



Security & Privacy Disclosure, Final Report

wo gibr's was Android (com.undabot.android.wgw)

A deals-finder app declares continuous background location together with a boot-start receiver, wires Facebook Codeless Event Logging into its screens so that browsing and tapping behavior can flow to Meta, starts AdMob and Firebase before any consent dialog, and ships three Firebase API keys in the production build, with ten messages over 67 days answered by zero replies and one permanent bounce

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 19 SEPTEMBER 2026. TEN MESSAGES SENT, NO REPLY OF ANY KIND

Target	wogibtswas.at GmbH, Weyrgasse 9 TOP 11, 1030 Wien (subsidiary of Offerista Group)
Package	com.undabot.android.wgw, version 64 (versionCode 4035088)
Developer of record	Undabot d.o.o., Zagreb, Croatia (build partner)
Platform Audited	Android, static analysis of the production APK (30.3 MB, pulled 2026-06-25)
Initial Disclosure (R1)	2026-06-25 (REF #WGW-001)
Disclosure / Embargo Date	2026-09-19
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	6 (2 Critical, 2 High, 2 Medium)
Correspondence	10 messages sent by RFI-IRFOS between 2026-06-25 and 2026-08-31 to team@wogibtswas.at, datenschutz@wogibtswas.at, datenschutz@offerista.com and support@wogibtswas.at. 0 replies of any kind. 1 permanent bounce (support@wogibtswas.at, 2026-06-25)
Authorities	Austrian Datenschutzbehörde (DSB), blind copy on the first messages, copy from 2026-07-03

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	5
4.1	C1: ACCESS_BACKGROUND_LOCATION with a boot-start receiver in a shopping deals app	6
4.2	C2: Facebook Codeless Event Logging classes embedded in a shopping app .	6
4.3	H1: AdMob and Firebase start through ContentProviders before any consent dialog	7
4.4	H2: Three Firebase API keys hardcoded in the production binary	7
4.5	H3: allowBackup enabled in the application manifest	8
4.6	M1: AppsFlyer and Android AdServices custom-audience permissions in a deals app	8
5	What the Operator Gets Right	9
6	Impact Analysis	9
7	The Complete Chain: From Install to Ten Unanswered Messages	9
8	Data Protection: Article by Article	10
9	Regulatory & Legal Landscape	10
10	Indicators of Compromise	11
11	Disclosure Timeline & Outcome	11
12	Residual Risk & Recommendations	12

Executive Summary

wogibtswas.at is an Austrian shopping deals and flyer app operated by wogibtswas.at GmbH, a subsidiary of the Offerista Group. A root level static analysis of the production Android binary (com.undabot.android.wgw, version 64) found six findings: two CRITICAL, two HIGH and two MEDIUM.

The app declares `ACCESS_BACKGROUND_LOCATION` together with `RECEIVE_BOOT_COMPLETED`. For an app whose stated purpose is finding offers nearby, this combination allows location collection while the app is closed and from every device start (C1). The Facebook SDK's Codeless Event Logging classes, including `AutoLoggingOnClickListener`, are present, so which offers a person taps and which stores they look at can be reported to Meta without a line of per-event code in the app. Which events are active is configured on Meta's servers and is not visible in the binary (C2). AdMob and Firebase start through ContentProviders at initOrder 100 before any activity or consent dialog, and Firebase is direct-boot aware (H1). Three separate Firebase API keys sit in the production binary (H2). `allowBackup` is enabled (H3). AppsFlyer and the Android AdServices custom-audience permission are declared (M1).

RFI-IRFOS disclosed these findings on 25 June 2026 and stated a coordinated disclosure date of 19 September 2026. Across ten messages in total, to every operator and parent-company privacy address RFI-IRFOS could identify, not one reply of any kind was received, no automated acknowledgment and no human answer. The only inbound message in the record is the permanent delivery failure for support@wogibtswas.at.

ID	Severity	Title
C1	CRITICAL	<code>ACCESS_BACKGROUND_LOCATION</code> with a boot-start receiver in a shopping deals app
C2	CRITICAL	Facebook Codeless Event Logging classes embedded in a shopping app
H1	HIGH	AdMob and Firebase start through ContentProviders before any consent dialog
H2	HIGH	Three Firebase API keys hardcoded in the production binary
H3	MEDIUM	<code>allowBackup</code> enabled in the application manifest
M1	MEDIUM	AppsFlyer and Android AdServices custom-audience permissions in a deals app

Subject & Operator Context

The brand owner is wogibtswas.at GmbH, Weyrgasse 9 TOP 11, 1030 Wien, a subsidiary of the Offerista Group. The Android build was produced with Undabot d.o.o. of Zagreb, Croatia. The app's privacy policy is hosted in an Offerista Amazon S3 bucket (public-legal-docs.offerista) and not on a wogibtswas.at domain, which is relevant for the controller question: the operator is Austrian, so the Austrian Datenschutzbehörde is the competent supervisory authority and no third-country adequacy question arises for the operator itself. Published contact points are team@wogibtswas.at and support@wogibtswas.at. The Offerista group privacy contact is datenschutz@offerista.com.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 25 June 2026 at 14:01 UTC to support@wogibtswas.at and team@wogibtswas.at under REF #WGW-001, with the Austrian Datenschutzbehörde and CERT.at in blind copy. The message to support@wogibtswas.at failed permanently within seconds (SMTP 5.1.3, the account does not exist). The message to team@wogibtswas.at was delivered without a delivery failure. The disclosure stated a coordinated disclosure date of 19 September 2026.

RFI-IRFOS followed up on 27 June, 3 July, 7 July, 17 July, 27 July, 4 August, 15 August and 31 August 2026 to team@wogibtswas.at, and on 28 June 2026 in a separate message to datenschutz@wogibtswas.at and datenschutz@offerista.com. That is ten messages in total. Each restated the findings and the same three direct questions. From 3 July the Austrian Datenschutzbehörde was in copy instead of blind copy. No message produced a reply, an automated acknowledgment or a delivery failure other than the one for support@wogibtswas.at.

Findings

C1: ACCESS_BACKGROUND_LOCATION with a boot-start receiver in a shopping deals app

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2: continuous background location capability and boot-start in an app whose purpose is finding nearby offers

android.permission.ACCESS_BACKGROUND_LOCATION	continuous background GPS
android.permission.ACCESS_FINE_LOCATION	GPS precision
android.permission.ACCESS_COARSE_LOCATION	network location
android.permission.RECEIVE_BOOT_COMPLETED	starts after every device boot

Observed fact: the permissions are declared in the shipped manifest. Legal inference: a stated purpose of finding nearby offers does not by itself justify a permanent background movement log under Art. 5(1)(b) and Art. 5(1)(c). RFI-IRFOS did not observe live transmission of location data to a remote endpoint, the finding concerns the declared capability and the purpose-limitation question it raises.

Impact: The manifest declares ACCESS_BACKGROUND_LOCATION, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION and RECEIVE_BOOT_COMPLETED. Together they allow the app to collect precise location while it is closed and to restart collection after every device boot. For an app whose purpose is showing offers near the user, background access builds a movement profile: where a person commutes, which retailers they visit, when they are near a competitor. Looking up nearby offers while the app is open does not require any of it. RFI-IRFOS blast-radius escalation: raised from HIGH/8.2 to CRITICAL because the combination yields a continuous movement profile of every installed user of a mass-market consumer app, a continuity and volume of location data that the CVSS technical scope does not capture.

C2: Facebook Codeless Event Logging classes embedded in a shopping app

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2: UI interaction logging toward Meta can run without per-event developer code

```
com.facebook.appevents.codeless.CodelessLoggingEventListener
com.facebook.appevents.codeless.CodelessLoggingEventListener.
    AutoLoggingOnClickListener
com.facebook.appevents.codeless.internal.EventBinding
com.facebook.appevents.suggestedevents.ViewOnClickListener$Companion
com.facebook.appevents.iap.InAppPurchaseBillingClientWrapper
com.facebook.appevents.cloudbridge.AppEventsConversionsAPITransformer
```

Limit of the evidence: the active event configuration lives on Meta's servers and is not part of the binary. This report therefore documents the capability and the data categories it can carry. It does not claim a measured volume of events.

Impact: The binary contains the Facebook SDK's codeless logging classes, including AutoLoggingOnClickListener and ViewOnClickListener. These attach to UI elements and report interactions to Meta according to a configuration held on Meta's servers. In a deals app

that means which offers a person taps, which products they view, which retailers and price categories they look at can reach Meta's advertising infrastructure, a US recipient, with no disclosed reason in the app's own information. RFI-IRFOS blast-radius escalation: raised from HIGH/8.2 to CRITICAL because the data concerned is the shopping behavior of Austrian consumers and the recipient is a US advertising platform, a consequence the CVSS technical scope does not capture.

H1: AdMob and Firebase start through ContentProviders before any consent dialog

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3: advertising and analytics SDKs initialize at process creation, ahead of any consent decision

```
com.undabot.android.wgw.mobileadsinitprovider    initOrder=100
com.google.firebase.provider.FirebaseInitProvider  initOrder=100, directBootAware=
true
```

Impact: Two ContentProviders with initOrder 100 run at process creation, before any activity exists and before any consent dialog can be shown: the app's own mobileadsinitprovider (AdMob) and Firebase's FirebaseInitProvider, which is also directBootAware and can therefore run before the device is unlocked. Consent must precede processing under Art. 7, and an SDK that initializes first has already begun. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the pre-consent initialization sits in the same app that declares background location, so the consent gap covers the most sensitive data category in the build.

H2: Three Firebase API keys hardcoded in the production binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9: three separate Firebase projects referenced from one release build

```
Firestore key 1: AIzaSyArX2 [truncated]
Firestore key 2: AIzaSyCpY6 [truncated]
Firestore key 3: AIzaSyDRKQ [truncated]
```

Impact: Three distinct Google/Firebase API keys are present in the shipped build. Several keys point to several Firebase projects, possibly including development or staging environments carried into the release. Each key is a quota and billing exhaustion vector against the operator's own Firebase services, and a key shipped in a released binary cannot be rotated for existing installs without an app update. A key is not a secret in the Firebase model, but the burden to show that restrictions and App Check are in place lies with the controller under Art. 5(2). RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because keys in a released binary stay exposed for every existing install and cannot be withdrawn by the operator.

H3: allowBackup enabled in the application manifest

MEDIUM, 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, 5.1: app data eligible for device and cloud backup without exclusion rules

```
android:allowBackup="true"
```

Impact: android:allowBackup is true. Saved deals, shopping history, location-linked offer preferences and store favorites are eligible for backup without exclusion rules. Backup extraction requires local access to the device or the user's own cloud account, which lowers the technical severity. Severity correction: the first disclosure message listed this finding as HIGH. Scoring it with CVSS v4.0 gives 5.1, MEDIUM, and this report carries the lower, computed rating.

M1: AppsFlyer and Android AdServices custom-audience permissions in a deals app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3: attribution and cross-app audience building capability declared

```
AppsFlyer SDK (appsflyer_backup_rules.xml present)
ACCESS_ADSERVICES_AD_ID
ACCESS_ADSERVICES_ATTRIBUTION
ACCESS_ADSERVICES_CUSTOM_AUDIENCE
com.google.android.gms.permission.AD_ID
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA
```

Impact: The build includes the AppsFlyer SDK and declares ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_CUSTOM_AUDIENCE and com.google.android.gms.permission.AD_ID, and a Huawei HMS common-data permission. ACCESS_ADSERVICES_CUSTOM_AUDIENCE supports building behavioral cohorts for cross-app advertising. Shopping behavior is commercially valuable profiling data and the purpose is not explained in the app's information.

What the Operator Gets Right

A `networkSecurityConfig` is present. The operator is an Austrian company, which gives the Austrian Datenschutzbehörde direct jurisdiction and removes any adequacy question for the operator itself. The app delivers a real consumer benefit through price and offer comparison. The analysis found no biometric SDK, no microphone and no camera permission. The 30 MB package is focused, and every finding above can be addressed without an architectural rebuild.

Impact Analysis

Everyone who installed the app is affected, and the effect compounds across the findings. C1 gives the app the technical ability to know where a person is when they are not using it. C2 gives Meta a route to learn what they look at inside the app. H1 means SDKs start before the person has been asked. M1 adds an audience-building layer on top. Individually each is a gap. Together they describe a deals app that can turn daily movement and shopping behavior into advertising signals, for people who installed it to save money.

The bystander effect is limited here, because the data concerns the account holder's own device. The relevant human impact is the profile: commute, shopping routes, retailer preferences and price sensitivity, assembled without the person having chosen it.

The Complete Chain: From Install to Ten Unanswered Messages

Step 1, install: a person installs `wogibts was` to find offers. The manifest asks for location, including background location, and registers a boot receiver.

Step 2, process start: before any activity or consent dialog exists, `AdMob` and `Firebase` initialize through `ContentProviders` at `initOrder 100`. `Firebase` is direct-boot aware.

Step 3, interaction: the embedded Facebook codeless classes attach to the app's screens, so that taps and views can be reported to Meta under a server-side configuration.

Step 4, profile: background location and the attribution and audience permissions supply the movement and shopping dimensions of a profile.

Step 5, disclosure: on 25 June 2026 RFI-IRFOS reports all of this to the operator and states 19 September 2026 as the disclosure date. The address `support@wogibtswas.at` does not exist. `team@wogibtswas.at` receives the message.

Step 6 to 14, follow-ups: eight further messages follow between 27 June and 31 August 2026, one of them to the data protection addresses of the operator and the parent company. No reply of any kind arrives.

Step 15, embargo: the stated date passes on 19 September 2026 without any response.

Step 16, publication: this report publishes on 17 October 2026, 28 days after the embargo date.

Data Protection: Article by Article

Art. 5(1)(b) and Art. 5(1)(c) GDPR, purpose limitation and data minimisation: C1's background location and boot-start capability go beyond the purpose of showing nearby offers.

Art. 6(1) GDPR, lawfulness: no legal basis for continuous background location or for Meta-bound interaction logging is disclosed in the app.

Art. 7 GDPR, conditions for consent: H1's AdMob and Firebase initialization precedes any consent decision.

Art. 13(1)(c) and Art. 13(1)(e) GDPR, transparency: the purposes and the recipient category (Meta) are not explained to the user at the point of collection.

Art. 25 GDPR, data protection by design and by default: pre-consent SDK start and default-on backup are the opposite of protective defaults.

Art. 32(1)(b) GDPR, security of processing: H2's three hardcoded keys and H3's backup eligibility.

Art. 44 GDPR, third-country transfers: C2's Meta recipient is a US company, and no transfer mechanism is documented in the app.

Regulatory & Legal Landscape

The operator is an Austrian company, so the competent authority is the Austrian Datenschutzbehörde. It was in blind copy on the first messages and in open copy from 3 July 2026. The CERT.at team was in blind copy on the first two messages.

Fine exposure under GDPR: Art. 83(5) applies to the principles and consent issues in C1, C2 and H1, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 25 and Art. 32 issues in H1 to H3, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Ten written messages without any reply, including one addressed to the group privacy mailbox, is a fact a regulator can weigh alongside the technical findings.

The research was conducted under ISO/IEC 29147 and the freedom of scientific research (Art. 17 StGG).

Indicators of Compromise

The identifiers below were extracted from the production APK by static analysis only. No server, account or infrastructure of wogibtswas.at GmbH, Offerista, Meta, AppsFlyer or Google was probed.

```
Package:      com.undabot.android.wgw
Version:      64 (versionCode 4035088)
APK:          wgw_base.apk, 30.3 MB, pulled 2026-06-25
Permissions:  ACCESS_BACKGROUND_LOCATION, ACCESS_FINE_LOCATION,
               ACCESS_COARSE_LOCATION,
               RECEIVE_BOOT_COMPLETED, ACCESS_AD SERVICES_AD_ID,
               ACCESS_AD SERVICES_ATTRIBUTION,
               ACCESS_AD SERVICES_CUSTOM_AUDIENCE, com.google.android.gms.permission.
               AD_ID
Providers:    com.undabot.android.wgw.mobileadsinitprovider (initOrder=100)
               com.google.firebase.provider.FirebaseInitProvider (initOrder=100,
               directBootAware)
Facebook SDK: com.facebook.appevents.codeless.*, com.facebook.appevents.
               suggestedevents.*
Keys:         3 Firebase API keys, values truncated in this report
Backup:       android:allowBackup=true
```

Disclosure Timeline & Outcome

2026-06-25 Initial disclosure to support@wogibtswas.at and team@wogibtswas.at, REF #WGW-001. Austrian DSB and CERT.at in blind copy. Disclosure date stated as 2026-09-19. support@wogibtswas.at fails permanently (5.1.3, account does not exist).

2026-06-27 First follow-up to team@wogibtswas.at. No reply.

2026-06-28 Separate follow-up to datenschutz@wogibtswas.at and datenschutz@offerista.com. No reply, no delivery failure.

2026-07-03, 2026-07-07, 2026-07-17, 2026-07-27, 2026-08-04, 2026-08-15 Six further follow-ups to team@wogibtswas.at, Austrian DSB in copy. No reply.

2026-08-31 Eighth follow-up to team@wogibtswas.at, 67 days after the first message. No reply.

2026-09-19 Disclosure date reached, as stated on 2026-06-25 and never revised.

2026-10-17 This report published. Correspondence record: ten RFI-IRFOS messages, zero replies of any kind, one permanent bounce.

Residual Risk & Recommendations

C1: remove ACCESS_BACKGROUND_LOCATION and RECEIVE_BOOT_COMPLETED unless a documented feature requires them, and if one does, document its purpose and legal basis and request the permission only at the point of use.

C2: disable Codeless Event Logging, or gate the Facebook SDK behind an explicit consent decision, and document the Art. 44 transfer mechanism for any Meta-bound event.

H1: initialize AdMob and Firebase Analytics only after the consent decision, not through ContentProviders at process creation.

H2: restrict each Firebase key by package name and certificate, enforce App Check, remove non-production projects from the release build, and rotate the keys.

H3: set allowBackup to false, or define backup exclusion rules for saved deals, history and location-linked preferences.

M1: document the purpose and legal basis for AppsFlyer and the AdServices custom-audience permission, or remove them.

Across all findings: establish a monitored intake path for disclosures. support@wogibtswas.at does not exist, and ten messages to the remaining published addresses produced no answer.

RFI-IRFOS security@rfi-irfos.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 analysis of the published application using publicly available tooling. No wogibtswas.at, Offerista, Meta, AppsFlyer or Google servers, accounts or 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 WGW-001.