



Security & Privacy Disclosure, Final Report

ASOS (com.asos.app)

A hardcoded Firebase key and production database URL ship alongside a fully exposed Braze CRM API key, a complete Android Privacy Sandbox permission stack runs on body-measurement and style-preference data, and two analytics SDKs initialise before OneTrust's own consent dialogue can fire, unresolved through 109 days and a 19-day-overdue embargo, with zero substantive reply across five messages

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28
SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

Target	ASOS plc, London, United Kingdom (LON:ASC)
Package	com.asos.app
Platform Audited	Android, static analysis of the production APK (61,525 smali classes)
Initial Disclosure (R1)	2026-06-30, to dpo@asos.com (bounced, address not found) and security@asos.com (delivered)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (1 Critical, 4 High)
Correspondence	5 messages sent by RFI-IRFOS (one address bounced on R1, the other delivered), 0 substantive replies ever received from ASOS plc
Authorities CC'd	Austrian Datenschutzbehörde (DSB) · European Data Protection Supervisor (EDPS)

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	C1: Hardcoded Firebase key, production database URL, and a fully exposed Braze CRM API key	5
4.2	H1: Full Android Privacy Sandbox stack (Topics, Custom Audiences, Attribution, AD_ID x2) on body-measurement and style-preference data	6
4.3	H2: READ_PHONE_STATE (IMEI access) with no apparent purpose on a fashion shopping app	6
4.4	H3: ContentSquare and Google Mobile Ads initialise before consent, despite OneTrust's CMP being present	7
4.5	H4: Klarna (356 classes), AppsFlyer, Facebook SDK, and four BOOT_COMPLETED receivers	7
5	Impact Analysis	8
6	The Complete Chain: A Bounced DPO Address and 109 Days of Silence at a Working One	8
7	Data Protection – Article by Article	9
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	11

Executive Summary

ASOS plc is a UK-headquartered online fashion retailer. A root-level static analysis of the production Android APK (61,525 smali classes) found five findings, one CRITICAL and four HIGH, notable because they coexist with OneTrust, a real consent management platform that ASOS has genuinely implemented, not because the app lacks privacy tooling altogether.

A Firebase API key and production Realtime Database URL ship hardcoded in every installed copy of the app, alongside a fully exposed Braze CRM API key (d0bf68d2-1d8d-4c54-bfda-bc49cb303311) and its EU endpoint, giving anyone who decompiles the APK direct API access to ASOS's own customer-engagement infrastructure (C1). The app declares all four Android Privacy Sandbox permissions simultaneously (Topics, Custom Audiences, Attribution, AD_ID) plus the legacy AD_ID permission, building interest profiles from clothing browsing patterns that can touch on body image and financial capacity (H1). READ_PHONE_STATE grants IMEI-level device identification with no apparent purpose on a fashion shopping app (H2). ContentSquare's session-analytics SDK and Google Mobile Ads both initialise via ContentProvider before OneTrust's own consent dialogue can fire, an implementation gap rather than an absence of intent (H3). A 356-class Klarna buy-now-pay-later integration, AppsFlyer, Facebook SDK, and four separate BOOT_COMPLETED receivers round out a stack that moves creditworthiness-relevant and cross-app attribution data to US entities (H4).

RFI-IRFOS disclosed these findings on 30 June 2026 to dpo@asos.com and security@asos.com, CC press@asos.com, the Austrian Datenschutzbehoerde, and the European Data Protection Supervisor. The dpo@asos.com address bounced outright, address not found, the same day; security@asos.com received the disclosure without issue. Four further messages followed, restating the findings at 17, 29, 60, and 74 days of silence. Across 109 days and five messages sent to a working address, not one substantive reply was ever received.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase key, production database URL, and a fully exposed Braze CRM API key
H1	HIGH	Full Android Privacy Sandbox stack (Topics, Custom Audiences, Attribution, AD_ID x2) on body-measurement and style-preference data
H2	HIGH	READ_PHONE_STATE (IMEI access) with no apparent purpose on a fashion shopping app
H3	HIGH	ContentSquare and Google Mobile Ads initialise before consent, despite OneTrust's CMP being present
H4	HIGH	Klarna (356 classes), AppsFlyer, Facebook SDK, and four BOOT_COMPLETED receivers

Subject & Operator Context

ASOS plc is a London-headquartered online fashion and beauty retailer, listed on the London Stock Exchange (LON:ASC), with revenue in the region of GBP 3.5 billion and substantial EU customer operations. The Android app (com.asos.app) is the company's primary mobile shopping channel, processing clothing size, style preference, browsing, and payment-adjacent data for a large EU user base.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to dpo@asos.com and security@asos.com, CC press@asos.com, the Austrian Datenschutzbehörde, and the European Data Protection Supervisor. The dpo@asos.com address bounced the same morning with an 'address not found' delivery failure; security@asos.com received the disclosure successfully, and all subsequent correspondence continued to that address.

RFI-IRFOS followed up on 17 July 2026 (17 days of silence), 15 August 2026 (29 days), 29 August 2026 (60 days, a third follow-up restating the full findings list), and 12 September 2026 (74 days, a fourth restatement under REF com.asos.app). Each follow-up restated the open findings and the specific questions asked in the original disclosure. No message across this five-message, 109-day record ever received a substantive reply from ASOS plc.

Findings

C1: Hardcoded Firebase key, production database URL, and a fully exposed Braze CRM API key

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — direct API access to ASOS's own CRM infrastructure available to anyone who decompiles the APK

```
google_api_key: AIzaSyBjDhrCleBF1kf0oCbHggHWRq0HAHDWhPI
firebase_database_url: https://api-project-498109357888.firebaseio.com
com_braze_api_key: d0bf68d2-1d8d-4c54-bfda-bc49cb303311
com_braze_custom_endpoint: sdk.fra-02.braze.eu
Braze SDK footprint: 523 smali classes
```

Impact: A Firebase API key (AIzaSyBjDhrCleBF1kf0oCbHggHWRq0HAHDWhPI) and a production Realtime Database URL (api-project-498109357888.firebaseio.com) ship hardcoded in every installed copy of the APK. Alongside them, a Braze CRM API key (d0bf68d2-1d8d-4c54-bfda-bc49cb303311) is hardcoded next to 523 Braze smali classes, the full CRM platform covering push campaigns, in-app messaging, behavioural analytics, and user segments. The EU endpoint (sdk.fra-02.braze.eu) is a genuine data-residency positive, but it does not address the exposure of the key itself: anyone who decompiles the APK has direct API access to ASOS's own Braze CRM infrastructure.

H1: Full Android Privacy Sandbox stack (Topics, Custom Audiences, Attribution, AD_ID x2) on body-measurement and style-preference data

HIGH (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, 5.3)
— interest profiling from fashion browsing patterns that can touch body image and financial capacity, potentially engaging Art. 9

```
ACCESS_ADSERVICES_TOPICS
ACCESS_ADSERVICES_CUSTOM_AUDIENCE
ACCESS_ADSERVICES_ATTRIBUTION
ACCESS_ADSERVICES_AD_ID
com.google.android.gms.permission.AD_ID
```

Impact: The app declares all four Android Privacy Sandbox permissions simultaneously (ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_CUSTOM_AUDIENCE, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID), plus the legacy com.google.android.gms.permission.AD_ID. On a fashion app that holds clothing sizes, style preferences, and browsing patterns, the Topics API builds interest profiles from product-category browsing and Custom Audiences builds cross-app retargeting segments from shopping behaviour. In a fashion context, interest inference can touch on body image, health, and spending capacity, areas where Art. 9(1) special categories may be engaged.

H2: READ_PHONE_STATE (IMEI access) with no apparent purpose on a fashion shopping app

HIGH (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, 5.3)
— a non-resettable hardware identifier available for persistent cross-session tracking

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

Impact: android.permission.READ_PHONE_STATE grants access to the device's hardware identifier (IMEI/MEID). On a fashion shopping app there is no apparent use case requiring persistent hardware-level device identification. IMEI is a non-resettable identifier that survives factory resets, meaning it can serve as a persistent cross-session tracking identifier outside the user's control.

H3: ContentSquare and Google Mobile Ads initialise before consent, despite OneTrust's CMP being present

HIGH (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, 5.3)
 — a real consent management platform exists but is not enforced at SDK initialisation time

```
com.contentsquare.android.internal.features.initialize.AutoStart (ContentProvider)
com.google.android.gms.ads.MobileAdsInitProvider, initOrder=100
com.onetrust.otpublishers (OneTrust CMP, present)
ContentSquare footprint: 27 smali classes
```

Impact: ContentSquare (27 classes, session analytics and heatmaps) initialises via a CSAutoStart ContentProvider, and Google Mobile Ads initialises with initOrder=100. Both fire before the user reaches OneTrust's consent screen, before any consent signal can be collected or applied. OneTrust is genuinely present in the APK as a consent management platform, which makes this finding an implementation gap rather than an absence of intent, the CMP is architecturally present but not enforced at SDK initialisation.

H4: Klarna (356 classes), AppsFlyer, Facebook SDK, and four BOOT_COMPLETED receivers

HIGH (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, 5.9)
 — creditworthiness-relevant buy-now-pay-later data and cross-app attribution data transferred to US entities

```
Klarna (Stockholm) BNPL SDK: 356 smali classes
AppsFlyer SDK: cross-app attribution and conversion tracking
Facebook SDK: cross-app attribution and conversion tracking
BOOT_COMPLETED receivers declared: 4
```

Impact: RFI-IRFOS blast-radius escalation: scored at the upper end of the HIGH band rather than the baseline 5.3 used for H1-H3, because this finding combines three independent third-party data flows (Klarna, AppsFlyer, Facebook) with four BOOT_COMPLETED autostart receivers in one app, widening both the data-sensitivity profile (creditworthiness assessment via Klarna's buy-now-pay-later integration) and the consent-timing exposure relative to the other HIGH findings. Klarna's 356-class Stockholm-based BNPL integration involves creditworthiness assessment and instalment profiles on EU customers. AppsFlyer and Facebook SDK provide cross-app attribution and conversion tracking. Four separate BOOT_COMPLETED receivers start components at device boot. All three integrations require documented legal bases and, where applicable, GDPR Art. 28 data processing agreements, and all three route data to US-based corporate entities (Klarna US, Facebook US, AppsFlyer US).

Impact Analysis

This report's single CRITICAL finding and four HIGH findings share a pattern distinct from a typical privacy audit: ASOS has genuinely invested in consent infrastructure, OneTrust is present, the Braze endpoint is EU-resident, and the company is large enough to carry real GDPR accountability obligations, yet every finding here sits alongside that investment rather than in its absence. C1 is a plain security-hygiene failure, a hardcoded key family exposing CRM infrastructure to anyone who decompiles the app, independent of any consent question. H1 and H2 are data-minimisation and purpose-limitation gaps on sensitive-adjacent fashion data. H3 is the clearest illustration of the pattern: the CMP exists, but two SDKs do not wait for it. H4 widens the third-country-transfer and creditworthiness-data surface with a financial-services integration.

What ties all five findings together procedurally is the same failure that affected every other message in this record: a disclosure sent to the company's own published DPO address bounced outright, and once a working channel was found, four further restatements over 109 days produced zero substantive engagement from a GBP 3.5 billion public company.

The Complete Chain: A Bounced DPO Address and 109 Days of Silence at a Working One

Step 1 – Disclosure sent, partial bounce: RFI-IRFOS sends the full disclosure on 30 June 2026 to dpo@asos.com and security@asos.com, CC press@asos.com, the Austrian Datenschutz zbehoerde, and the EDPS. dpo@asos.com bounces the same morning, address not found. security@asos.com receives the disclosure without issue.

Step 2 – Seventeen days, first follow-up: On 17 July 2026, RFI-IRFOS follows up to security@asos.com, noting the dpo@asos.com bounce and restating the findings. No reply.

Step 3 – Twenty-nine days, second follow-up: On 15 August 2026, RFI-IRFOS follows up again. No reply.

Step 4 – Sixty days, third follow-up: On 29 August 2026, RFI-IRFOS sends a third follow-up restating the full findings list. No reply.

Step 5 – Seventy-four days, fourth restatement: On 12 September 2026, RFI-IRFOS sends a fourth restatement under REF com.asos.app. No reply.

Step 6 – Embargo reached and passed: The embargo, stated as 2026-09-28 in the original disclosure, passes with all five findings unaddressed.

Step 7 – Publication: This report publishes 19 days after the embargo date. Across 109 days and five messages sent, one address bounced outright and the other, working throughout, never once produced a substantive reply.

Data Protection – Article by Article

Art. 32(1)(b), Art. 25 GDPR – Security of processing and data protection by design: C1's hardcoded Firebase and Braze CRM keys fall short of the technical measures and by-design minimisation these provisions require.

Art. 5(1)(b), Art. 6(1), Art. 13, potentially Art. 9(1) GDPR – Purpose limitation, lawfulness, transparency, and special categories: H1's full Privacy Sandbox stack on fashion browsing data raises all four in combination.

Art. 5(1)(c), Art. 13 GDPR – Data minimisation and transparency: H2's READ_PHONE_STATE /IMEI access has no disclosed purpose proportionate to a fashion shopping app.

Art. 7 GDPR – Conditions for consent: H3's pre-consent SDK initialisation defeats the purpose of the OneTrust CMP that is otherwise present.

Art. 28, Art. 44-49 GDPR – Processor agreements and third-country transfers: H4's Klarna, AppsFlyer, and Facebook integrations all transfer data to US entities.

Regulatory & Legal Landscape

ASOS plc is headquartered in London, with substantial EU customer operations bringing it within GDPR's territorial scope under Art. 3(2). RFI-IRFOS informed the Austrian Datenschutzbehörde (DSB) and the European Data Protection Supervisor (EDPS) of these findings per GDPR Art. 83(2)(b) at the time of the original disclosure.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 5, 6, 9, and 13 issues in H1 and H2, and to the Art. 7 issue in H3, up to EUR 20,000,000 or 4% of total worldwide annual turnover, a meaningful figure against ASOS's approximately GBP 3.5 billion revenue. Art. 83(4) applies to the Art. 32, 25, and 28 issues in C1 and H4, up to EUR 10,000,000 or 2% of total worldwide annual turnover. A public company of this size, with a genuinely implemented CMP already in place, is well positioned to close the gap between having the tooling and fully enforcing it.

Indicators of Compromise

The following identifiers, SDK packages, and permissions were extracted from the production APK via static analysis only. No ASOS servers, accounts, or infrastructure were probed.

```
C1 -- google_api_key: AIzaSyBjDhrCleBF1kf0oCbHggHWRq0HAHDWhPI
    firebase_database_url: https://api-project-498109357888.firebaseio.com
    com_braze_api_key: d0bf68d2-1d8d-4c54-bfda-bc49cb303311 (523 classes)

H1 -- ACCESS_AD SERVICES_TOPICS, ACCESS_AD SERVICES_CUSTOM_AUDIENCE,
    ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID, legacy AD_ID

H2 -- android.permission.READ_PHONE_STATE

H3 -- com.contentsquare.android.internal.features.initialize.AutoStart,
    com.google.android.gms.ads.MobileAdsInitProvider (initOrder=100)

H4 -- Klarna BNPL SDK (356 classes), AppsFlyer, Facebook SDK,
    4x BOOT_COMPLETED receivers
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to dpo@asos.com (bounced, address not found) and security@asos.com (delivered), CC press@asos.com, the Austrian DSB, and the EDPS. Embargo stated as 2026-09-28.

2026-07-17 First follow-up, 17 days of silence. No reply.

2026-08-15 Second follow-up, 29 days of silence. No reply.

2026-08-29 Third follow-up, 60 days of silence, full findings restated. No reply.

2026-09-12 Fourth restatement, 74 days of silence, under REF com.asos.app. No reply.

2026-09-28 Embargo date reached. Correspondence record: five RFI-IRFOS messages, one bounce, zero substantive replies.

2026-10-17 This report published, 19 days after the embargo date. All five findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 – Immediate: rotate the exposed Firebase and Braze CRM API keys, restrict them by package name and signing certificate, and enforce Firebase App Check to prevent replay from outside the genuine app.

H1 – Near-term: document the Art. 6(1) legal basis and conduct an Art. 35 DPIA for Topics and Custom Audiences profiling on fashion-category browsing data, given its potential proximity to Art. 9(1) special categories.

H2 – Near-term: remove READ_PHONE_STATE unless a specific, disclosed purpose requires IMEI-level identification; if no such purpose exists, this permission should simply be dropped.

H3 – Immediate: gate ContentSquare's CSAutoStart ContentProvider and Google Mobile Ads initialisation behind the OneTrust consent decision, closing the gap between having a CMP and enforcing it.

H4 – Near-term: document Art. 28 processing agreements and Art. 44-49 transfer safeguards for Klarna, AppsFlyer, and Facebook, and review whether all four BOOT_COMPLETED receivers are necessary.

Across all findings: correct the dpo@asos.com routing failure, since the address a regulator or researcher is most likely to use for a formal GDPR notice was the one that bounced outright.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the pub-

lished application using publicly available tooling. No ASOS servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF ASOS-2026.