Coordinated Security & Privacy Disclosure, Final Report

Glovo for Android (com.glovo)

Facebook registered as the buyer in an on-device ad auction built from food-order behavior, three dead intake addresses, one engaged reply, then silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ONE ENGAGED REPLY, THEN FORTY DAYS OF SILENCE

Target	Delivery Hero SE, Berlin, Germany (Glovo)
Product audited	Glovo for Android, com.glovo, v7.209.0 / build 2026.24.0
Disclosure reference	REF GLOVO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (hardcoded credentials / no certificate pinning, 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

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Glovo Android application and identified six findings, one CRITICAL, two HIGH, two MEDIUM, one LOW. The most significant: Glovo implements the Android Privacy Sandbox Protected Audience API and registers facebook.com as the declared buyer in an on-device ad auction built from food-ordering behavior, restaurants visited, order frequency, price range, and time patterns, with no disclosed Art. 26 joint-controller arrangement between Glovo and Meta Platforms Ireland Ltd.

Separately, three hardcoded credentials, a Firebase key, a Braze API key, and a Facebook client token, remain extractable from the production binary, and the network security configuration contains no domain-specific entries or certificate pins for the app's payment or API endpoints. Instabug's screen-recording service also ships with no confirmed exclusion of payment screens from its capture scope, and the app accesses the address book of non-consenting third parties with no lawful basis identified.

Ten written notices were sent over 90 days, three of Glovo's own published intake addresses, privacy@glovoapp.com, security@glovoapp.com, and press@glovoapp.com, were confirmed dead as Google Groups during the correspondence. One month after R1, Mark Cunningham of Glovo's product security team engaged genuinely, asking for evidence of prior contact given those dead addresses. RFI-IRFOS answered in full. No further reply of any kind, from him or anyone else at Glovo or Delivery Hero, followed across five further written notices and over 40 days through the close of the embargo.

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

Disposition

R1 sent 20 June 2026 to security@glovoapp.com and legal@deliveryhero.com, bcc the Austrian DSB, CERT.at, Berlin's BlnBDI, and Spain's AEPD (the AEPD address bounced immediately). One month later, Mark Cunningham of Glovo's product security team engaged genuinely, asking for proof of prior contact given the addresses on record. RFI-IRFOS answered in full. No further reply of any kind followed across five subsequent written notices and over 40 days.

ID	Severity	Title
C1	CRITICAL	Facebook registered as the buyer in an on-device ad auction built from food-order behavior
H1	HIGH	Instabug screen recording active, payment screens not excluded from capture scope
H2	HIGH	Three hardcoded credentials in the production APK
M1	MEDIUM	No certificate pinning on payment or API endpoints

ID	Severity	Title
M2	MEDIUM	Contact book access: phone numbers of non-consenting third parties
L1	LOW	Ravelin DeviceIdService exported without permission restriction

Subject & Operator Analysis

Glovo is operated under the Delivery Hero group, headquartered in Berlin, Germany, with Berlin's BlnBDI as lead supervisory authority and Spain's AEPD separately relevant as the app's primary Spanish market authority.

Positive Observations

- Braze correctly uses the EU endpoint sdk.fra-01.braze.eu, so this particular engagement pipeline does not route data to US servers.

Findings

C1: Facebook registered as the buyer in an on-device ad auction built from food-order behavior

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

Glovo implements the Android Privacy Sandbox Protected Audience API (FLEDGE). CustomAudience$Builder.setBuyer("facebook.com") declares Facebook as the buyer for on-device ad auctions built from order-behavior segments.

```
CustomAudienceManager.get(context)              <- initializes on-device auction
CustomAudience$Builder.setName(...)              <- audience segment name
CustomAudience$Builder.setBuyer("facebook.com")   <- Facebook registered as buyer
CustomAudience$Builder.setDailyUpdateUri("?daily&app_id=...")

Permission: android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

No response was received naming this finding. Custom Audience segments are built from restaurants visited, order frequency, price range, and time patterns. No Art. 26 joint-controller arrangement between Glovo and Meta Platforms Ireland Ltd. is disclosed in Glovo's privacy policy. Delivery Hero reported 68 million monthly EU orders in 2025; if Glovo alone exceeds 45 million EU monthly active users it would meet the DSA's VLOP threshold, triggering Art. 26 ad-transparency obligations not currently met.

Impact: Food-ordering behavioral segments are shared into an on-device advertising auction with a named third-party buyer, with no disclosed joint-controller basis under Art. 26.

Fix: Disclose the Art. 26 joint-controller arrangement with Meta Platforms Ireland Ltd., or remove Facebook as a registered FLEDGE buyer.

H1: Instabug screen recording active, payment screens not excluded from capture scope

---

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 Instabug SDK, repackaged under ai.luciq.*, starts ScreenRecordingService via MediaProjectionManager. No conditional exclusion of ProcessOut payment checkout or card-entry screens from the recording scope is visible in static analysis.

No response was received naming this finding. Recordings route through Instabug Inc. servers in the US, a third party not named in Glovo's data-processing disclosures.

Impact: Screen recordings, potentially including payment card entry, are captured and transmitted to an undisclosed US third party.

Fix: Exclude payment and card-entry screens from the Instabug recording scope explicitly, and name Instabug as a data processor with its Art. 46 transfer mechanism.

H2: Three hardcoded credentials 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 Firebase API key, a Braze API key, and a Facebook client token are all statically embedded and extractable from the production binary.

```
google_api_key:       AIzaSyDl7mQ58JFvv7nP-ZaYXzOFrJRRJYi7J9A
Firebase project:     eloquent-clover-721
com_braze_api_key:    61d24282-98d2-4ca1-b2e7-f8703fc2b83b
facebook_client_token: 5002ad6dcd746f745c48bb45418fd207
```

No response was received naming this finding, including the direct question of whether the Firebase key has been rotated. Positive note: Braze correctly uses the EU endpoint sdk.fra-01.braze.eu, so engagement data does not route to US servers, a mitigating detail RFI-IRFOS credits explicitly.

Impact: Three publicly extractable credentials enable probing of the associated projects and potential further backend access.

Fix: Rotate all three credentials and restrict them to the production certificate fingerprint.

M1: No certificate pinning on payment or API endpoints

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

The network security configuration contains only a base config trusting system CAs, with no domain-specific entries or pin-sets for api.glovoapp.com, checkout.glovoapp.com, or the ProcessOut payment gateway.

No response was received naming this finding. A compromised CA or MDM proxy can silently intercept TLS traffic including payment sessions.

Impact: Payment and API traffic has no application-level protection against a compromised or hostile certificate authority.

Fix: Add certificate pinning for api.glovoapp.com, checkout.glovoapp.com, and the payment gateway domain.

M2: Contact book access: phone numbers of non-consenting third parties

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

The app accesses ContactsContract.CommonDataKinds.Phone.CONTENT_URI and ContactsContract.Contacts.CONTENT_URI.

No response was received naming this finding. Uploaded contacts include people who have never used Glovo, gave no consent, and have no GDPR rights pathway available to them.

Impact: Contact data belonging to non-users with no relationship to Glovo is processed with no lawful basis identified.

Fix: Restrict contact access to the minimum needed for an explicit, opt-in referral feature, and publish the lawful basis for processing non-user contact data.

L1: Ravelin DeviceIdService exported without permission restriction

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

com.ravelin.core.repository.services.DeviceIdService is declared android:exported="true" with no android:permission attribute.

No response was received naming this finding. Any installed app can bind to the service and retrieve the Ravelin persistent device identifier, undermining its fraud-detection value.

Impact: The fraud-detection device identifier can be retrieved by any other installed app, weakening its intended anti-fraud purpose.

Fix: Set android:exported="false" on the DeviceIdService component.

Glovo's Response, Recorded in Full

One month after R1, on 20 July 2026, Mark Cunningham of Glovo's product security team replied, in full: "I'm from the product security team in Glovo. This is a message to say I've received your email and will be looking into your security reports and evaluate what you have sent us for triage/validation. From checking with the security team here behind security@glovoapp.com, this message appears to be the first that we've been informed of these issues. In your email you referenced 'To the Glovo Security Team and Delivery Hero Legal', can you please forward EML copies of those emails to verify who you used as a point of contact along with the headers/dates to try understand why we haven't recieved those before. However, I understand you have already engaged with Glovo's legal department. The Glovo security team will sync with legal internally after a review and follow up with you."

This is a legitimate question: three of Glovo's own published intake addresses, privacy@glovoapp.com, security@glovoapp.com, and press@glovoapp.com, were separately confirmed as dead, non-existent Google Groups at different points in this correspondence. RFI-IRFOS answered with the full inline thread history on 27 July and again on 9 August. No further reply from Mark Cunningham, or from anyone else at Glovo or Delivery Hero, arrived after that point, across five further written notices and more than 40 days through the close of the embargo.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 26, Art. 13; DSA Art. 26	Undisclosed joint-controller ad auction with Meta
H1	GDPR Art. 5(1)(f), Art. 32(1)(a)	Screen recording, payment screens not excluded
H2	GDPR Art. 32(1)(b)	Hardcoded, publicly extractable credentials
M1	GDPR Art. 32(1)(a)	No certificate pinning on payment/API traffic
M2	GDPR Art. 6	Non-consenting third-party contact data
L1	Component export hygiene	Exported fraud-detection identifier service

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@glovoapp.com and legal@deliveryhero.com, bcc Austrian DSB/CERT.at/BInBDI/AEPD (AEPD bounced), 6 findings
2026-06-27 / 06-28	Follow-ups; privacy@glovoapp.com confirmed dead as a Google Group
2026-07-17	Follow-up restating findings, no reply
2026-07-20	Mark Cunningham (Glovo product security) replies, asks for proof of prior contact given dead addresses
2026-07-27 / 08-09	RFI-IRFOS answers in full; security@glovoapp.com and press@glovoapp.com also confirmed dead as Google Groups
2026-08-18 / 09-03 / 09-12	Further follow-ups restating the three standing questions; legal@deliveryhero.com auto-acknowledges each, no substantive reply
2026-09-19	Embargo, as stated consistently since the first follow-up, closes and this report publishes

Glovo’s product security team engaged once, genuinely, questioning delivery given multiple dead intake addresses. RFI-IRFOS answered fully. No further reply of any kind followed across five subsequent written notices and more than 40 days. All six findings stand exactly as originally reported.

Residual Risk & Recommendations

- Disclose the Art. 26 joint-controller arrangement with Meta Platforms Ireland Ltd. or remove Facebook as a registered FLEDGE buyer; this is the single highest-priority item given the undisclosed cross-controller data flow.
- Rotate all three hardcoded credentials and restrict them to the production certificate fingerprint.
- Add certificate pinning for payment and API endpoints.
- Exclude payment screens from Instabug's screen-recording scope and name Instabug as a processor.
- Repair or retire the three confirmed-dead published intake addresses, privacy@glovoapp.com, security@glovoapp.com, and press@glovoapp.com, so future disclosures actually reach a live inbox.

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, 13, 26, 32, 46; Digital Services Act Art. 26. REF GLOVO-2026-R1.