Coordinated Security & Privacy Disclosure, Final Report

Lieferando for Android (at.lieferservice.android)

A home-address location profile sent to a US fraud-intelligence vendor, one reply, and its own hidden metadata proving it was filed as ”order not found”

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE REPLY, FILED AS A LOST-ORDER TICKET

Target	Takeaway.com Group B.V., Amsterdam, Netherlands (Lieferando)
Product audited	Lieferando for Android, at.lieferservice.android, v11.29.0
Disclosure reference	REF LIEFERANDO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase keys / C2 zero 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 Lieferando Android application and identified six findings, two CRITICAL, four HIGH. The most significant: Incognia, a US location-intelligence vendor, is embedded with 2,171 classes, the largest third-party SDK in the app, and receives the full street address and GPS coordinates of every delivery, explicitly labeled 'home' in the transmitted data, building a persistent home-location fingerprint with no EU adequacy decision covering the transfer.

Three hardcoded Firebase production API keys were also extracted, with the database URL itself containing the word 'prod', and the network security configuration contains no certificate pinning at all, exposing payment traffic and location transmission alike to interception. Three further findings raise undisclosed third-party data flows: Rokt injecting targeted advertising immediately after completed food orders using restaurant and order-value data; mParticle distributing behavioral data to undisclosed downstream vendors including Braze; and Huawei HMS, subject to China's National Security Law, embedded in a payment-enabled food-delivery app.

Nine written notices were sent over 91 days. privacy@justeattakeaway.com bounced five separate times and was dropped from distribution. The only non-automated reply received, from a named customer-service agent, carried hidden HTML routing metadata classifying the disclosure as an ordinary lost-order support ticket, not a privacy or security matter. All six findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026, first attempt to privacy@justeattakeaway.com bounced within seconds, redelivered the same day to info@lieferando.at, the only address that has ever functioned across the entire case. Eight further written notices followed. privacy@justeattakeaway.com bounced five separate times before being dropped from distribution. The only non-automated reply received, from a named Lieferando customer-service agent, carried hidden HTML routing metadata classifying the GDPR disclosure as an ordinary lost-order support ticket.

ID	Severity	Title
C1	CRITICAL	Three hardcoded Firebase production API keys
C2	CRITICAL	Zero certificate pinning on a payment-processing food-delivery app
H1	HIGH	Incognia: full home address and GPS coordinates, explicitly labeled "home", to a US fraud-intelligence vendor
H2	HIGH	Rokt: post-order targeted advertising using meal-order context

ID	Severity	Title
H3	HIGH	mParticle and Braze: behavioral data distributed to undisclosed downstream vendors
H4	HIGH	Huawei HMS: Chinese platform infrastructure in a payment-enabled food-delivery app

Subject & Operator Analysis

Takeaway.com Group B.V. (Amsterdam, Netherlands), part of Just Eat Takeaway.com, operates Lieferando as its Austrian and German consumer-facing food-delivery brand.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Three hardcoded Firebase production API keys

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

Three Firebase API keys are hardcoded in the public APK. The database URL, just-eat-consumer-android-prod.firebaseio.com, contains the word "prod", explicitly confirming production status.

```
AIzaSyCRONyNHWoy30PI-YUCZYaqnG_6TsRndeo
AIzaSyD1nhgVVpGtrUDnU0sjdlFusCOyY7uVV6Q
AIzaSyDYC2ElaSgU1kmb9p_7U61IIBswPbiwox8
Database: https://just-eat-consumer-android-prod.firebaseio.com
```

No response was received naming this finding, including the direct question of whether the keys have been rotated. The linked database is stated as deactivated, but all three keys remain permanently embedded in every installed version of the app regardless.

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

Fix: Rotate all three credentials and restrict them to the production certificate fingerprint, independent of the linked database's current status.

C2: Zero certificate pinning on a payment-processing food-delivery app

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 no domain entries and no pin sets at all.

No response was received naming this finding. All connections, including Braintree/PayPal payment processing and Incognia location transmission, are susceptible to interception, with no server certificate verification enforced beyond the Android system default.

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

Fix: Implement certificate pinning for all production API and payment endpoints.

H1: Incognia: full home address and GPS coordinates, explicitly labeled "home", to a US fraud-intelligence vendor

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

Incognia Inc. (Palo Alto, US), 2,171 classes, the largest third-party SDK in the app. EventAddress and EventLocation objects carry the full delivery street address and GPS coordinates, with a literal "home" label applied.

No response was received naming this finding, including the repeated question of where Incognia is disclosed as a data processor and its Art. 44 transfer mechanism. Every time a user enters a delivery address, Incognia receives the full address and coordinates, building a persistent home-location behavioral fingerprint tied to the device identifier for its fraud-detection product. No EU adequacy decision covers the US transfer.

Impact: A persistent, explicitly-labeled home-location profile is built and transmitted to a US fraud-intelligence vendor with no disclosed processor relationship or transfer safeguard.

Fix: Name Incognia as a data processor under Art. 13(1)(e), publish its Art. 44-49 transfer mechanism, and confirm whether the address/location data is retained beyond the fraud-check window.

H2: Rokt: post-order targeted advertising using meal-order context

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

3,452 Rokt (New York, US) classes inject a targeted-advertising overlay immediately after completed food orders, using restaurant, cuisine category, and order value as targeting signals.

No response was received naming this finding. Using meal-order data for third-party ad targeting immediately post-purchase is a purpose distinct from delivering the food-delivery service itself.

Impact: Order context is repurposed for third-party advertising with no disclosed separate consent basis for this specific use.

Fix: Disclose Rokt as a named advertising recipient under Art. 13(1)(e) and obtain distinct consent for post-order ad targeting.

H3: mParticle and Braze: behavioral data distributed to undisclosed downstream vendors

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

mParticle (New York, US), 387 classes, aggregates behavioral events and distributes them to downstream vendors; Braze (New York, US), 867 classes, is confirmed as one recipient via custom serialization classes.

No response was received naming this finding. Individual downstream recipients reached through mParticle are not disclosed to users.

Impact: Behavioral data is distributed to an undisclosed set of downstream vendors through a US customer-data platform.

Fix: Publish the full list of downstream vendors receiving data via mParticle, and name Braze specifically as a confirmed recipient under Art. 13(1)(e).

H4: Huawei HMS: Chinese platform infrastructure in a payment-enabled food-delivery app

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

Huawei Mobile Services is integrated with 861 classes.

No response was received naming this finding. Huawei Technologies Co., Ltd. is subject to China's National Security Law, under which Chinese authorities can compel data disclosure, a supply-chain governance question given the app processes home addresses and purchase history.

Impact: A supply-chain component subject to compelled state disclosure obligations processes infrastructure adjacent to home-address and purchase data.

Fix: Confirm what data, if any, transits through Huawei HMS components and document the applicable Art. 44 safeguard.

Lieferando's Response, Recorded in Full: Filed as a Lost Order

The only non-automated reply in 91 days arrived on 14 July 2026, from a named customer-service agent, Kirankumar C, in full: "vielen Dank für Ihre Nachricht an uns. Wir haben Ihr Anliegen an die zuständige Abteilung weitergeleitet. Diese wird schnellstmöglich die gewünschte Bearbeitung vornehmen."

RFI-IRFOS subsequently inspected the reply's own hidden HTML routing metadata and found the classification tags requestType:customer, alongside routing tokens including site_hyderabad, site_istanbul, order::not_found, order::reference_email, order::requester_mismatch, and no_csat. This is documentary evidence, from the reply's own source, that a formal GDPR security and privacy disclosure was processed internally as an ordinary lost-order customer-support ticket, not a privacy or security matter. RFI-IRFOS's follow-ups of 18 August and 4 September state explicitly that this misclassification does not relieve Takeaway.com Group B.V. of its Art. 33 obligations, and no further reply, from this agent or anyone else, was ever received.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Hardcoded, publicly extractable production credentials
C2	GDPR Art. 32(1)(a), Art. 5(1)(f)	Zero certificate pinning on payment traffic
H1	GDPR Art. 44, Art. 13(1)(e), Art. 5(1)(b)	Home-location profile to an undisclosed US processor
H2	GDPR Art. 5(1)(b), Art. 13	Undisclosed post-order advertising using order context
H3	GDPR Art. 13(1)(e), Art. 44	Undisclosed downstream vendor distribution
H4	GDPR Art. 25, Art. 44	Chinese platform infrastructure, compelled-disclosure exposure

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 to privacy@justeattakeaway.com bounces immediately; redelivered same day to info@lieferando.at, 6 findings
2026-06-28 / 07-04 / 07-07	Follow-ups; three standing questions posed and repeated, 48h deadline set and missed
2026-07-14	Only non-automated reply received, from Kirankumar C, later shown by its own hidden metadata to be a lost-order support ticket classification
2026-07-27 / 08-09	Follow-ups; privacy@justeattakeaway.com confirmed bounced repeatedly and eventually dropped from distribution
2026-08-18	Follow-up explicitly documents the hidden-metadata misclassification finding
2026-09-04 / 09-12	Final follow-ups restate all findings, three new questions posed, weekly SHA-256 re-diffing instituted
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Nine written notices across 91 days produced one non-automated reply, which the reply's own hidden routing metadata proves was processed as an unrelated customer-service ticket. privacy@justeattakeaway.com bounced five separate times before being dropped from distribution. All six findings stand exactly as originally reported.

Residual Risk & Recommendations

- Name Incognia as a data processor and publish its Art. 44 transfer mechanism; this is the single highest-priority item given the explicitly home-labeled location profile it receives.
- Rotate all three Firebase credentials and implement certificate pinning across production and payment endpoints.
- Publish the full downstream vendor list reached via mParticle and disclose Rokt's post-order advertising use.
- Repair the privacy@justeattakeaway.com intake channel, confirmed dead across five separate delivery attempts.
- Route GDPR and security disclosures to a function equipped to recognize and handle them, rather than the customer-support ticketing queue this case was processed through.

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, 13, 25, 32, 33, 44. REF LIEFERANDO-2026-R1.