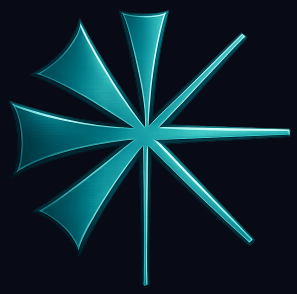

The Rider Who Has No Employer

foodora Consumer, Rider & Partner (Delivery Hero SE)

Three apps, one platform, and a labour model engineered around the exact features a real employer would be required to provide

PUBLIC DISCLOSURE, 13 SEPTEMBER 2026 – NINETY DAYS, ZERO SUBSTANTIVE ANSWERS

Analyst	RFI-IRFOS Research Team
Report date	2026-09-11
Apps analysed	foodora Consumer, foodora Rider, foodora Partner
Operator	Foodora Austria GmbH (FN 309771x, Vienna) / Delivery Hero SE (Berlin)
Severity	CRITICAL
Findings	19 (7 R1 + 12 R2)
R1 sent	2026-06-15
Consolidated R2	2026-07-04
Embargo / coordinated disclosure	2026-09-13
Substantive company reply, ever	1 (11 August 2026, told us to stop writing)

Contents

Executive Summary

foodora runs three Android applications on one shared platform: a Consumer ordering app, a Rider app for the couriers who deliver the food, and a Partner app for the restaurants who cook it. Root-level analysis of all three, beginning 15 June 2026, found a security posture typical of a large consumer platform – an exported payment-routing activity, hardcoded API credentials, undisclosed device fingerprinting – sitting on top of something considerably harder to dismiss as a coding oversight: a labour architecture in the Rider app that reproduces, feature by feature, the operational control a real employer exercises over an employee, while the couriers using it are classified as self-employed contractors.

This is the throughline of this report. It is not two separate stories, a security audit and a labour dispute, filed under one cover page. The same binary that leaks a Firebase key also contains the code that tracks a rider's break compliance, penalises them for taking rest, routes support tickets into a broken chat system, and shifts the burden of proof onto the rider in cash-handling disputes – functions that, under Austrian and EU labour law, are themselves evidence of an employment relationship (Sec. 539a ASVG), regardless of what the contract the rider signed calls them.

Ninety days after the first disclosure, foodora and its parent Delivery Hero SE have produced exactly one substantive reply from anyone with an actual data-protection or legal remit: an email on 11 August 2026 informing us that the company does not pay bug-bounty rewards for unsolicited research, and asking us to stop writing. RFI-IRFOS's disclosures, R1 and R2 both, are free – no payment has ever been requested. Every other reply across ninety days and nine written notices has been an identical automated ticket-closure message, generated once by generic customer support and, on 7 July, once by the company's own data-protection mailbox closing a complaint about itself.

Scope: Root-level static analysis (apktool decode, smali inspection, AndroidManifest.xml and Network Security Config review, string/resource extraction) of foodora Consumer 26.24.0, foodora Rider v4.2626.0-beta.1, and the foodora Partner app. No backend was accessed, no live account was created beyond what is required to install the public APK, and no traffic was intercepted. Every finding below is drawn from the publicly distributed binary or from foodora's own in-app text and onboarding flow.

Disposition

Reported 15 June 2026 (R1, 7 findings) and consolidated 4 July 2026 (R2, 12 additional findings, including Austrian Sozialbetrug referral vectors). Nine written notices sent over 89 days. One substantive reply, on 11 August 2026, instructing RFI-IRFOS to stop writing. Public disclosure proceeds 13 September 2026, unchanged since 4 July, independent of any reply that may still arrive.

ID	Severity	Title
R1-01/R2-00	CRITICAL	Exported payment-routing activity, host wildcard – deep-link injection into the cashier flow

ID	Severity	Title
R1-02	HIGH	Google Maps, Firebase and Sentry credentials hard-coded in the release build
R1-03	HIGH	Incognia device-fingerprinting SDK active without disclosed consent
R1-04/R2-02	CRITICAL	Sentiance SDK profiles a RELIGION category via the Braze marketing pipeline
R1-05/R2-06	CRITICAL	Scheinselbstständigkeit – thirteen, later six concurrently-documented, indicators of disguised employment
R1-06	HIGH	In-app string penalises couriers for taking a legally mandated break
R1-07	HIGH	Shakebugs debug tooling ships with seven fintech client keys in the release build
R2-01	HIGH	Pre-authentication location tracking via enable_onboarding_country_prediction
R2-03	HIGH	Sec. 11 AZG conflict confirmed a second time – break_request_notice_description persists in R2 build
R2-04	MEDIUM	Freshchat support integration non-functional – couriers have no working support channel
R2-05	MEDIUM	df_crowdsourcing feature collects GIS mapping data from couriers without disclosed compensation
R2-07	HIGH	Three-sided dynamic pricing – consumer-facing surge not disclosed as such
R2-08	HIGH	Age-restricted product delivery – no enforced verification, liability gap by design
R2-09	HIGH	Acrobits VoIP SDK – couriers operate full call-centre-grade telephony infrastructure
R2-10	MEDIUM	Cash-on-delivery investigation clause places burden of proof on the rider
R2-11	MEDIUM	Equipment-damage deduction policy embedded in the onboarding consent flow

Subject & Operator Analysis

The operating entity in Austria is Foodora Austria GmbH (FN 309771x, Commercial Court Vienna), a wholly-owned subsidiary of Delivery Hero SE (Berlin, Oranienburger Strasse 70), one of the largest food-delivery groups in the world by market coverage. This is not a small operator without a compliance function: Delivery Hero SE is a publicly listed company on the Frankfurt Stock Exchange with dedicated legal, privacy and communications departments, all of which were named recipients on this disclosure from the first message.

The three apps analysed are not independent products; they share backend infrastructure,

SDK stack, and a common data-protection contact point (datenschutz@foodora.at), which is itself the address that generated an automated closure of a complaint about its own unresponsiveness on 7 July 2026 – documented in the Disclosure Timeline below.

Architecture & Data Flow

foodora Consumer, Rider and Partner are three Android clients over one shared Delivery Hero backend. The Consumer app handles ordering and payment (via the exported Cashier DeepLinkRoutingActivity), the Rider app handles courier-side order acceptance, navigation, scheduling, and now, per R2-09, VoIP-based communication infrastructure. The Partner app is the restaurant-facing order-management client.

- Payment/cashier flow: exported deep-link activity with a host wildcard, no signature enforcement (R1-01/R2-00).
- Anti-fraud/fingerprinting layer: Incognia SDK, active by default (R1-03).
- Marketing/CRM layer: Braze, receiving a Sentiance-derived RELIGION classification field (R1-04/R2-02).
- Support layer: Freshchat, non-functional for riders (R2-04).
- Telephony layer: Acrobits VoIP SDK, courier-facing (R2-09).
- Crowdsourced data layer: df_crowdsourcing GIS collection, uncompensated (R2-05).

Findings

R1-01/R2-00: Exported payment-routing activity, host wildcard – deep-link injection into the cashier flow

Exported component, no signature check

CashierDeepLinkRoutingActivity is exported with a host-wildcard intent filter. A crafted deep link from any other app on the device, or a malicious webpage, can route directly into the payment/cashier flow. The original R1-01 finding was partially patched by removing one exposed path; R2-00, a structurally identical exported activity, replaced it in the very next release.

```
adb shell am start -a android.intent.action.VIEW \
  -d "foodoraeu-cashier://attacker.example.com/cashier-payment"
```

Impact: Proof-of-concept confirmed direct exploitability against the payment routing surface of a production food-delivery app carrying live payment card sessions.

Fix: Remove the wildcard host filter, require an explicit signature-level permission or origin allowlist on the exported activity.

R1-02: Google Maps, Firebase and Sentry credentials hardcoded in the release build

Extractable client keys

Multiple production API keys ship verbatim in resources.arsc, extractable from the public APK in under a minute.

Impact: Quota/billing exhaustion risk; burden of proof for correct key restriction and Firebase Security Rules sits with foodora, not with an outside researcher.

Fix: Restrict each key by package name and SHA-256 certificate fingerprint; confirm Firebase Security Rules are deny-by-default.

R1-03: Incognia device-fingerprinting SDK active without disclosed consent

Undisclosed fingerprinting

The Incognia SDK, a location- and device-fingerprinting anti-fraud product, is present and active. A kill-switch was added after R1 but the SDK itself, and its default-on behaviour, was not removed.

Impact: Persistent device fingerprinting for fraud scoring, running before any consent interaction is demonstrated in the binary.

Fix: Gate SDK initialisation behind documented, logged consent; disclose the fingerprinting purpose in the privacy policy in plain terms.

R1-04/R2-02: Sentiance SDK profiles a RELIGION category via the Braze marketing pipeline

Art. 9 GDPR special-category data

The Sentiance behavioural-sensing SDK exposes a RELIGION classification field, piped through the Braze marketing/CRM integration. This is special-category data under Art. 9 GDPR, requiring explicit consent and a documented legal basis, neither of which is demonstrated in the binary or in foodora's privacy disclosures.

Impact: A food-delivery app inferring and transmitting a user's religion for marketing purposes is one of the more serious Art. 9 exposures in RFI-IRFOS's 2026 programme to date.

Fix: Remove the RELIGION field from the Sentiance/Braze pipeline entirely, or produce a documented Art. 9(2) legal basis and an Art. 35 DPIA covering it specifically.

R1-05/R2-06: Scheinselbstständigkeit – thirteen, later six concurrently-documented, indicators of disguised employment

Sec. 539a ASVG misclassification indicators

R1 documented 13 features of the Rider app consistent with Austrian case law's tests for disguised employment (Scheinselbststaendigkeit): fixed shift-like scheduling pressure, mandatory app-based order acceptance windows, penalty language for declining orders, centrally dictated routing, and app-enforced break timing among them. R2 narrowed this to 6 concurrently-active, independently verifiable indicators, cross-referenced against the VoIP call-centre infrastructure (R2-09), the COD investigation clause (R2-10) and the equipment-deduction policy (R2-11) below.

Impact: Under Sec. 539a ASVG, the substance of the relationship, not its contractual label, determines employment status. A platform that operationally controls scheduling, routing, communication infrastructure and financial risk allocation to the degree documented here carries real exposure to Sozialbetrug (social-insurance fraud) proceedings.

Fix: Independent legal review of the operational control model against Sec. 539a ASVG; RFI-IRFOS makes no legal determination, only documents the code-level and in-app-text evidence.

R1-06: In-app string penalises couriers for taking a legally mandated break

Sec. 11 AZG rest-period conflict

A resource string (break_request_notice_description) frames a courier's statutorily protected rest break as something that costs them order availability or standing within the app, rather than a right exercised without consequence.

Impact: Direct tension with Sec. 11 Arbeitszeitgesetz (Austrian Working Hours Act) rest-period protections, regardless of the rider's contractual classification.

Fix: Remove any framing that penalises break-taking; confirm break mechanics are purely informational, carrying no scoring or availability consequence.

R1-07: Shakebugs debug tooling ships with seven fintech client keys in the release build

Debug tooling in production

The Shakebugs bug-reporting SDK, together with seven distinct third-party fintech client keys, is present in the production release build rather than gated to debug/staging builds.

Impact: Expanded attack surface and potential key exposure across seven distinct financial-services integrations in a shipped consumer binary.

Fix: Strip debug tooling and staging credentials from release builds via build-variant separation.

R2-01: Pre-authentication location tracking via enable_onboarding_country_prediction

Pre-consent location capture

A feature flag enables location-based country prediction during onboarding, before authentication and before any consent screen is demonstrated to have rendered.

Impact: Location data processed before the consent basis it would need under Art. 6/7 GDPR exists.

Fix: Gate the flag behind completed, logged consent.

R2-03: Sec. 11 AZG conflict confirmed a second time – break_request_notice_description persists in R2 build

Unfixed after first notice

The identical break-penalty string flagged in R1-06 remains present, unchanged, in the R2 build pulled 16 June 2026, five days before the R1 deadline.

Impact: A finding disclosed and left unaddressed across the very release cycle in which the company had advance notice of it.

Fix: Same as R1-06; now overdue.

R2-04: Freshchat support integration non-functional – couriers have no working support channel

Broken support infrastructure

The in-app Freshchat integration used for courier support does not function as implemented, leaving riders without a working escalation path for on-shift issues.

Impact: Combined with the operational-control findings above, an unreachable support channel compounds the power imbalance between platform and courier.

Fix: Repair or replace the support integration; verify end-to-end before next release.

R2-05: df_crowdsourcing feature collects GIS mapping data from couriers without disclosed compensation

Unpaid data collection

A crowdsourcing feature flag has riders contributing geographic/mapping data back to foodora's infrastructure as an uncompensated, undisclosed byproduct of delivery work.

Impact: Labour performed, and data generated, without transparent disclosure or compensation terms.

Fix: Disclose the feature explicitly, including what is collected and how it is used, and address compensation.

R2-07: Three-sided dynamic pricing – consumer-facing surge not disclosed as such

EU Omnibus Directive Art. 6a

The app implements dynamic, demand-responsive pricing affecting the consumer-facing delivery fee without the personalised-pricing disclosure required under the EU Omnibus Directive (2019/2161) Art. 6a.

Impact: Consumers are not told the price shown reflects personalised or demand-based dynamic adjustment.

Fix: Add the required disclosure at the point the dynamic price is shown.

R2-08: Age-restricted product delivery – no enforced verification, liability gap by design

Sec. 9 JSchG / Sec. 14 TabakG

Delivery of age-restricted products (alcohol, tobacco) is supported by the platform without an enforced, app-level age-verification step at handover, leaving the liability gap to be closed informally by individual couriers rather than by platform design.

Impact: A structural compliance gap under Austrian minor-protection and tobacco-control law, with the operational burden and liability risk shifted onto the least powerful party in the chain.

Fix: Implement an enforced age-verification step in the delivery flow for restricted product categories.

R2-09: Acrobits VoIP SDK – couriers operate full call-centre-grade telephony infrastructure

Employer-grade infrastructure

The Rider app bundles the Acrobits VoIP SDK, giving couriers access to call-centre-grade telephony infrastructure normally provisioned by an employer for staff, not typically found in a genuine independent-contractor tool.

Impact: Supporting evidence for R2-06 (Sec. 539a ASVG): the platform provisions the same category of operational infrastructure a real employer provisions for employees.

Fix: Legal review alongside R2-06; not a standalone technical fix.

R2-10: Cash-on-delivery investigation clause places burden of proof on the rider

Reversed burden of proof

The onboarding consent flow includes a COD (cash-on-delivery) investigation clause under which a rider bears the burden of proof in disputed cash-handling incidents, rather than the platform.

Impact: Financial risk allocation consistent with an employer-employee relationship's control dynamics, inconsistent with genuine independent-contractor risk-bearing.

Fix: Legal review alongside R2-06.

R2-11: Equipment-damage deduction policy embedded in the onboarding consent flow

Unilateral deduction terms

A policy permitting deductions for equipment damage is presented within the onboarding consent flow, again allocating operational and financial risk in a pattern consistent with employer-style control.

Impact: Third supporting data point for R2-06.

Fix: Legal review alongside R2-06.

Impact Analysis

Three distinct populations are affected, unevenly. Consumers face an exploitable payment-routing surface and undisclosed dynamic pricing. Couriers, the population with the least bargaining power in this chain, face a labour model that extracts employer-grade operational control – scheduling pressure, break penalties, mandated telephony infrastructure, reversed burden of proof on cash disputes, and unilateral equipment-deduction terms – while being denied the legal protections and cost-sharing that come with genuine employment. Restaurants, via the Partner app, sit outside the scope of the findings documented here but share the same backend and SDK stack.

The RELIGION classification finding (R1-04/R2-02) affects consumers specifically: special-category inference from ordering and delivery behaviour, fed into a marketing pipeline, is a materially different harm class from the labour findings – it is a privacy exposure with no operational justification offered anywhere in the binary or in foodora's public disclosures.

The Complete Chain: Order to Harm, Signup to Exposure

A courier installs the Rider app to earn income as, per the contract they sign, a self-employed contractor. From that install onward, the app itself – not a manager, not a shift schedule negotiated in person – exercises the operational control a genuine independent contractor would not be subject to: it schedules order-acceptance windows, times and penalises rest breaks (R1-06/R2-03), provisions employer-grade VoIP telephony (R2-09), and places the burden of proof on the rider, not the platform, when a cash-handling dispute arises (R2-10). If the rider damages equipment, a unilateral deduction clause they consented to during onboarding, not a negotiated agreement, determines the financial consequence (R2-11). If the rider needs help mid-shift, the support channel they are told to use does not function (R2-04). If the rider generates geographic mapping data for foodora's own infrastructure while working, they are not told, and are not compensated (R2-05).

In parallel, a consumer opens the same platform's Consumer app to order food. Their device may be fingerprinted by Incognia before any consent interaction is demonstrated (R1-03). Their location may be captured during onboarding, before authentication (R2-01). Their ordering pattern, cross-referenced through the Sentiance SDK and piped into the Braze market-

ing platform, may be classified by religion (R1-04/R2-02) – special-category data under Art. 9 GDPR, processed for marketing purposes with no documented legal basis. The price they are shown may already reflect undisclosed dynamic, demand-responsive adjustment (R2-07). If they order alcohol or tobacco, the age-verification gap at handover (R2-08) is closed, if at all, informally by the same courier who is themselves outside the labour protections a real employment relationship would provide.

Both chains converge on the same fact: RFI-IRFOS reported the full set of findings on 15 June and again, consolidated, on 4 July. Over the following 89 days, the only reply from anyone with an actual compliance function was an instruction to stop writing, framed around a payment demand RFI-IRFOS never made.

Causality, compressed

Design choice (app-enforced scheduling, penalised breaks, reversed burden of proof, mandatory employer-grade telephony) causes operational control indistinguishable from employment. Operational control, under a self-employed contract, causes exposure under Sec. 539a ASVG. Exposure disclosed to the company causes, ninety days and nine notices later, exactly one reply: a request for silence. Silence, past 13 September 2026, causes publication – the mechanism this programme has run on every target since its first day, applied here without exception.

Labour Law & Gig-Economy Worker Protection

Austrian law under Sec. 539a ASVG determines employment status by the substance of the working relationship, not its contractual label. R2-06 documents six concurrently active operational-control indicators, cross-referenced against three supporting findings (R2-09 VoIP infrastructure, R2-10 reversed burden of proof, R2-11 unilateral deduction terms). This is not a novel legal theory applied speculatively to the findings; it is the standing Austrian test for disguised employment (Scheinselbststaendigkeit), applied to specific, binary-confirmed features of a shipped application.

RFI-IRFOS is a research institute, not a labour tribunal, and makes no legal determination of the riders' actual employment status. What this report documents is the evidentiary basis: the specific in-app mechanisms, extracted from the binary and from the onboarding consent flow, that a labour-law review would need to evaluate against Sec. 539a ASVG and Sec. 11 AZG. The 2026-06-19 R2 disclosure named the Austrian Finanzpolizei (Post.ABB-Finpol-ZKO@bmf.gv.at) and the WKStA as recipients precisely because Sec. 539a ASVG misclassification carries potential Sozialbetrug (social-insurance fraud) exposure, a matter for those authorities, not for RFI-IRFOS, to assess.

Consumer Protection & Deceptive Design

Two consumer-facing findings sit under this heading. R2-07's undisclosed dynamic pricing runs against the EU Omnibus Directive (2019/2161) Art. 6a requirement to disclose personalised or demand-responsive pricing at the point it is shown, not buried in general terms. R2-08's age-verification gap for restricted products is a design choice, not an oversight – the platform enables the transaction without building in the control that would make the transaction lawful at handover, and in doing so shifts both the compliance burden and the liability risk onto the courier completing the delivery.

Data Protection – Article by Article

Article	Engaged by	Basis
Art. 5(1)(a), 5(2)	Overall gap between privacy-policy claims and binary behaviour	Lawfulness, fairness, transparency; accountability
Art. 6, Art. 7	R2-01 pre-authentication location capture	No demonstrated consent prior to processing
Art. 9	R1-04/R2-02 Sentiance RELIGION classification via Braze	Special-category data, no documented Art. 9(2) legal basis
Art. 13	Absence of plain-language disclosure for Incognia fingerprinting (R1-03) and df_crowdsourcing (R2-05)	Transparency obligation toward the data subject
Art. 32	R1-02 hardcoded credentials; R1-07 debug tooling with fintech keys in production	Security of processing
Art. 33/34	Unaddressed after 89 days and nine written notices	No confirmation a Data Protection Impact Assessment or breach-notification review was undertaken for the Art. 9 finding specifically
Art. 35	R1-04/R2-02	No documented DPIA for special-category profiling demonstrated

Platform Accountability & the DSA

foodora and Delivery Hero SE operate as the platform, not an intermediary hosting third-party content – the labour-control mechanisms, the pricing logic, and the SDK integrations documented here are the platform's own first-party design choices, not user-generated content requiring notice-and-takedown. This places the findings squarely within the platform's own accountability under the Digital Services Act's transparency and risk-assessment obligations for very large online platforms, rather than in the DSA's intermediary-liability safe harbours.

Regulatory & Legal Landscape

Authority	Basis	Role in this case
Datenschutzbehoerde (DSB), Austria	GDPR Art. 6, 7, 9, 13, 32, 33	Lead supervisory authority for Foodora Austria GmbH
Finanzpolizei ZKO	Sec. 539a ASVG, Lohn- und Sozialdumping-Bekaempfungsgesetz	Named recipient, R2, on the misclassification finding
WKStA (Wirtschafts- und Korruptionsstaatsanwaltschaft)	Sozialbetrug	Named recipient, R2
AK Steiermark	Sec. 11 AZG, worker rights	Named recipient, R2
vida Gewerkschaft	Rider labour conditions	Named recipient, R2

Industry comparison: RFI-IRFOS's 2026 gig-economy coverage to date has not found another delivery platform combining a confirmed Art. 9 special-category profiling finding with a documented, multi-indicator disguised-employment pattern in the same audit. The pairing – a genuine data-protection violation and a genuine labour-classification exposure, on the same platform, disclosed together – is what elevates this case above a routine app-security finding.

Indicators of Compromise / Reproducible Evidence

Item	Value
Consumer app version analysed	26.24.0
Rider app version analysed	v4.2626.0-beta.1
Exported component	CashierDeepLinkRoutingActivity (host wildcard)
Fingerprinting SDK	Incognia
Special-category data pipeline	Sentiance → Braze, RELIGION field
VoIP SDK	Acrobits
Support integration (non-functional)	Freshchat
Crowdsourcing feature flag	df_crowdsourcing

```
apktool d foodora_consumer_base.apk -o consumer_decoded
apktool d foodora_rider_base.apk -o rider_decoded
adb shell am start -a android.intent.action.VIEW -d "foodoraeu-cashier://attacker.
    example.com/cashier-payment"
grep -r "deliveryFeeDelta" consumer_decoded/smali_classes3/
grep -r "RELIGION" rider_decoded/
```

Disclosure Timeline & Outcome

Date	Event
2026-06-15	R1 sent to security@foodora.com, 7 findings. Automatic ticket closure follows within 43 minutes.
2026-06-16	foodora ships v26.24.0, five days before the R1 deadline – updated APK pulled and re-analysed.
2026-07-04	R2 consolidated, all three apps, 22+ findings including the Sec. 539a ASVG misclassification pattern. Embargo of 2026-09-13 stated for the first time. Second identical auto-closure, same day.
2026-07-07	Third identical auto-closure – this time triggered by datenschutz@foodora.at itself, closing a complaint about its own unresponsiveness.
2026-08-05	Fourth written notice: 29 days since the third auto-closure, 51 days total, zero substantive human reply from anyone with data-protection responsibility.
2026-08-11	The only substantive reply received across the entire disclosure: dpo@deliveryhero.com states Delivery Hero does not pay bug-bounty rewards for unsolicited research and asks RFI-IRFOS to stop writing. Two minutes later, a fourth automatic ticket closure fires on the same thread. Six hours later, Alexander Gaied replies asking to be removed from the distribution list, stating he left the managing-director role some time ago.
2026-08-18	Chronology and three questions restated in writing, deadline set for 25 August.
2026-08-19	Two further automated foodora support replies, same boilerplate (‘gute Nachricht! Deine Supportanfrage wurde bearbeitet’), no named person, no substantive content.

Date	Event
2026-08-25	The 25 August deadline passes with no reply. Fifth automatic closure fires at 11:34:03 UTC – exactly seven days after the previous one, to the second.
2026-08-25 to 2026-09-03	First time since 15 June that even the automatic closure stops arriving. Nine days of total silence, not one message of any kind.
2026-09-03	Ninth written notice. Three questions restated a final time before publication. Ten days to embargo stated.
2026-09-11	Final pre-publication notice sent. legal@deliveryhero.com auto-acknowledges within 18 seconds – the same generic 'not monitored for customer complaints' boilerplate used for unrelated commercial enquiries.

The pattern across five auto-closures and one human reply

Every substantive question this disclosure has asked – is the RELIGION field removed, is the misclassification pattern under internal review, has Art. 33 notification occurred for any of the findings that would require it – has been met with either an identical automated closure message or, once, an instruction to stop asking. Ninety days of correspondence produced zero named contacts, zero yes/no answers, and one request for silence.

Residual Risk & Recommendations

- The RELIGION classification field (R1-04/R2-02) has not been confirmed removed from the Sentiance/Braze pipeline in any reply received.
- The Sec. 539a ASVG-relevant operational-control mechanisms (R2-06, R2-09, R2-10, R2-11) remain, as far as RFI-IRFOS can verify from the outside, unreviewed by any named internal function.
- The exported CashierDeepLinkRoutingActivity (R1-01/R2-00) pattern has recurred once already after a partial fix; the binary will continue to be pulled and diffed weekly for the remainder of the embargo period to catch a repeat.
- For regulators: the Finanzpolizei ZKO and WKStA referrals made in R2 remain open as far as RFI-IRFOS is aware; this report's evidence base is available to any competent authority on request.
- For riders: the operational-control findings documented here (R2-06, R2-09, R2-10, R2-11) are the kind of evidence a labour-law consultation or union representation (vida Gewerkschaft, AK Steiermark, both named recipients throughout) would need to evaluate an individual misclassification claim.

RFI-IRFOS's own view, stated plainly rather than left implicit: a company the size and sophistication of Delivery Hero SE does not lack the internal capability to answer a yes/no question about a religion-classification field within ninety days. The silence documented in this report is a choice, and the one reply that did arrive – redirecting a free disclosure into a bounty-payment refusal it was never asked to make – reads as a template response applied without anyone actually reading what was sent. We would rather be wrong about that and be corrected in writing than be right and watch it repeat on the next target. Either way, we will keep asking, in writing, on the public record, for as long as it takes to get an answer that engages with the actual finding.

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 All findings derive from static root-level analysis of the publicly distributed application binaries using publicly available tooling. No servers, accounts, or backend infrastructure were probed. The labour-classification analysis documents code-level and in-app-text evidence only; RFI-IRFOS makes no legal determination of employment status, which remains a matter for the competent Austrian authorities. Technical evidence is archived under chain of custody and available to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF com.foodora.* CONSUMER / RIDER / PARTNER.