Coordinated Security & Privacy Disclosure, Final Report

Starbucks Austria for Android (com.starbucks.at, EMEA edition, v9.6.6204)

Six written notices across two channels, ninety-one days, one reply that redirected to a bug-bounty programme

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

Target	Starbucks Coffee Company, Seattle, USA – Austrian market app
Product audited	Starbucks Austria for Android, com.starbucks.at, v9.6.6204 (a German-language channel refers to the same app under the package label com.starbucks.mobile; both are reported here, unreconciled)
Disclosure reference	REF AT-STARBUCKS-2026-R1
R1 sent	2026-06-20/21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Network Security Config debug-overrides trusting user-installed certificates on a payment and loyalty app, CVSS v4.0 9.1, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20/21 June 2026, RFI-IRFOS performed static analysis of the production Starbucks Austria Android application and identified two CRITICAL and five HIGH findings: two Firebase production API keys hardcoded in the public APK, one of which is also present in the McDonald's Austria app, creating a shared attack surface between two separate restaurant chains' customer data, a Network Security Config debug-override that trusts user-installed certificates in production, enabling machine-in-the-middle interception on any developer-enabled or rooted device with no compensating certificate pinning on a payment and loyalty application, an Airship SDK (3,622 classes, a US vendor) receiving a combined loyalty, GPS, and purchase data stream, an ACCESS_FINE_LOCATION permission that timestamps every order into a movement profile capable of revealing home and work locations and commute routes, the same cross-brand Firebase credential raising an Art. 26/28 joint-controllership and vendor-management question, an undisclosed high-sampling-rate sensor permission with no apparent loyalty-app justification, and, via a separate German-language channel, pre-consent tracking together with an incomplete data-safety disclosure on the loyalty app.

Across six written notices over ninety-one days and two parallel disclosure channels, the only substantive-appearing reply this case produced, from privacy@starbucks.com on 29 June, redirected RFI-IRFOS to Starbucks' HackerOne bug-bounty programme rather than engaging with any of the three GDPR questions asked. RFI-IRFOS declined the redirect in writing the same day. The separate German-language channel to datenschutz@starbucks.at bounced immediately as a nonexistent address and never reached a human. No further human reply of any kind arrived afterward, only an automated multilingual customer-care auto-reply on 12 August. None of RFI-IRFOS's standing questions, on a joint-controller agreement with McDonald's Austria, credential rotation, an Art. 28 DPA with Airship Inc., or Art. 33 notification to the lead supervisory authority, ever received an answer.

Scope: Static analysis of the publicly downloaded production Starbucks Austria Android APK (v9.6.6204), on an authorized test device, only. No Starbucks account, backend, or infrastructure was accessed or tested. A related McDonald's Austria Firebase-credential overlap (C1/H3) is noted here as a cross-reference only and is not itself the subject of this report.

Disposition

R1 sent 20/21 June 2026 (the two parallel channels this case used, English and German, disagree by one day, no message from that date itself survives in this mailbox; only retrospective follow-up references to it do) to dpo@starbucks.com, privacy@starbucks.com, office@starbucks.at, contact@customerservice.starbucks.at, and datenschutz@starbucks.at (bounced, address does not exist), cc starbucks.at@grayling.com and ATstarbucks@starbucks.com, cc/bcc the Austrian Datenschutzbehoerde and CERT.at. Across six written notices over ninety-one days, the only substantive-appearing reply, from privacy@starbucks.com on 29 June, redirected RFI-IRFOS to Starbucks' HackerOne bug-bounty programme without answering any of the three GDPR questions asked; RFI-IRFOS declined the same day. No further human reply of any kind followed.

ID	Severity	Title
C1	CRITICAL	Two Firebase production API keys hardcoded in the public APK, one shared with the McDonald's Austria app
C2	CRITICAL	Network Security Config debug-overrides trust user-installed certificates on a payment and loyalty app
H1	HIGH	Airship SDK (3,622 classes) receiving a combined loyalty, GPS, and purchase data stream
H2	HIGH	ACCESS_FINE_LOCATION creates a timestamped movement profile
H3	HIGH	Cross-brand shared credential implies shared vendor/supply-chain credential management
H4	HIGH	Undisclosed high-sampling-rate sensor access
H5	HIGH	Pre-consent tracking and incomplete data-safety disclosure on the loyalty app

Subject & Operator Analysis

Starbucks Coffee Company is headquartered in Seattle, USA, and operates its Austrian market presence through the Starbucks Austria Android app. Correspondence in this case was addressed both to Starbucks' global Data Privacy team (privacy@starbucks.com) and to an Austria-specific address (datenschutz@starbucks.at) that does not exist.

Findings

C1: Two Firebase production API keys hardcoded in the public APK, one shared with the McDonald's Austria app

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

Two keys are hardcoded: AIzaSyApcIL19FelypljbNY_zZEDVJgkG4upQCM and AIzaSyDgmW4ZMvNblSXqMOgsbY8uRrTnfR3E7pY, the latter also present in the McDonald's Austria app, against a named production database at https://starbucks-austria.firebaseio.com.

A cross-brand, cross-company Firebase credential creates a shared attack surface between two separate restaurant chains' customer data: a compromise of the key by either party's incident affects the other's customers. No reply of any kind addressed this finding.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console, and here that surface extends to a second, unrelated company's app.

Fix: Rotate both exposed keys, issue each brand its own dedicated credential, and confirm deny-by-default security rules with App Check enforced.

C2: Network Security Config debug-overrides trust user-installed certificates on a payment and loyalty app

CRITICAL, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.1

The shipped Network Security Config trusts user-installed certificate authorities via a debug-override that remains active in the production build, with no compensating certificate pinning anywhere in the app.

On any developer-enabled or rooted device, this is machine-in-the-middle-ready in production for a payment and loyalty application. No reply of any kind addressed this finding.

Impact: Payment and loyalty traffic can be intercepted or altered on any device where the debug trust override is reachable.

Fix: Remove the debug-override network security configuration from production builds and implement certificate pinning.

H1: Airship SDK (3,622 classes) receiving a combined loyalty, GPS, and purchase data stream

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

The Airship SDK (Urban Airship, Portland OR, USA), 3,622 classes, receives a combined loyalty, GPS, and purchase data stream. Whether Starbucks EMEA holds a signed Art. 28 DPA with Airship Inc. covering this specific data combination is unresolved.

No reply of any kind addressed this finding.

Impact: A combined location, loyalty, and purchase data stream may be processed by a US vendor with no confirmed processing agreement covering that combination.

Fix: Confirm and publish an Art. 28 DPA with Airship Inc. covering the specific data categories transmitted, or narrow the data sent.

H2: ACCESS_FINE_LOCATION creates a timestamped movement profile

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

ACCESS_FINE_LOCATION is recorded with every order, producing a timestamped GPS record per purchase. Months of order history can reveal home location, work location, commute route, and holiday-absence patterns.

No reply of any kind addressed this finding.

Impact: Ordinary loyalty-app usage accumulates into a movement profile capable of revealing sensitive lifestyle patterns.

Fix: Decouple precise location capture from routine order placement, or disclose and time-limit retention of the resulting movement data explicitly.

H3: Cross-brand shared credential implies shared vendor/supply-chain credential management

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

The same Firebase credential identified in C1 spans two NASDAQ/NYSE-listed companies' consumer apps simultaneously, raising an Art. 26/28 joint-controllership and vendor-management question distinct from the technical exposure itself.

No reply of any kind addressed this finding.

Impact: Shared credential management between unrelated companies may leave governance and incident-response responsibility undefined for either party's customers.

Fix: Document a joint-controller agreement covering the shared credential, or eliminate the sharing arrangement entirely.

H4: Undisclosed high-sampling-rate sensor access

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

HIGH_SAMPLING_RATE_SENSORS (above 200Hz) is declared with no apparent loyalty-app justification and no disclosed purpose.

No reply of any kind addressed this finding.

Impact: A high-frequency sensor permission is held with no disclosed, verifiable purpose for a coffee-loyalty application.

Fix: Remove the permission unless tied to a disclosed, active feature.

H5: Pre-consent tracking and incomplete data-safety disclosure on the loyalty 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

A separate German-language channel of this same disclosure identified tracking activity occurring before consent is obtained, together with an incomplete Play Store data-safety disclosure, filed against a package label (com.starbucks.mobile) that may be the same app under a different or older label; this discrepancy is reported here unreconciled.

The German-language notice raising this finding, sent to datenschutz@starbucks.at, bounced immediately as a nonexistent address and never reached a human recipient.

Impact: Tracking activity occurring before a consent decision is made lacks a valid Art. 6/7 legal basis for that window.

Fix: Gate all tracking SDK initialization behind an affirmative consent decision, and complete the Play Store data-safety disclosure.

Two Channels, One Redirect, Zero Substantive Answers

This case ran across two parallel disclosure channels that disagree by one day on the R1 date and by package label on the app itself, a discrepancy this report flags rather than silently resolves. The English-language channel produced the case's only substantive-appearing reply: on 29 June, privacy@starbucks.com redirected RFI-IRFOS to Starbucks' HackerOne bug-bounty programme, answering none of the three GDPR questions posed. RFI-IRFOS declined the redirect in writing the same day, restating all findings and requesting a joint DPO and security-leadership review. The German-language channel, addressed to daten schutz@starbucks.at, bounced immediately as a nonexistent address and never reached a human recipient. Across both channels and six notices over ninety-one days, no further human reply of any kind arrived, only an automated multilingual customer-care auto-reply on 12 August.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 26, Art. 32	Cross-brand Firebase credential shared with an unrelated company's app
C2	GDPR Art. 32(1)(a)	Debug certificate-trust override active in production on a payment/loyalty app
H1	GDPR Art. 28, Art. 44	Undocumented processing agreement for a combined location/loyalty/purchase data stream
H2	GDPR Art. 5(1)(b)(c), Art. 13(2)(f)	Movement profile inferable from timestamped order-location data
H3	GDPR Art. 26, Art. 28	Undefined joint-controllership over a shared credential
H4	GDPR Art. 13	Undisclosed high-frequency sensor permission
H5	GDPR Art. 6, Art. 7	Tracking activity occurring before consent

Disclosure Timeline & Outcome

Date	Event
2026-06-20/21	R1 sent via two parallel channels (English and German); no surviving message from this date, only retrospective references
2026-06-28	Follow-up (8 days, no reply) restates C1/C2/H3 and three questions
2026-06-29	privacy@starbucks.com replies, redirecting to HackerOne; RFI-IRFOS declines the same day, restates all findings
2026-07-28	Separate German-language follow-up to datenschutz@starbucks.at bounces (address not found)
2026-08-18	Follow-up formalizes REF AT-STARBUCKS-2026-R1, sets a three-questions deadline of 25 August
2026-08-24	Follow-up invokes the Art. 33(4) 72-hour notification clock, restates the unchanged 19 September embargo
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Remove the production debug certificate-trust override and implement certificate pinning.
- Rotate both exposed Firebase keys and issue each brand its own dedicated credential.
- Document an Art. 28 DPA with Airship Inc. covering the combined GPS, loyalty, and purchase data stream.
- Gate all tracking SDK initialization behind an affirmative consent decision.
- Reconcile the two disclosure channels' package-label discrepancy and establish a functioning Austria-specific privacy contact.

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, 7, 13, 26, 28, 32, 44. REF AT-STARBUCKS-2026-R1.