



Security & Privacy Disclosure, Final Report

Zalando for Android (de.zalando.mobile)

Europe's largest fashion e-commerce platform hardcodes a production Firebase key, ships zero certificate pinning on a payment-processing app, and routes undisclosed voice and behavioral data through a WebView bridge and a US marketing cloud, unresolved through 119 days and a 28-day-overdue embargo, with no reply ever from its own dedicated privacy channel

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 19 SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED

Target	Zalando SE, Valeska-Gert-Strasse 5, 10243 Berlin, Germany (XETRA: ZAL)
Package	de.zalando.mobile
Platform Audited	Android · v26.11.1 (versionCode 2130), static analysis of the production APK
Initial Disclosure (R1)	2026-06-20 (REF ZALANDO-2026)
Disclosure / Embargo Date	2026-09-19
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (2 Critical, 3 High)
Correspondence	10 messages sent by RFI-IRFOS across six fragmented threads, approximately 9 automated customer-service/press-team autoresponses received, 0 substantive replies from the dedicated privacy channel (datenschutz@zalando.de) or any named human
Authorities BCC'd / CC'd	Austrian Datenschutzbehoerde (DSB) · CERT.at · Berliner Beauftragte fuer Datenschutz und Informationsfreiheit (BlnBDI, lead supervisory authority) · German BfDI · Zalando press (presse@zalando.de)

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	6
4	Findings	6
4.1	C1: Firebase production API key and Realtime Database URL hardcoded in the production binary	6
4.2	C2: No certificate pinning on any API domain despite TLS-only external traffic	7
4.3	H1: Virtual Assistant (87 classes): voice shopping queries via WebView JS bridge, data scope and destination undisclosed	7
4.4	H2: Adjust (248 classes) + com.adjust.preinstall.READ_PERMISSION: attribution tracking begins before first app open	8
4.5	H3: Braze (611 classes, US): detailed purchase and browsing behavioral profile to a US marketing cloud	9
5	Impact Analysis	9
6	The Complete Chain: A Disclosure That Never Found a Human, Across Six Threads and 119 Days	10
7	Data Protection — Article by Article	11
8	Regulatory & Legal Landscape	11
9	Indicators of Compromise	12
10	Disclosure Timeline & Outcome	12
11	Residual Risk & Recommendations	13

Executive Summary

Zalando SE is Europe's largest fashion e-commerce platform, XETRA-listed, processing purchase history, style preferences, body-size data, browsing behavior, and wishlist data for more than 50 million active users. Its Android application, `de.zalando.mobile` (v26.11.1), was found during this audit to have a materially stronger security baseline than most apps in RFI-IRFOS's current research series: no session-replay SDK, no debug HTTP interceptor, no Chinese SDKs in functional capacity, no location tracking, and a near-current `targetSdk` of 35. The five findings in this report are the delta between that baseline and a fully correct implementation, not evidence of a generally neglected app.

Static analysis identified five findings, two CRITICAL and three HIGH. A Google API key and Firebase Realtime Database URL are hardcoded in the production binary (C1). The app's Network Security Configuration correctly blocks cleartext traffic but defines no domain-specific certificate pin-sets for `zalando.de`, Adjust, or Braze, leaving every connection, including payment confirmations and Virtual Assistant voice data, reliant on system CA validation alone (C2). A voice-powered Virtual Assistant (87 smali classes) processes shopping queries through a WebView JavaScript bridge whose server-side behavior can change without a new APK release, leaving the scope and destination of voice data undocumented and unauditable from static review (H1). Adjust (248 classes) declares `com.adjust.preinstall.READ_PERMISSION`, confirming pre-installation attribution agreements with device partners that begin collecting referral data before the user has ever opened the app or seen a privacy notice (H2). Braze (611 classes, Braze Inc., New York) receives a detailed behavioral profile of items viewed, wishlisted, purchased, and sizes selected, a US transfer with no documented Art. 44 safeguard (H3).

RFI-IRFOS disclosed these findings on 20 June 2026 under REF ZALANDO-2026 to `datenschutz@zalando.de`, BCC the Austrian DSB, CERT.at, and the Berliner Beauftragte fuer Datenschutz und Informationsfreiheit (BlnBDI, Zalando's lead supervisory authority). Across the following 72 days RFI-IRFOS sent nine further messages, fragmented across six separate email threads because Zalando's customer-service system does not preserve subject-line continuity and repeatedly misrouted a security and GDPR disclosure through its order-complaint intake flow, at one point asking RFI-IRFOS to confirm an order number for a report that explicitly stated no order exists. The dedicated privacy channel, `datenschutz@zalando.de`, directly addressed or CC'd on at least seven of these ten messages, never once replied, not even with an automated acknowledgment. The only responses received were generic customer-service and press-team autoresponders. The stated embargo of 19 September 2026 passed 28 days ago with all five findings unaddressed.

ID	Severity	Title
C1	CRITICAL	Firebase production API key and Realtime Database URL hardcoded in the production binary
C2	CRITICAL	No certificate pinning on any API domain despite TLS-only external traffic
H1	HIGH	Virtual Assistant (87 classes): voice shopping queries via WebView JS bridge, data scope and destination undisclosed

ID	Severity	Title
H2	HIGH	Adjust (248 classes) + com.adjust.preinstall.READ_PERMISSION: attribu- tion tracking begins before first app open
H3	HIGH	Braze (611 classes, US): detailed purchase and brows- ing behavioral profile to a US marketing cloud

Subject & Operator Context

Zalando SE is Europe's largest fashion e-commerce platform, headquartered in Berlin, Germany, and listed on the XETRA exchange. Its Android app is used by more than 50 million active shoppers to browse, purchase, and manage returns for clothing, footwear, and accessories, and processes purchase history, payment confirmations, style preferences, and size data as a routine part of that function.

This audit is unusual in this disclosure series for a reason worth stating plainly: Zalando's overall security baseline is genuinely strong. No session-replay SDK, no production debug interceptor, no Chinese SDK in functional capacity, no location permission, and a near-current targetSdk were found, all of which exceed the median of the 30-app research series this audit belongs to. The five findings below are specific, fixable gaps, not evidence of a neglected codebase, and RFI-IRFOS said as much in the original disclosure. What has not been fixable, over 119 days, is getting any of the five findings in front of a human being who could act on them.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 20 June 2026 under REF ZALANDO-2026 to datenschutz@zalando.de, BCC the Austrian DSB, CERT.at, and the BlnBDI (Zalando's lead supervisory authority, since Zalando SE is headquartered in Berlin). No reply followed within seven days; a follow-up was sent 27 June 2026 to the same address, CC presse@zalando.de, restating the two most severe findings and setting a 29 June 2026 deadline.

From this point the correspondence fragments. Zalando's generic contact system does not preserve subject-line threading: every message to datenschutz@zalando.de, service@zalando.de, or privacy@zalando.nl triggers a new, unthreaded auto-acknowledgment from donotreply@zalando.de, and several of RFI-IRFOS's follow-ups were met with customer-service templates asking to confirm an order number, a full name, or account access details, despite each message stating explicitly that no order exists and that the correspondence concerns a security and data-protection disclosure. RFI-IRFOS sent further messages on 28 June, 23 July, 25 July (clarifying the order-confirmation confusion directly: 'wir haben keine bestellung, wir waren nie kundschaft'), 29 July (twice, including a formalized re-statement of the full disclosure after the order-intake misrouting), 9 August, and twice on 31 August 2026, the second of which was sent to privacy@zalando.nl after Zalando's own auto-responder named that address as a verified data-protection channel. In total, ten messages were sent across six separate email threads. The dedicated privacy mailbox, datenschutz@zalando.de, was a direct recipient or CC on at least seven of them and never replied once, not even with an automated acknowledgment; every response received came from the generic customer-service or press-team systems. The stated embargo of 19 September 2026 passed 28 days before this report's publication date, with zero substantive engagement from any named human across the full 119-day correspondence record.

Findings

C1: Firebase production API key and Realtime Database URL hardcoded in the production binary

CRITICAL (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) — unauthenticated backend reachable via a hardcoded key on a 50M-user payment-processing platform, blast-radius escalated from MEDIUM

```
res/values/strings.xml
google_api_key = AIzaSyAxJUruTieZzY86Ny70sUwYaSAiY8kJcTo
firebase_database_url = https://api-project-960858143323.firebaseio.com
gcp_project_id = 960858143323 (raw Google Cloud project number)
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the key and its associated Realtime Database URL (api-project-960858143323.firebaseio.com) are extractable from the publicly distributed APK in under 60 seconds, and Zalando is a payment-processing platform used by more than 50 million people, where the correctness of Firebase security-rule restrictions is self-administered and not independently verifiable by an external party who has only extracted the key from a Play Store download. For a

XETRA-listed company at this scale, the burden of demonstrating adequate restriction sits with Zalando, not with the researcher who found the key.

C2: No certificate pinning on any API domain despite TLS-only external traffic

CRITICAL (CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 6.8) — a rogue CA-signed certificate can intercept payment confirmations and Virtual Assistant voice data, blast-radius escalated from MEDIUM

```
res/xml/network_security_config.xml
cleartextTrafficPermitted=false, exceptions: 127.0.0.1 only (correct)
<pin-set> entries found for: NONE
Domains relying on system CA validation only:
    zalando.de, adjust.com, Braze endpoints, all other API hosts
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.8 to CRITICAL because the Network Security Configuration does the hard part correctly, cleartext traffic is restricted to localhost, but defines zero domain-specific pin-sets for zalando.de, Adjust, or Braze, meaning every connection relies solely on system CA validation. On a platform processing purchase history, payment-method data, and address data for 50M+ users, with a Virtual Assistant whose voice queries already carry undisclosed-destination risk (see H1), a compromised or rogue CA-signed certificate on a shared network (airport, cafe, corporate Wi-Fi) is sufficient to intercept all of it. GDPR Art. 32(1)(a) requires technical measures proportionate to what is being protected, and nothing here is pinned.

H1: Virtual Assistant (87 classes): voice shopping queries via WebView JS bridge, data scope and destination undisclosed

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, 5.1) — voice data processing scope and server-controlled behavior cannot be determined or audited from the shipped APK

```
de.zalando.mobile.features.virtualassistant.screen.impl.internal.feature.
    VirtualAssistantFragment
de.zalando.mobile.features.virtualassistant.screen.impl.internal.feature.
    VirtualAssistantFragment$virtualAssistantWebInterface$2$1
de.zalando.mobile.features.virtualassistant.screen.impl.internal.feature.
    VirtualAssistantFragment$h
de.zalando.mobile.features.virtualassistant.screen.impl.internal.feature.
    VirtualAssistantFragment$k
```

```
Permissions active: RECORD_AUDIO, MICROPHONE
Voice-data destination: undetermined from static analysis,
    not disclosed in privacy notice
```

Impact: Zalando ships a voice-powered Virtual Assistant (VirtualAssistantFragment, virtualAssistantWebInterface, 87 smali classes) running inside a WebView with a JavaScript bridge.

RECORD_AUDIO and MICROPHONE are active, but whether voice queries are transcribed on-device, sent to Zalando's own backend, or routed to a third-party ASR provider is not determinable from static analysis and is not disclosed in the privacy notice. Because the assistant's behavior is server-updatable through the JS bridge without a new APK release, the processing scope accepted by users at onboarding cannot account for behavior added post-install. Voice queries to a shopping assistant routinely contain body-size descriptions, style preferences, budget, and personal occasion context (a request for an outfit for a specific event), none of which is covered by a documented, stable processing purpose.

H2: Adjust (248 classes) + com.adjust.preinstall.READ_PERMISSION: attribution tracking begins before first app open

HIGH (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, 4.6)
— pre-installation attribution collects referral data before any privacy notice is shown, on OEM/carrier pre-loaded devices

```
AndroidManifest.xml
  <uses-permission android:name="com.adjust.preinstall.READ_PERMISSION" />

Adjust SDK: 248 classes (Adjust GmbH, Berlin / AppLovin Corp., US)
OEM/carrier partners, data points, retention period: not disclosed
```

Impact: The declared com.adjust.preinstall.READ_PERMISSION confirms Zalando has pre-installation attribution agreements with device manufacturers or carriers. On devices where Zalando ships pre-loaded, Adjust (248 classes, Adjust GmbH, Berlin, now owned by AppLovin Corp., US) reads referral attribution data before the user has ever opened the app, seen a privacy notice, or given any consent. The specific OEM/carrier partners, the data points collected at pre-install time, and the retention period are not disclosed anywhere identified during this audit. Art. 13(1)(a) requires the controller's identity and processing purpose to be communicated at the time of collection, which for pre-install attribution is before first open; Art. 25(1) requires this kind of tracking to be minimised to what is strictly necessary by design.

H3: Braze (611 classes, US): detailed purchase and browsing behavioral profile to a US marketing cloud

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, 5.1) — US third-country transfer of a fashion behavioral profile with implied body-size data, no Art. 44 safeguard identified

Braze SDK: 611 classes (Braze Inc., New York, US)
 Events observed: item_viewed, item_wishlisted, item_purchased,
 category_browsed, size_selected, promo_interacted
 Art. 44 transfer safeguard: not identified

Impact: Braze (Braze Inc., New York, 611 classes) is Zalando's marketing-automation platform, receiving behavioral events including items viewed, items wishlisted, items purchased, categories browsed, and sizes selected. Combined over time, this is a detailed fashion-preference profile with implied body-measurement data, held by a US company with no EU adequacy decision. Art. 44 requires a documented transfer safeguard (such as Standard Contractual Clauses) for this data reaching the US, and no such safeguard was identified in Zalando's available disclosures during this audit. Art. 13(1)(e)(f) requires Braze to be individually named as a recipient with the categories of data shared; Art. 5(1)(b) requires its own legal basis for using a detailed behavioral profile for marketing automation beyond order fulfillment.

Impact Analysis

Zalando is an unusual case in this disclosure series: the overall engineering baseline is genuinely strong, and the two CRITICAL findings are both compounding issues (a hardcoded key on a payment-processing app at 50M-user scale; a missing-pinning gap on the same payment flows plus an already-opaque voice feature) rather than evidence of a neglected codebase. The three HIGH findings share a common shape: each is a real, identifiable data flow (voice queries, pre-install attribution, a US marketing profile) that is technically present and functioning, but not disclosed to users in a way that satisfies Art. 13's transparency requirement.

What makes this case distinctive is not the technical findings but the correspondence failure around them. Zalando directly addressed its own dedicated privacy mailbox, datenschutz@zalando.de, on at least seven of ten messages sent over 72 days, and that mailbox never replied once, not even with an automated acknowledgment. Every reply received came from systems designed for order complaints or press inquiries, neither of which is equipped to engage with a GDPR disclosure, and the order-complaint system twice asked RFI-IRFOS to confirm an order number for a report that explicitly stated no order exists.

The Complete Chain: A Disclosure That Never Found a Human, Across Six Threads and 119 Days

Step 1 — Disclosure sent: RFI-IRFOS sends the original findings to datenschutz@zalando.de on 20 June 2026 under REF ZALANDO-2026, BCC the Austrian DSB, CERT.at, and the BlnBDI, Zalando's lead supervisory authority.

Step 2 — First follow-up, first auto-ack: On 27 June 2026, seven days with no reply, RFI-IRFOS follows up to the same address, CC presse@zalando.de, with a 29 June deadline. The only response is a generic 'Ihre Nachricht an Zalando' auto-acknowledgment from donotreply@zalando.de, unconnected to the actual content.

Step 3 — The order-complaint system takes over: A further follow-up on 28 June references the still-unanswered acknowledgment. From late July, Zalando's customer-service system begins actively misrouting the correspondence: on 25 July and 29 July, RFI-IRFOS receives templates asking it to confirm a full name, account access, or an order number, each time against a report that opens by stating no order was ever placed. RFI-IRFOS replies plainly on 25 July: 'wir haben keine bestellung. wir waren nie kundschaft.'

Step 4 — Re-statement and escalation: On 29 July, RFI-IRFOS sends a formalized re-statement of the full disclosure directly to service@zalando.de, CC datenschutz@zalando.de and the regulator BCC list, after Zalando's own system auto-generates an 'ESCALATION' ticket notice citing 37 days of silence, an escalation triggered by Zalando's own process, not by any human review.

Step 5 — A new address, same silence: On 9 August and twice on 31 August 2026, RFI-IRFOS sends further follow-ups, the second of 31 August addressed to privacy@zalando.nl after an auto-responder names it as a verified data-protection channel. No reply of any kind, human or automated, follows from either datenschutz@zalando.de or privacy@zalando.nl at any point in the entire record.

Step 6 — Embargo reached, then passed: The stated embargo of 19 September 2026 passes with the correspondence record unchanged: ten messages sent, roughly nine generic autore-sponses received, zero substantive replies.

Step 7 — Publication: This report publishes 28 days after the embargo date, on the terms stated from the first message.

Across 119 days, the only Zalando systems that responded at all were systems built to handle order complaints and press inquiries. The system built specifically to receive this kind of report, the dedicated privacy mailbox, never responded once.

Data Protection — Article by Article

Art. 32(1)(b) GDPR — Security of processing, confidentiality: C1's hardcoded Firebase key and database URL fall short of the technical measures Art. 32 requires for a payment-processing app at 50M-user scale.

Art. 32(1)(a) GDPR — Security of processing, pseudonymisation/encryption-equivalent measures: C2's absence of any certificate pin-set leaves payment and voice-assistant traffic reliant on system CA validation alone.

Art. 13 GDPR — Information to be provided, transparency: H1's Virtual Assistant voice-data destination and H3's Braze third-country recipient are both undisclosed processing details that Art. 13 requires to be communicated.

Art. 25(1) GDPR — Data protection by design: H2's pre-installation attribution tracking begins before any privacy notice can act, the opposite of privacy by design.

Art. 44 GDPR — General principle for transfers: H3's Braze data flow to a US company has no documented Art. 46 safeguard identified in Zalando's available disclosures.

Regulatory & Legal Landscape

Zalando SE is headquartered in Berlin, Germany, placing it under the lead supervisory authority of the Berliner Beauftragte fuer Datenschutz und Informationsfreiheit (BInBDI), BCC'd on the original disclosure and every substantive follow-up. The Austrian DSB and CERT.at were also BCC'd throughout, given RFI-IRFOS's Austrian registration and the cross-border nature of a platform operating in Austria.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 security-of-processing issues in C1 and C2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 13 transparency and Art. 44 transfer issues in H1 and H3, up to EUR 20,000,000 or 4% of total worldwide annual turnover. For a XETRA-listed company with Zalando's market capitalisation, the 4% tier is the materially larger exposure. That the dedicated privacy channel never once responded, across ten messages and 119 days, while BInBDI was BCC'd on substantially all of them, is itself a fact relevant to any regulator assessing institutional engagement with a disclosed finding.

Indicators of Compromise

The following identifiers, SDK packages, and credentials were extracted from the production APK (v26.11.1, versionCode 2130) via static analysis only. No Zalando servers, accounts, or infrastructure were probed.

```
C1 -- google_api_key AIzaSyAxJUruTieZzY86Ny70sUwYaSAiY8kJcTo,  
    firebase_database_url api-project-960858143323.firebaseio.com  
  
C2 -- network_security_config.xml, zero <pin-set> entries for any  
    external domain  
  
H1 -- de.zalando.mobile.features.virtualassistant.* (87 classes),  
    RECORD_AUDIO + MICROPHONE  
  
H2 -- com.adjust.preinstall.READ_PERMISSION, Adjust SDK (248 classes)  
  
H3 -- Braze SDK (611 classes, Braze Inc., New York, US)
```

Disclosure Timeline & Outcome

2026-06-20 Initial disclosure sent under REF ZALANDO-2026 to datenschutz@zalando.de. BCC: Austrian DSB, CERT.at, BlnBDI.

2026-06-27 Follow-up sent to datenschutz@zalando.de, CC presse@zalando.de, 29 June deadline set. Auto-acknowledgment received from donotreply@zalando.de; no substantive reply.

2026-06-28 Further follow-up referencing the unacknowledged deadline. No reply.

2026-07-23 Follow-up noting 26 days since the auto-acknowledgment, CC Austrian DSB. No reply.

2026-07-25 Zalando's customer-service system requests order/account confirmation; RFI-IRFOS clarifies no order exists. No substantive reply follows.

2026-07-29 Zalando's system auto-generates an escalation ticket citing 37 days of silence. RFI-IRFOS sends a formalized re-statement of the full disclosure to service@zalando.de, CC datenschutz@zalando.de and the regulator BCC list, same day.

2026-08-09 Follow-up sent to service@zalando.de, CC datenschutz@zalando.de, BlnBDI, Austrian DSB, presse@zalando.de. No reply.

2026-08-31 Two further follow-ups, the second addressed to privacy@zalando.nl following an auto-responder's naming of that address as a verified channel. No reply from either address.

2026-09-19 Stated embargo date reached. The correspondence record shows ten RFI-IRFOS messages, roughly nine generic autoresponses, and zero substantive replies.

2026-10-17 This report published, 28 days after the embargo date. All five findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 — Immediate: Rotate the hardcoded Firebase API key and database URL, and confirm the associated Firebase project's security rules require authentication for all read and write operations.

C2 — Immediate: Add domain-specific certificate pin-sets for zalando.de, Adjust, and Braze endpoints, particularly given the volume of payment and voice-assistant traffic these connections carry.

H1 — Near-term: Document the Virtual Assistant's voice-data processing chain explicitly, including whether a third-party ASR provider is used, and ensure the privacy notice is updated whenever server-side behavior changes expand the assistant's data collection.

H2 — Near-term: Disclose the specific OEM/carrier pre-install attribution partners, the data points collected, and the retention period; evaluate whether pre-install tracking can be deferred until after the first privacy notice is shown.

H3 — Near-term: Name Braze individually as a data recipient with a documented Art. 44 transfer safeguard in the privacy notice.

Across all findings: establish a monitored path for security and data-protection disclosures that does not depend on datenschutz@zalando.de alone. Over 119 days and ten messages, every reply Zalando sent came from a system built for order complaints or press inquiries; the mailbox built specifically to receive this kind of report never responded once, a process gap worth correcting independently of the five technical findings in this report.

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 root-level analysis of

the published application using publicly available tooling. No Zalando 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 ZALANDO-2026.