



Security & Privacy Disclosure, Final Report

DoorDash for Android (com.dd.doordash)

Biometric KYC, hardcoded Firebase credentials, and session-replay capture of dietary data ship in a food-delivery app that answered ten weeks of GDPR disclosure with seven identical automated bot replies and zero human response

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26
SEPTEMBER 2026, EIGHT FINDINGS REMAIN UNADDRESSED**

Target	DoorDash, Inc.
Package	com.dd.doordash
Platform Audited	Android · 164,643 smali classes across 15 DEX files, 197MB base APK
Initial Disclosure (R1)	2026-06-21 (REF DOORDASH-2026-R1)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	8 (3 Critical, 5 High)
Correspondence	7 messages sent by RFI-IRFOS, 7 identical automated HackerOne-redirect replies, 0 human reply at any point
Authorities BCC'd	Austrian Datenschutzbehoerde (DSB) - CERT.at - Irish Data Protection Commission

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	6
4.1	C1: withPersona biometric KYC SDK (com.withpersona.sdk, com.withpersona.sdk2) — 4,806 smali classes — biometric identity verification disproportionate to a food-delivery purpose	6
4.2	C2: Three Firebase credentials hardcoded in the production binary	7
4.3	C3: Sentry Session Replay (RRweb) records full visual interaction on order screens showing dietary filters and payment method	7
4.4	H1: Facebook SDK (967 smali) transmits dietary preference and precise delivery-address data to Meta	8
4.5	H2: Deliveroo codebase embedded undisclosed — 799 smali classes	8
4.6	H3: READ_CONTACTS and WRITE_CONTACTS permissions exceed disclosed feature scope	9
4.7	H4: Four independent behavioural fraud-profiling SDKs operate without Art. 13 disclosure	9
4.8	H5: Singular preinstall attribution tracking begins before any consent screen	10
5	Impact Analysis	10
6	The Complete Chain: From Download to Undisclosed Cross-Border Profiling	11
7	Data Protection — Article by Article	12
8	Regulatory & Legal Landscape	13
9	Indicators of Compromise	14
10	Disclosure Timeline & Outcome	15
11	What DoorDash Got Right	16
12	Residual Risk & Recommendations	16

Executive Summary

DoorDash, Inc. operates one of the largest food-delivery platforms in North America. The DoorDash Android application manages account identity, payment methods, delivery addresses, order history, and dietary preferences for a large consumer user base, and is freely downloadable from the Google Play Store.

Static analysis of the production application identified eight findings. A 4,806-class with-Persona biometric identity-verification SDK is bundled into an ordinary food-delivery app, performing government-ID scanning, facial liveness matching, and NFC passport reading without a demonstrable proportionate basis under Art. 9 GDPR. Three Firebase credentials — a database URL, a Google App ID, and two additional API keys — are hardcoded in the binary. Sentry Session Replay (RRweb) records full visual interactions on order screens that display dietary filters, restaurant choices, delivery address, and payment method, data that qualifies as health-adjacent under GDPR Art. 9 when systematically collected. A competing platform's codebase, Deliveroo, is embedded in the binary without disclosure. Four independent, undisclosed behavioural fraud-profiling engines run in parallel (Sift Science, Riskified, Signifyd, Forter), the Facebook SDK transmits dietary and precise location data to Meta's advertising infrastructure, READ_CONTACTS/WRITE_CONTACTS access exceeds what any disclosed feature requires, and Singular attribution tracking begins at install, before any consent screen is shown.

RFI-IRFOS disclosed these findings to security@doordash.com and privacy@doordash.com on 21 June 2026 under REF DOORDASH-2026-R1, with the Austrian Datenschutzbehoerde, CERT.at, and the Irish Data Protection Commission BCC'd. Over the following ten weeks, RFI-IRFOS sent seven messages in total, each escalating in urgency and each restating the same findings and the same 26 September 2026 embargo date. Every single one of the seven replies received was the identical automated "Global Threat Defense Team" HackerOne-redirect message from security+noreply@doordash.com. At no point — including after an explicit Art. 33(4) GDPR 72-hour notification warning issued on 24 August 2026 — did a human being from DoorDash ever reply. The 90-day coordinated-disclosure embargo elapsed on 26 September 2026. This report, published 21 days after that date, confirms all eight findings remain unaddressed and unacknowledged by any human contact.

ID	Severity	Title
C1	CRITICAL	withPersona biometric KYC SDK (com.withpersona.sdk, com.withpersona.sdk2) — 4,806 smali classes — biometric identity verification disproportionate to a food-delivery purpose
C2	CRITICAL	Three Firebase credentials hardcoded in the production binary
C3	CRITICAL	Sentry Session Replay (RRweb) records full visual interaction on order screens showing dietary filters and payment method
H1	HIGH	Facebook SDK (967 smali) transmits dietary preference and precise delivery-address data to Meta
H2	HIGH	Deliveroo codebase embedded undisclosed — 799 smali classes

ID	Severity	Title
H3	HIGH	READ_CONTACTS and WRITE_CONTACTS permissions exceed disclosed feature scope
H4	HIGH	Four independent behavioural fraud-profiling SDKs operate without Art. 13 disclosure
H5	HIGH	Singular preinstall attribution tracking begins before any consent screen

Subject & Operator Context

DoorDash, Inc. (San Francisco, California, USA) operates a food, grocery, and retail delivery platform across the United States, Canada, Australia, New Zealand, and Japan. The company is publicly traded (NYSE: DASH) and reports tens of millions of monthly active consumers.

The audited application, com.dd.doordash, handles account identity and verification, stored payment methods, delivery addresses, order history, dietary filter preferences, and in-app customer support chat. Users complete identity verification flows, link payment instruments, and place orders that are routed to restaurant and retail partners and fulfilled by independent delivery contractors (Dashers).

The presence of a full-stack biometric identity-verification SDK, four independent undisclosed fraud-profiling engines, and an embedded competitor codebase in a consumer food-ordering application places the data model of this app well beyond what a food-delivery service requires to function, and raises an immediate proportionality question under GDPR purpose limitation and data minimisation principles for any EU-resident user of the globally distributed Play Store build.

Engagement Summary

RFI-IRFOS sent the initial disclosure (REF DOORDASH-2026-R1) to security@doordash.com and privacy@doordash.com on 21 June 2026, BCC to the Austrian Datenschutzbehörde, CERT.at, and the Irish Data Protection Commission. The automated reply received eleven seconds later, from security+noreply@doordash.com, was a standard "Global Threat Defense Team" message redirecting security researchers to DoorDash's HackerOne bug-bounty programme.

RFI-IRFOS sent six further follow-ups over the following ten weeks — 27 June, 23 July, 5 August, 15 August, 24 August, and 31 August 2026 — each restating the findings, each noting the escalating day-count since the original disclosure, and each adding regulators to open CC as the silence continued. press@doordash.com was added to CC on 27 June and again on 31 August; a subsequent notice indicated that address was itself no longer monitored. Every one of these seven messages, without exception, received only the identical automated HackerOne-redirect reply — the same text, from the same sender, regardless of content or urgency.

On 24 August 2026, RFI-IRFOS noted explicitly that the first reply, while automated, had at least been a contextually appropriate acknowledgment of a formal disclosure rather than a complete non-response — and that every reply since had been the same bot text with no human engagement at any point. That message also invoked Art. 33(4) GDPR: if DoorDash considers the underlying issues a personal data breach, the 72-hour notification clock to the

competent supervisory authority was already running, and an internal review in progress is not grounds to delay that initial notification. The final message in the correspondence, sent 31 August 2026, again drew only the automated reply. No human reply was received at any point before, during, or after the 90-day embargo, which elapsed on 26 September 2026.

Findings

C1: withPersona biometric KYC SDK (com.withpersona.sdk, com.withpersona.sdk2) — 4,806 smali classes — biometric identity verification disproportionate to a food-delivery purpose

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — Persona biometric KYC bundled into a food-delivery app

```
com.withpersona.sdk    -- identity verification core
com.withpersona.sdk2   -- identity verification, v2 API
Combined: 4,806 smali classes
```

Capabilities present in bundled SDK: government ID document scan, facial liveness match, NFC passport chip reading

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL. Persona is a full-stack identity-verification platform performing government-ID document scanning, facial liveness matching, and NFC passport-chip reading — special-category biometric data under Art. 9(1) GDPR, for which processing is prohibited absent an explicit Art. 9(2) basis. Ordering food does not establish a basis proportionate to collecting and verifying a user's biometric identity against a government-issued document. Persona processes this data in the United States with no EU adequacy decision in place, engaging Art. 44 (Chapter V) transfer restrictions, and Persona was not identified as an Art. 28 data processor in the DoorDash privacy documentation reviewed for this audit. The population affected is not a narrow subset flagged for fraud review — the SDK is bundled into every installation of the general consumer application.

C2: Three Firebase credentials hardcoded in the production binary

CRITICAL (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) — Firebase database URL, App ID, and two API keys hardcoded

```
firebase_database_url: https://doordash-consumer-android.firebaseio.com
google_app_id:        1:302242645714:android:6d1d682471fc54fd
Additional API key 1:  AIzaSyBqiyThWC0b7pvmAsrNSwHyA-yYsZ-lmyg
Additional API key 2:  AIzaSyChoIqwjT1n60tEJY4cPGQMnpWafmwidjE
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL. The Firebase Realtime Database URL, Google App ID, and two independent Firebase API keys are present in plaintext in the production binary, extractable from any Play Store download in under a minute with standard reverse-engineering tooling. Depending on Firebase security-rule configuration, these credentials can enable unauthenticated probing of the Realtime Database, Remote Config manipulation, or Cloud Messaging quota-exhaustion attacks. This is a production credential set shipped to every consumer installing the application, not a development or staging artifact.

C3: Sentry Session Replay (RRweb) records full visual interaction on order screens showing dietary filters and payment method

CRITICAL (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) — undisclosed session-replay capture of dietary and order data

```
io.sentry      -- 1,619 smali classes total (error tracking)
io.sentry.rrweb --   23 smali classes (session replay module)

Screens in scope: order/cart, dietary filter selection, delivery
address, payment method selection
Data destination: Sentry, Inc. (United States)
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL. io.sentry.rrweb (23 smali classes within a 1,619-class Sentry integration) implements pixel-level session replay, reconstructing exactly what a user taps, scrolls, and views. Order screens display restaurant choices, dietary filters, delivery address, and payment method selection in combination. Dietary preferences tied to a medical condition (allergy, diabetic, or other medically directed restriction) constitute Art. 9 health data when systematically and visually captured in this way, and the data destination is Sentry's US infrastructure. Art. 5(1)(b) purpose limitation and Art. 5(1)(c) data minimisation both apply to transmitting a full visual record of order and payment interactions to an error-tracking vendor whose stated purpose is technical diagnostics, not behavioural capture.

H1: Facebook SDK (967 smali) transmits dietary preference and precise delivery-address data to Meta

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, 6.9) — dietary and location data to Meta advertising infrastructure

```
com.facebook.appevents, com.facebook.applinks, com.facebook.core
Combined: 967 smali classes
Data observed in scope: cuisine/dietary filters, order frequency,
precise GPS delivery coordinates
```

Impact: com.facebook.appevents, com.facebook.applinks, and com.facebook.core together total 967 smali classes. Cuisine type, dietary filter selections, order frequency, and precise GPS delivery-address data flow to Meta's advertising infrastructure through this SDK. Dietary preference and home-delivery address are not data categories compatible with advertising-profiling purposes under Art. 5(1)(b). Meta operates as a joint controller for data collected through its SDKs (CJEU C-40/17, Fashion ID), engaging the Art. 26 joint-controller arrangement requirement and an Art. 6(1)(a) consent basis that was not confirmed as present for this specific data flow during this audit.

H2: Deliveroo codebase embedded undisclosed — 799 smali classes

HIGH (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, 7.1) — competing platform's codebase embedded without disclosure

```
com.deliveroo.common
com.deliveroo.logging
com.deliveroo.rooblocks
Combined: 799 smali classes
```

Impact: com.deliveroo.common, com.deliveroo.logging, and com.deliveroo.rooblocks together total 799 smali classes embedded in the DoorDash production binary. Deliveroo is a competing food-delivery platform operating in UK and EU markets. The presence of this codebase suggests either a white-label arrangement or an acquisition-integration artifact that is not disclosed anywhere in DoorDash's user-facing documentation reviewed for this audit. This raises an unresolved data-routing question: whether any user data is processed through, or shared with, Deliveroo infrastructure as a consequence of this shared codebase, a disclosure users are not in a position to evaluate or consent to without knowing the integration exists.

H3: READ_CONTACTS and WRITE_CONTACTS permissions exceed disclosed feature scope

HIGH (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, 7.1) — full read/write contact-database access on a food-delivery app

```
android.permission.READ_CONTACTS
android.permission.WRITE_CONTACTS
```

Impact: The application declares both `android.permission.READ_CONTACTS` and `android.permission.WRITE_CONTACTS`. A "send food to a friend" style feature justifies, at most, read access to a user-selected subset of contacts via the Android system contact picker, which requires no special permission at all. It does not justify standing read access to the entire contact database, and it does not justify write access, which allows the application to create or modify contact-database entries. This is a data-minimisation failure under Art. 5(1)(c) independent of whether the broader access has been exploited.

H4: Four independent behavioural fraud-profiling SDKs operate without Art. 13 disclosure

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, 7.3) — four undisclosed parallel fraud-profiling engines

```
siftscience/android      -- 56 smali classes (behavioural fraud scoring)
com.riskified.android_sdk -- order fraud profiling
com.signifyd.profiling    -- transaction risk profiling
com.forter.mobile         -- real-time behavioural biometrics (typing
                           rhythm, scroll velocity) for fraud scoring
```

Impact: Sift Science (`siftscience/android`, 56 smali classes), Riskified (`com.riskified.android_sdk`), Signifyd (`com.signifyd.profiling`), and Forter (`com.forter.mobile`) run in parallel, each independently scoring the user for fraud risk. None of the four appear in the EU Art. 13 transparency documentation reviewed for this audit. Forter's mobile SDK specifically performs behavioural-biometric profiling — typing rhythm and scroll velocity — a category of data that sits adjacent to Art. 9 biometric data and that a typical user has no visibility into at all. Running four independent, overlapping risk engines against the same transaction without disclosure raises both a transparency question under Art. 13(1)(e) and, to the extent any of these feeds automated account or order decisions, an Art. 22 automated-decision-making question.

H5: Singular preinstall attribution tracking begins before any consent screen

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 7.0)
— attribution tracking active before first user interaction

```
com.singular.preinstall.READ_PERMISSION_SINGULAR
```

Behaviour confirmed: install-attribution signal collection begins at install time, prior to first app launch and prior to any consent screen

Impact: com.singular.preinstall.READ_PERMISSION_SINGULAR registers install-attribution tracking that becomes active before the user has opened the app for the first time and before any consent dialogue is shown. Attribution data collection that begins at install, ahead of any consent capture mechanism, is structurally the same Art. 7(1) timing failure as a pre-consent analytics SDK: the processing starts before consent can exist to cover it.

Impact Analysis

C1, C2, and C3 together describe an application that collects substantially more about its users, and transmits substantially more of what it collects to third parties, than a food-delivery service requires. C1 means a subset of DoorDash's user base undergoes government-ID and facial-biometric verification without a basis proportionate to ordering food. C2 is a production credential-hygiene failure independent of any other finding — an extractable Firebase key set with no special targeting required. C3 means that, for any user with a medically relevant dietary restriction, a visual record of their order-selection behaviour is replayed on US infrastructure outside DoorDash's own systems.

H1 through H5 compound this picture rather than standing apart from it: the same order interaction that triggers Sentry replay also feeds dietary and location signals to Meta (H1), is scored in parallel by four independent undisclosed fraud engines including one using behavioural biometrics (H4), and sits inside a binary that also embeds a competitor's codebase (H2), requests contact-database write access beyond any disclosed feature (H3), and began tracking the user via Singular before the app was ever opened (H5). No single finding here is, by itself, an exotic attack. Collectively, they describe a data-collection architecture that is broader than disclosed and that a user has no practical way to evaluate before installing the app.

The Complete Chain: From Download to Undisclosed Cross-Border Profiling

Step 1 — Download: Install DoorDash (com.dd.doordash) from the Google Play Store. No account or identity verification is required to download.

Step 2 — Extract: Pull the installed APK bundle via adb pull, or obtain it directly from Play. The base.apk is approximately 197 MB, spanning 15 DEX files.

Step 3 — Decompile: Run apktool d base.apk. All 164,643 smali classes and resource files are baksmali'd and decompressed, exposing every SDK listed in this report in plaintext class and string form.

Step 4 — Observe pre-consent tracking: Before the user ever opens the app, com.singular.p.reinstall.READ_PERMISSION_SINGULAR (H5) has already begun collecting install-attribution data.

Step 5 — Identity verification: During account setup or an order flagged for verification, the bundled Persona SDK (C1, 4,806 smali classes) performs government-ID scanning, facial liveness matching, and NFC passport-chip reading — a biometric identity check disproportionate to the stated purpose of ordering food.

Step 6 — Order interaction: As the user browses restaurants, selects dietary filters, and enters a delivery address, Sentry's RRweb module (C3) visually records the full interaction. Simultaneously, the Facebook SDK (H1) transmits dietary and precise-location signals to Meta's advertising infrastructure, and four independent fraud engines — Sift Science, Riskified, Signifyd, and Forter (H4) — score the same interaction in parallel, Forter via behavioural biometrics such as typing rhythm and scroll velocity.

Step 7 — Payment and completion: Payment-method selection is captured in the same Sentry session replay as the dietary and address data (C3). The hardcoded Firebase credential set (C2) remains present and extractable in this same binary throughout, independent of anything the user does.

Step 8 — Ancillary surfaces: READ_CONTACTS/WRITE_CONTACTS (H3) gives the application standing access to the full contact database well beyond what any "send to a friend" feature requires, and the embedded Deliveroo codebase (H2) raises an open, undisclosed data-routing question about whether any of this flows through a competing platform's infrastructure.

By the time a single order is completed, a user's biometric identity, dietary preferences, precise location, visual interaction history, and contact-database access have reached at least nine distinct third-party processors — Persona, Firebase/Google, Sentry, Meta, Sift Science, Riskified, Signifyd, Forter, and Singular — several without a demonstrable Art. 6 or Art. 9 legal basis, and none of this requires any special attacker capability to observe: it is the application's designed behaviour, visible to anyone who decompiles the public binary.

Data Protection — Article by Article

Art. 9(1)/Art. 9(2) GDPR — Special categories of data: C1's biometric identity verification processes special-category data. Art. 9(1) prohibits this absent an Art. 9(2) basis, and ordering food is not a basis that establishes the necessity of biometric identification of the general user population. C3's dietary-preference capture via session replay raises the same Art. 9 question conditionally, wherever the preference reflects a medical condition.

Art. 32 GDPR — Security of processing: C2's hardcoded Firebase credentials are a direct failure of the technical measures Art. 32(1)(b) requires to maintain ongoing confidentiality of systems processing personal data.

Art. 44 GDPR (Chapter V) — General principle for transfers: C1's biometric data is processed by Persona in the United States. Absent a valid transfer mechanism and adequacy finding specific to this processing, this is an unlawful international transfer of special-category data.

Art. 28 GDPR — Processor: Persona was not identified as a disclosed Art. 28 processor in the DoorDash privacy documentation reviewed for this audit (C1), nor were the four fraud-profiling vendors in H4.

Art. 7(1) GDPR — Conditions for consent: H5's Singular attribution tracking begins at install, before any consent mechanism can be presented — a structural timing failure identical in kind to a pre-consent analytics SDK.

Art. 5(1)(b) GDPR — Purpose limitation: H1's transmission of dietary and location data to Meta's advertising infrastructure, and C3's visual capture of the same categories for session replay, both exceed the stated operational purpose of fulfilling a food order.

Art. 5(1)(c) GDPR — Data minimisation: H3's contact-database read/write access exceeds what any disclosed feature requires.

Art. 13(1)(e) GDPR — Transparency, recipients of data: H2's embedded Deliveroo codebase and H4's four fraud-profiling vendors were not identified as data recipients in the documentation reviewed.

Art. 26 GDPR — Joint controllers: H1 engages Meta's joint-controller status for data collected through its SDK (CJEU C-40/17), requiring an Art. 26 arrangement.

Art. 22 GDPR — Automated decision-making: H4's four parallel fraud-scoring engines raise an open question of whether any resulting automated decision (order block, account restriction) falls under Art. 22 and its associated safeguards.

Art. 33(4) GDPR — Notification of a personal data breach: RFI-IRFOS explicitly invoked this provision on 24 August 2026. If DoorDash determines any of C1-C3 constitutes a personal data breach with risk to data subjects, the 72-hour notification clock runs from the date DoorDash became aware — at the latest, 21 June 2026, the date of initial disclosure.

Regulatory & Legal Landscape

RFI-IRFOS BCC'd three supervisory authorities across this correspondence as the inferred relevant regulators for a GDPR disclosure concerning a globally distributed Play Store application processing data of EU-resident users under Art. 3(2) extraterritorial scope: the Austrian Datenschutzbehörde (dsb@dsb.gv.at), CERT.at, and the Irish Data Protection Commission (info@dataprotection.ie) — the Irish DPC as the plausible lead authority for a US company's EU-facing data processing, consistent with the common practice of US technology companies routing EU operations through an Irish entity. RFI-IRFOS has not independently confirmed DoorDash's specific EU corporate structure or lead supervisory authority designation; this report states the regulators notified, not a confirmed Art. 56 lead-authority finding.

DoorDash, Inc. is a US company additionally subject to the California Consumer Privacy Act (CCPA/CPRA) for California residents and to FTC Act Section 5 unfair-or-deceptive-practices enforcement for undisclosed data collection and sharing practices generally.

Fine exposure under GDPR, to the extent EU-resident users are processed under Art. 3(2): Art. 83(5) applies to Art. 9 special-category violations (C1, conditionally C3) and Art. 32 security failures (C2) — administrative fines up to EUR 20,000,000 or 4% of total worldwide annual turnover, whichever is higher. Art. 83(4) applies to Art. 5, 13, and 28 violations (H1-H5) — up to EUR 10,000,000 or 2% of total worldwide annual turnover.

Indicators of Compromise

The following identifiers were extracted from the production APK (base.apk, audited 2026-06-21) via static analysis only. No DoorDash servers, accounts, or infrastructure were probed. Any access logs or API calls referencing these identifiers outside DoorDash's own legitimate application traffic should be treated as a potential unauthorized-access indicator.

```
C2 -- Firebase Realtime Database URL
Value: https://doordash-consumer-android.firebaseio.com

C2 -- Firebase Google App ID
Value: 1:302242645714:android:6d1d682471fc54fd

C2 -- Firebase API Key 1
Value: AIzaSyBqiyThWC0b7pvmAsrNSwHyA-yYsZ-1myg

C2 -- Firebase API Key 2
Value: AIzaSyChoIqwJTln60tEJY4cPGQMnpWafmwidjE

C1 -- Persona SDK packages
com.withpersona.sdk, com.withpersona.sdk2 (4,806 smali classes)

C3 -- Sentry / RRweb packages
io.sentry (1,619 smali classes), io.sentry.rrweb (23 smali classes)

H2 -- Embedded Deliveroo packages
com.deliveroo.common, com.deliveroo.logging, com.deliveroo.rooblocks

H4 -- Fraud-profiling SDK packages
siftscience/android, com.riskified.android_sdk,
com.signifyd.profiling, com.forter.mobile

H5 -- Singular attribution permission
com.singular.preinstall.READ_PERMISSION_SINGULAR
```

Disclosure Timeline & Outcome

2026-06-21 Initial disclosure (R1, REF DOORDASH-2026-R1) sent to security@doordash.com and privacy@doordash.com. BCC: Austrian DSB, CERT.at, Irish Data Protection Commission. Automated "Global Threat Defense Team" HackerOne-redirect reply received the same day.

2026-06-27 6-day follow-up. CC press@doordash.com added. BCC: DSB, CERT.at. Identical automated reply received.

2026-07-23 Follow-up, 27 days since R1 by RFI-IRFOS's own count. CC: DSB. Identical automated reply received.

2026-08-05 45-day follow-up. CC: DSB, CERT.at. Identical automated reply received.

2026-08-15 55-day follow-up. Notes a new "no longer monitored" notice on an address that had never substantively replied either. CC: DSB. Identical automated reply received.

2026-08-24 Follow-up explicitly invoking Art. 33(4) GDPR: if treated as a personal data breach, the 72-hour supervisory-authority notification clock was already running, and an internal review in progress does not delay the initial notification. Notes that the very first reply (21 June) was at least a contextually appropriate automated acknowledgment, and that every reply since had been the identical bot text with zero human engagement. Embargo restated: 26 September 2026. CC: DSB. Identical automated reply received.

2026-08-31 Final follow-up in this thread, formalising REF DOORDASH-2026-R1 in the subject line. "Seven days since our last message, same automated redirect." CC: DSB, CERT.at, press@doordash.com. Identical automated reply received — the seventh and last reply in the thread, and, like every one before it, from the automated system rather than a human being.

2026-09-26 90-day coordinated-disclosure embargo elapses. No human reply, confirmation, or remediation evidence received at any point in the preceding 97 days.

2026-10-17 This report published, 21 days after the embargo date. All eight findings confirmed unaddressed on the basis of the correspondence record; no re-verification download was performed for this report.

What DoorDash Got Right

The application declares both `DETECT_SCREEN_CAPTURE` and `DETECT_SCREEN_RECORDING`, actively monitoring for screen capture and screen recording attempts — a deliberate anti-fraud and anti-scraping measure that reflects genuine security awareness in the engineering process, not an oversight. The Network Security Configuration's cleartext-override exception is scoped to debug builds only and does not apply to the production risk surface.

These choices do not offset the findings in this report. DoorDash actively defends against a user screen-recording their own session while simultaneously shipping no certificate pinning on any production API endpoint, meaning payment and order traffic has no additional protection against network-level interception on a compromised network beyond standard TLS. Security awareness in one area does not substitute for it in another, and the gap between the two is itself informative: the application's threat model appears to weight fraud and IP-protection concerns (screen capture, behavioural biometrics, pre-install attribution) considerably more heavily than it weights data minimisation and transparency toward the user whose data is being collected.

Residual Risk & Recommendations

C1 — Immediate: Conduct and document a formal necessity and proportionality assessment for Persona biometric verification against an Art. 9(2) basis, scoped specifically to the food-delivery context in which it is deployed. Disclose Persona as an Art. 28 processor. Resolve the Art. 44 international-transfer basis for biometric data processed in the United States, or restrict biometric verification to the narrow subset of cases (if any) where it is genuinely necessary and disclosed.

C2 — Immediate: Rotate all three Firebase credentials and both additional API keys. Apply Firebase console API-key restrictions (Android package + method restrictions). Audit Firebase Realtime Database security rules for unauthenticated read/write exposure.

C3 — Structural: Exclude dietary filter, order, address, and payment screens from Sentry Session Replay capture, or disable RRweb entirely in favour of non-visual error diagnostics. Where any visual capture of order interactions is retained, document the Art. 9 basis for any dietary data that may constitute health data.

H1 — Governance: Confirm an Art. 26 joint-controller arrangement with Meta covering the specific data flows identified, and an Art. 6(1)(a) consent basis for dietary and location signals reaching advertising infrastructure. Add Meta to the Art. 13 transparency notice if not already present with this level of specificity.

H2 — Transparency: Disclose the Deliveroo codebase integration and clarify, in writing, whether any user data is processed through or shared with Deliveroo infrastructure as a result.

H3 — Immediate: Remove `WRITE_CONTACTS` entirely unless a specific, disclosed feature requires write access. Replace standing `READ_CONTACTS` with the Android system contact picker intent, which requires no special permission, for any "send to a friend" style feature.

H4 — Governance: Disclose Sift Science, Riskified, Signifyd, and Forter as data recipients under Art. 13(1)(e). Assess whether Forter's behavioural-biometric profiling, or any automated decision produced by the combination of all four engines, falls under Art. 22 and requires the associated safeguards.

H5 — Structural: Delay Singular attribution-tracking initialisation until after the consent screen is shown and a consent decision is recorded, consistent with Art. 7(1).

Network Security — Implement certificate pinning on all production API endpoints carrying payment and order data, independent of and in addition to the screen-capture detection already in place.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis of the published application using publicly available tooling. No servers, accounts, or DoorDash 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 DOORDASH-2026.