjx.com, gdpr@tkmaxx.co.uk, before settling on data_protection@tjxeurope.com), cc'ing the EDPS on one round. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six 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 TK Maxx Android application (com.tjx.tkmaxx, version 1.3.0, 30.9 MB, including the German-market split APK confirming active DE targeting), as pulled via ADB and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with TJX's backend infrastructure was performed.

Disposition

Six findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Dynatrace OneAgent, configured for touch-interaction recording, crash session replay, and user identification inside a retail checkout flow, reaches HIGH on the computed CVSS score alone, no editorial escalation needed. Dual pre-consent SDK initialization (Google ML Kit and Firebase both firing via directBootAware ContentProviders before any consent screen), Google Tag Manager's runtime tracking-injection capability, disproportionate precise-location access, and advertising-attribution tracking all correct to MEDIUM. A missing network security configuration corrects to MEDIUM on its own computed band. Sixteen messages were sent across 92 days, several bouncing before a working address was found. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Google ML Kit and Firebase Both Initialize Before Any Consent Screen

ID	Severity	Title
H1	HIGH	Dynatrace OneAgent Records Touch Interactions and Replays Crash Sessions in a Retail Checkout Flow
H2	MEDIUM	Google Tag Manager Allows Runtime Tracking Injection Without App Store Review
H3	MEDIUM	Precise GPS Location Disproportionate to Disclosed Store-Finder Purpose
H4	MEDIUM	Advertising ID and Attribution Tracking in a Shopping App
M1	MEDIUM	No Network Security Configuration, No Certificate Pinning
M2	OBSERVATIONAL	Boot-Persistent Auto-Start

Subject & Operator Analysis

TK Maxx is a discount retail chain operated by TJX Companies, Inc. (NYSE: TJX), with stores across Germany, Austria, the Netherlands, Poland, and the Czech Republic. The Android app is built on Flutter.

Several genuine positives are worth naming. allowBackup is correctly set to false. usesCleartextTraffic is not set, defaulting correctly to false. No Facebook SDK was found; social-sharing links are static icons only. The camera foreground-service type is justified by the ML Kit barcode scanner for product search. The Flutter cross-platform architecture reduces the native attack surface relative to a fully native app.

Sixteen Messages, Four Addresses, Zero Reply

This case's correspondence record involved repeated address failures before a working channel was found. Early attempts to privacy@tkmaxx.com, privacy@tjx.com, and gdpr@tkmaxx.co.uk bounced across multiple rounds between 25 June and 4 August 2026. From 27 July 2026 onward, data_protection@tjxeurope.com was also tried, and delivery began succeeding consistently from 21 August 2026. Sixteen messages were sent in total across 92 days. Not one reply, automated or human, was ever received on any address, before or after delivery began succeeding.

Findings

C1: Google ML Kit and Firebase 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.

Both MlKitInitProvider (initOrder=99) and FirebaseInitProvider (initOrder=100) are declared directBootAware="true", meaning both initialize at process creation, before any Activity and therefore before any consent screen, and can begin before the device is even fully unlocked. Firebase Analytics and Firebase Remote Config are confirmed compiled into the binary.

```
com.google.mlkit.common.internal.MlKitInitProvider
  android:initOrder=0x63 (99), android:directBootAware=true
com.google.firebase.provider.FirebaseInitProvider
  android:initOrder=0x64 (100), android:directBootAware=true
```

Impact: Two separate SDK bootstraps begin before a shopper has seen a single consent notice, one of them potentially before device unlock.

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

H1: Dynatrace OneAgent Records Touch Interactions and Replays Crash Sessions in a Retail Checkout Flow

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:N/SA:N, 8.7. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

Dynatrace OneAgent is configured, confirmed via SettingsApi.identifyUser, DTXCrash ReplayOptedIn, and EventApi.sendBizEvent, to record touch interactions, replay crash sessions including the touch events that led to them, link sessions to specific user identity, and log business events such as product views, cart additions, and purchases. None of this is disclosed as session recording in the app's privacy documentation as reviewed. Dynatrace, Inc. is a US company subject to the CLOUD Act.

```
com.dynatrace.android.dtxPref -- session persistence
DTXCrashReplayOptedIn -- crash session replay enabled
SettingsApi.identifyUser -- links session to known user identity
EventApi.sendBizEvent -- business event capture (product views, cart, checkout)
"Current screenshot == null, no need to beaconize touches" -- touch recording
```

Impact: A shopper's individual taps, scrolls, and interactions through the checkout flow are recorded and replayable on crash, linked to their identity, and sent to a US-based processor, with no disclosure of session recording anywhere in the app's privacy documentation.

Fix: Disclose Dynatrace session recording, crash replay, and user identification explicitly as data processing activities under Art. 13(1)(e), and document an Art. 28 basis for the Dynatrace relationship. No confirmation that this has occurred was ever received.

H2: Google Tag Manager Allows Runtime Tracking Injection Without App Store Review

---

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

Google Tag Manager is integrated, allowing TJX to push new tracking tags, analytics scripts, conversion pixels, remarketing code, into the running app at any time without a Play Store update. A user who reviewed the app's data practices at install time consented to the binary as it existed then, not to whatever tracking configuration is pushed afterward, invisibly and outside app-store review.

```
com.google.android.gms.tagmanager.ITagManagerApi
```

Impact: The app's actual tracking behavior can change at any time without a visible update, a user notice, or app-store review, meaning consent given at install time cannot meaningfully cover future tag configurations.

Fix: Disclose the use of Google Tag Manager and its runtime tag-injection capability explicitly, and commit to a change-notification process for material tracking updates. No confirmation that this has occurred was ever received.

H3: Precise GPS Location Disproportionate to Disclosed Store-Finder Purpose

---

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_FINE_LOCATION (GPS-precision, roughly 5m accuracy) is declared alongside ACCESS_COARSE_LOCATION. Store-finder functionality is adequately served by coarse location; precise GPS enables geofencing, detecting proximity to specific stores, competitor locations, or retail zones. No disclosure of geofencing or a precision-location purpose was located.

Impact: The app can determine a user's precise location well beyond what finding the nearest store requires, enabling undisclosed geofencing-based behavioral inference.

Fix: Downgrade to ACCESS_COARSE_LOCATION for store-finder functionality, or disclose the specific geofencing purpose requiring GPS precision. No confirmation that this has occurred was ever received.

H4: Advertising ID and Attribution Tracking in a Shopping 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.

AD_ID and the Privacy Sandbox ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION permissions are all declared, enabling cross-app behavioral profiling that links TK Maxx shopping behavior, product views, cart activity, purchases, to a user's broader device usage profile.

Impact: A user's TK Maxx shopping activity can be linked to their advertising profile across other apps on their device, with no disclosed purpose or legal basis located in the app's privacy documentation.

Fix: Document an individual Art. 6(1) legal basis and Art. 13(1)(c) disclosure for the advertising-attribution pipeline. No confirmation that this has occurred was ever received.

M1: No Network Security Configuration, No Certificate Pinning

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.3.

No android:networkSecurityConfig attribute is present in the manifest, and no certificate pinning is observable. A retail app processing purchase flows relies entirely on OS-level TLS validation with no additional transport-security hardening.

Impact: Purchase and account traffic relies solely on default OS certificate validation, with no pinning layer to detect a compromised or misissued certificate in the trust chain.

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

M2: Boot-Persistent Auto-Start

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

RECEIVE_BOOT_COMPLETED is declared with a corresponding BOOT_COMPLETED receiver, meaning the app starts automatically at device boot.

Impact: The app begins running at every device boot without an explicit user launch, a minor transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove it if not load-bearing for a specific, disclosed feature. 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	Dual pre-consent SDK initialization via direct-BootAware Content-Providers.
Art. 5(1)(a), Art. 13(1)(e), Art. 28	H1	Undisclosed session recording, crash replay, and user identification.
Art. 5(1)(a), Art. 13(1)(e)	H2	Runtime tracking-injection capability outside app-store review.
Art. 5(1)(b)/(c), Art. 6(1)	H3	Disproportionate precise-location access for a store-finder function.
Art. 5(1)(b), Art. 6(1)	H4	Undisclosed advertising-attribution tracking.
Art. 32	M1	No network security configuration or certificate pinning on purchase-flow traffic.

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, H1 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; C1, H2, H3, H4, and M1 correct to MEDIUM to match their own computed bands; M2 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: TKMAXX-2026-R1.