



---

# Security & Privacy Disclosure, Final Report

idealo (de.idealo.android), APK as analyzed 2026-06-30, 52.2 MB, 40,814 smali classes

A hardcoded Firebase key and exposed production database sit alongside Interest-Group ad-profiling built from price-comparison search queries, a pre-consent tracking auto-init, and an unprotected exported broadcast receiver, met with a blanket dismissal naming zero findings individually and then 106 days of silence, 19 days past an unmoved embargo

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28 SEPTEMBER 2026, ALL FOUR FINDINGS REMAIN UNADDRESSED**

---

|                                  |                                                                                                                                                                                                                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                    | idealo internet GmbH, Berlin, Germany (100% subsidiary of Axel Springer SE)                                                                                                                                                                                                                  |
| <b>Package</b>                   | de.ideal.android                                                                                                                                                                                                                                                                             |
| <b>Version Audited</b>           | Production APK, Google Play, analyzed 2026-06-30 (52.2 MB, 40,814 smali classes)                                                                                                                                                                                                             |
| <b>Platform</b>                  | Android, static analysis                                                                                                                                                                                                                                                                     |
| <b>Initial Disclosure (R1)</b>   | 2026-06-30 (REF DE.IDEALO.ANDROID)                                                                                                                                                                                                                                                           |
| <b>Disclosure / Embargo Date</b> | 2026-09-28                                                                                                                                                                                                                                                                                   |
| <b>Report Published</b>          | 2026-10-17                                                                                                                                                                                                                                                                                   |
| <b>Overall Severity</b>          | CRITICAL                                                                                                                                                                                                                                                                                     |
| <b>Findings</b>                  | 4 (1 Critical, 3 High)                                                                                                                                                                                                                                                                       |
| <b>Correspondence</b>            | 6 messages sent by RFI-IRFOS over 109 days (30 June through 31 August 2026) to security@ideal.de and datenschutz@ideal.o.de, 1 reply received on 2026-07-03 (blanket dismissal naming zero findings individually), 0 substantive reply ever received, 0 reply of any kind for 106 days since |
| <b>Authorities CC'd / BCC'd</b>  | Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Berlin — lead supervisory authority for idealo internet GmbH; CERT.at and the Austrian Datenschutzbehörde (DSB) copied from the research institute's own jurisdiction                                                |

---

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

## Contents

---

|           |                                                                                                                                    |           |
|-----------|------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Executive Summary</b>                                                                                                           | <b>4</b>  |
| <b>2</b>  | <b>Subject &amp; Operator Context</b>                                                                                              | <b>5</b>  |
| <b>3</b>  | <b>Engagement Summary</b>                                                                                                          | <b>5</b>  |
| <b>4</b>  | <b>Findings</b>                                                                                                                    | <b>6</b>  |
| 4.1       | C1: Firebase API key and production database URL hardcoded in the distributed binary . . . . .                                     | 6         |
| 4.2       | H1: ACCESS_ADSERVICES_CUSTOM_AUDIENCE: persistent Interest-Group ad-profiling built from price-comparison search queries . . . . . | 7         |
| 4.3       | H2: Firebase and Adjust pre-consent ContentProvider auto-init, Firebase BOOT_COMPLETED receiver . . . . .                          | 8         |
| 4.4       | H3: SendIntentBroadcastReceiver exported=true: idealo's own tracking receiver reachable by any app on the device . . . . .         | 9         |
| <b>5</b>  | <b>Impact Analysis</b>                                                                                                             | <b>9</b>  |
| <b>6</b>  | <b>The Complete Chain: Six Messages, One Non-Answer, 106 Days of Silence</b>                                                       | <b>10</b> |
| <b>7</b>  | <b>Disclosure Timeline &amp; Outcome</b>                                                                                           | <b>10</b> |
| <b>8</b>  | <b>Data Protection — Article by Article</b>                                                                                        | <b>11</b> |
| <b>9</b>  | <b>Regulatory Landscape &amp; Fine Exposure</b>                                                                                    | <b>11</b> |
| <b>10</b> | <b>Indicators of Compromise</b>                                                                                                    | <b>12</b> |
| <b>11</b> | <b>Residual Risk &amp; Recommendations</b>                                                                                         | <b>12</b> |

## Executive Summary

---

idealo internet GmbH operates idealo, Germany's largest price-comparison platform with approximately 50 million monthly users, as a 100% subsidiary of Axel Springer SE. A static analysis of the production Android APK (de.ideal.android), performed 2026-06-30, identified four findings, one CRITICAL and three HIGH, spanning credential hardcoding, behavioral ad-profiling built from shopping search queries, pre-consent tracking initialization, and an unprotected exported component.

A Google/Firebase API key and the production Firebase Realtime Database URL are hard-coded in res/values/strings.xml (C1), present verbatim in every installed copy of the app and extractable in under a minute with free tooling, creating a quota-exhaustion and, if database security rules are misconfigured, direct-data-access surface. idealo declares the android.permission.ACCESS\_AD\_SERVICES\_CUSTOM\_AUDIENCE permission (H1), Google's Privacy Sandbox Protected Audiences API, which builds persistent cross-app advertising Interest-Groups directly from price-comparison search queries, product category, model, and price range. Combined with Braze (behavioral CRM) and the Facebook SDK bundled in the same binary, a search for a specific television model or washing machine on idealo does not stay a price comparison, it becomes a standing advertising profile that follows the user across other apps. Firebase Performance and the Adjust attribution SDK both initialize via ContentProvider before any consent screen is shown, and Firebase's AppMeasurementReceiver is registered for BOOT\_COMPLETED, starting before the app is ever opened (H2). idealo's own tracking receiver, de.ideal.android.tracking.SendIntentBroadcastReceiver, is declared android:exported="true" with no permission attribute, meaning any other application installed on the same device can send it intents, triggering or injecting into idealo's own analytics pipeline from outside the app entirely (H3).

RFI-IRFOS disclosed these four findings to security@ideal.de and datenschutz@ideal.de on 2026-06-30. On 2026-07-03, security@ideal.de replied that some of the issues had previously been reported by another researcher and others did not constitute valid security or privacy vulnerabilities, closing the submission, without naming a single one of the four findings individually, and addressing only the Firebase key with a generic 'public by design, controlled through Firebase Security Rules' line that does not engage with the exposed production database URL at all. RFI-IRFOS rejected the blanket dismissal the same day and asked for a finding-by-finding response. Four further follow-ups (2026-07-17, 2026-07-27, 2026-08-09, 2026-08-31) repeated the same request. idealo has not replied again since 2026-07-03, a silence of 106 days as of publication, through an embargo deadline fixed at 2026-09-28 at the time of the original disclosure and never moved since. This report publishes 19 days past that embargo, with all four findings unaddressed by name.

| ID | Severity        | Title                                                                                                                 |
|----|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| C1 | <b>CRITICAL</b> | Firebase API key and production database URL hard-coded in the distributed binary                                     |
| H1 | <b>HIGH</b>     | ACCESS_AD_SERVICES_CUSTOM_AUDIENCE: persistent Interest-Group ad-profiling built from price-comparison search queries |
| H2 | <b>HIGH</b>     | Firebase and Adjust pre-consent ContentProvider auto-init, Firebase BOOT_COMPLETED receiver                           |

| ID | Severity    | Title                                                                                                        |
|----|-------------|--------------------------------------------------------------------------------------------------------------|
| H3 | <b>HIGH</b> | SendIntentBroadcastReceiver exported=true: idealo's own tracking receiver reachable by any app on the device |

## Subject & Operator Context

idealo internet GmbH, headquartered in Berlin, operates idealo.de, Germany's largest price-comparison platform by monthly active users (approximately 50 million). The company has been a 100% subsidiary of Axel Springer SE since 2019. This audit covers the Android application (de.idealoo.android) available on Google Play. A platform whose core function is helping users compare prices before a purchase sits in an unusually sensitive position for behavioral advertising: every search query is a direct signal of purchase intent, product category, and often an implicit budget range, well beyond what a generic browsing-history profile would reveal.

## Engagement Summary

RFI-IRFOS sent the initial disclosure on 2026-06-30 to security@idealo.de and datenschutztz@idealo.de, with presse@idealo.de CC'd and CERT.at, the Austrian Datenschutzbehörde (DSB), and the Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) copied as the lead supervisory authority for idealo's Berlin headquarters.

On 2026-07-03, security@idealo.de replied with a blanket dismissal: some issues previously reported by another researcher, others not valid security or privacy vulnerabilities, submission closed, with zero findings named individually and only a generic one-line response to the Firebase key ('public by design, controlled through Firebase Security Rules') that did not address the exposed production database URL. The same reply explicitly declined any commercial engagement or paid collaboration. RFI-IRFOS rejected the dismissal the same day, asking for a finding-by-finding response: confirmed, already reported with a date, or invalid with a reason, for each of the four findings individually.

Four further follow-ups were sent: 2026-07-17 (14 days since the dismissal), 2026-07-27 (10 days since the previous message), 2026-08-09 (13 days since the previous message, noting the pattern of 'disagreement without specifics'), and 2026-08-31 (22 days since the previous message, restating the full chronology and the Art. 33 GDPR weekly-diff and silent-ticket-closure clauses that apply to every target in this campaign). idealo has not replied again since 2026-07-03. The embargo deadline, fixed at 2026-09-28 in the original disclosure, was reached and passed with zero of the four findings confirmed, dated, or reasoned away individually.

## Findings

### C1: Firebase API key and production database URL hardcoded in the distributed binary

**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, 7.5 — unrestricted key enables quota exhaustion and a conditional database-read path**

```
google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to idealo in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to idealo in R1]
```

Both values are present verbatim in every installed copy of de.idealoidroid. idealoid's 2026-07-03 reply addressed the key ('public by design, controlled through Firebase Security Rules') but did not address the production database URL hardcoded alongside it.

**Impact:** A Google/Firebase API key and the production Firebase Realtime Database URL are hardcoded in res/values/strings.xml [REDACTED IN PUBLIC REPORT – disclosed privately to idealoid in R1], present verbatim in every installed copy of de.idealoidroid and extractable with free, widely available tooling in under a minute. idealoid's own 2026-07-03 reply addressed this finding with a single generic line, that Firebase API keys are public by design and access is controlled through Firebase Security Rules, not key secrecy. That statement is true as far as it goes and does not answer the finding: a key that is safe to ship does not make a quota-exhaustion attack against the shared project impossible, nor does it address the second, separate fact this finding reported, that the production database URL itself is hardcoded alongside the key, which is a configuration question entirely independent of whether the key is secret. idealoid's reply engaged with the half of C1 that was easiest to wave away and left the database-URL half unanswered. RFI-IRFOS blast-radius escalation: raised from HIGH/7.5 to CRITICAL because idealoid serves approximately 50 million monthly users as Germany's largest price-comparison platform, and this finding does not stand alone, it sits directly alongside H1's Interest-Group ad-profiling, H2's pre-consent tracking initialization, and H3's unprotected exported tracking receiver, forming one compounding stack rather than four independent issues.

**H1: ACCESS\_ADSERVICES\_CUSTOM\_AUDIENCE: persistent Interest-Group ad-profiling built from price-comparison search queries**

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N, 7.1 — shopping search queries, including price range and product model, converted into persistent cross-app advertising profiles**

```
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE"/>
```

Companion SDKs bundled in the same binary:

Braze – behavioral marketing CRM (push, in-app messaging, user profiling)

Facebook SDK – facebook\_app\_id + facebook\_client\_token hardcoded

idealo's 2026-07-03 reply: finding not named, not confirmed, not disputed.

**Impact:** de.ideal.android declares android.permission.ACCESS\_ADSERVICES\_CUSTOM\_AUDIENCE, Google's Android Privacy Sandbox Protected Audiences API, the designated successor to third-party cookies for cross-app ad-targeting. On a price-comparison platform, this permission's purpose is to place users into persistent Interest-Groups built directly from their search queries, product category, model, and implied price range, which are then used for cross-app ad-retargeting outside idealo entirely. idealo's reply of 2026-07-03 did not name this finding, confirm it, dispute it, or cite any legal basis for it. Combined with Braze (a behavioral marketing CRM handling push notifications, in-app messaging, and user profiling) and the Facebook SDK (facebook\_app\_id and facebook\_client\_token both hardcoded in the binary), idealo ships a complete behavioral-ad-profiling stack layered directly on top of shopping-intent data, a category of signal considerably more specific and commercially valuable than generic browsing history, since a price-comparison search inherently discloses purchase intent, product category, and an implicit budget range in one query.

## H2: Firebase and Adjust pre-consent ContentProvider auto-init, Firebase BOOT\_COMPLETED receiver

**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, 7.2 — tracking infrastructure initializes before any consent screen is shown, and before the app is ever opened**

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
  android:initOrder="100" android:directBootAware="true"/>
<provider android:name="com.adjust.sdk.SystemLifecycleContentProvider"
  android:authorities="de.idealos.android.adjust-lifecycle-provider"/>
<receiver android:name="com.google.android.gms.measurement.AppMeasurementReceiver">
  <action android:name="android.intent.action.BOOT_COMPLETED"/>
</receiver>
```

idealos's 2026-07-03 reply: finding not named, not confirmed, not disputed.

**Impact:** AndroidManifest.xml declares com.google.firebase.provider.FirebaseInitProvider with initOrder="100" and android:directBootAware="true", alongside com.adjust.sdk.SystemLifecycleContentProvider (declared authority de.idealos.android.adjust-lifecycle-provider). Android ContentProvider components initialize before any Activity, and therefore before any consent dialog can be shown to the user; directBootAware additionally means initialization can occur before the device is even unlocked. com.google.android.gms.measurement.AppMeasurementReceiver is separately registered for the BOOT\_COMPLETED broadcast, meaning Firebase measurement infrastructure starts at device boot, before the user has opened the app for the first time at all. idealos's 2026-07-03 reply did not name or address this finding.

### H3: `SendIntentBroadcastReceiver` `exported=true`: idealo's own tracking receiver reachable by any app on the device

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 7.0 — unprotected exported component allows any installed app to trigger or inject into idealo's own analytics pipeline**

```
<receiver android:exported="true"
    android:name="de.ideal.android.tracking.SendIntentBroadcastReceiver"/>
```

No `android:permission` attribute -- no protection against intents sent by any other application installed on the same device.

ideal's 2026-07-03 reply: finding not named, not confirmed, not disputed.

**Impact:** `de.ideal.android.tracking.SendIntentBroadcastReceiver` is declared `android:exported="true"` with no `android:permission` attribute, meaning any other application installed on the same Android device can send intents to this receiver directly, with no authorization check of any kind. This is functionally equivalent to an unauthenticated internal API endpoint exposed to idealo's entire device-level app ecosystem: another app on the device can trigger idealo's own tracking logic on demand, or inject fabricated events into idealo's analytics pipeline from outside idealo entirely. ideal's 2026-07-03 reply did not name or address this finding.

### Impact Analysis

These four findings are not four independent issues, they are one stack. C1's hardcoded credentials and exposed production database are the infrastructure-level gap. H2's pre-consent auto-init means Firebase and Adjust are already running, before the user has seen a consent screen, by the time H1's Custom Audience profiling and Braze/Facebook CRM integration begin converting price-comparison search queries into persistent, cross-app advertising profiles. H3's unprotected exported receiver means that entire pipeline, idealo's own tracking logic, is reachable and triggerable by any other application on the user's device, without authorization. On a platform whose core function is comparing prices before a purchase, this combination converts routine shopping research, which television, which washing machine, at what price point, into a standing, externally-triggerable, pre-consent advertising profile shared across Google's and Meta's ad ecosystems. idealo's single reply addressed none of this as a stack and did not engage with H1, H2, or H3 at all.

## The Complete Chain: Six Messages, One Non-Answer, 106 Days of Silence

---

2026-06-30: RFI-IRFOS sends the full disclosure to security@idealo.de and datenschutz@idealo.de, presse@idealo.de CC'd, CERT.at, the Austrian DSB, and the Berlin data protection authority (BlnBDI) copied. Embargo deadline established: 2026-09-28.

2026-07-03: security@idealo.de replies. Some issues previously reported by another researcher, others not valid security or privacy vulnerabilities, submission closed. Zero findings named individually. Only the Firebase key receives a generic response ('public by design, controlled through Firebase Security Rules'), which does not address the production database URL. Commercial engagement explicitly declined.

2026-07-03, same day: RFI-IRFOS rejects the blanket dismissal, requests a finding-by-finding response: confirmed, already reported with a date, or invalid with a reason, for each of the four findings.

2026-07-17: First follow-up. Request repeated, the pattern named as 'disagreement without specifics.'

2026-07-27: Second follow-up. Request repeated.

2026-08-09: Third follow-up. Request repeated, 37 days since the blanket dismissal noted explicitly.

2026-08-31: Fourth follow-up. Full chronology restated, 59 days since the blanket dismissal, the weekly APK-diff and silent-fix clauses under Art. 33 GDPR restated as standard procedure for this entire campaign.

idealo has not replied again since 2026-07-03. As of this report's publication (2026-10-17), that is 106 days of silence following the only reply this disclosure ever received, and 19 days past the 2026-09-28 embargo deadline fixed at the original disclosure and never moved since.

### Disclosure Timeline & Outcome

---

2026-06-30 Initial disclosure sent, four findings, embargo fixed at 2026-09-28.

2026-07-03 idealo replies: blanket dismissal, zero findings named individually.

2026-07-03 RFI-IRFOS rejects the dismissal, requests finding-by-finding response.

2026-07-17 First follow-up, request repeated.

2026-07-27 Second follow-up, request repeated.

2026-08-09 Third follow-up, request repeated.

2026-08-31 Fourth and final follow-up, full chronology restated.

2026-09-28 Embargo date reached. No further reply received since 2026-07-03.

2026-10-17 This report published, 19 days after embargo. All four findings unaddressed by name.

## Data Protection — Article by Article

---

Art. 32(1)(b) GDPR — Integrity and confidentiality of processing: C1's hardcoded credentials and exposed production database URL, and H3's unprotected exported tracking receiver, both fall below the technical measures this article requires.

Art. 25 GDPR — Data protection by design and by default: C1's hardcoded, non-rotatable credentials in a publicly distributed binary are a design-stage failure, not a runtime incident.

Art. 7(1) GDPR — Conditions for consent: H2's pre-consent ContentProvider auto-initialization and BOOT\_COMPLETED receiver mean tracking infrastructure is active before any consent mechanism can be presented to the user.

Art. 5(1)(b) GDPR — Purpose limitation: H1's conversion of price-comparison search queries into persistent, cross-app advertising Interest-Groups is a secondary use of data collected for price comparison, not advertising.

Art. 6(1) GDPR — Lawfulness of processing: idealo's 2026-07-03 reply did not state a legal basis for H1's Custom Audience profiling, and none was named in any subsequent correspondence.

Art. 13 GDPR — Information to be provided: none of H1's Interest-Group profiling, H2's pre-consent initialization, or H3's exported receiver were confirmed, disputed, or otherwise addressed in idealo's one reply, leaving the transparency question for all three open.

## Regulatory Landscape & Fine Exposure

---

idealo internet GmbH is headquartered in Berlin, placing it under the jurisdiction of the Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), which has been copied on this disclosure throughout. As a 100% subsidiary of Axel Springer SE processing data from approximately 50 million monthly users, idealo is subject to the full GDPR Article 83 fine structure.

Art. 83(5) GDPR — Maximum fines up to EUR 20,000,000 or 4% of worldwide annual turnover — applies to violations of Art. 5 (principles, implicated by H1's purpose-limitation gap), Art. 6 (lawfulness, implicated by H1's undisclosed legal basis), Art. 7 (conditions for consent, implicated by H2's pre-consent initialization), and Art. 25 (data protection by design, implicated by C1).

Art. 83(4) GDPR — Maximum fines up to EUR 10,000,000 or 2% of worldwide annual turnover — applies to violations of Art. 32 (security of processing), implicated by both C1 and H3.

A blanket dismissal that names zero findings individually does not discharge idealo's accountability obligation under Art. 5(2) GDPR, under which the burden of demonstrating compliance rests with the controller, not with the researcher who reported the gap.

## Indicators of Compromise

---

All findings derive from static analysis of the de.ideal.android production APK as published on Google Play, analyzed 2026-06-30. No idealo servers, accounts, or infrastructure were probed.

## Residual Risk & Recommendations

---

C1 – Hardcoded Firebase credentials: Rotate the exposed API key and treat the production database URL as a configuration item requiring its own review, independent of key secrecy. Document the Firebase Security Rules currently protecting this database instance and confirm they deny anonymous read/write by default. Report the finding internally under Art. 33 GDPR if a notification duty applies.

H1 – Custom Audience Interest-Group profiling: Document the Art. 6(1) legal basis for converting price-comparison search queries into persistent advertising profiles, disclose this processing specifically (not generically under a 'Firebase' or 'advertising partners' label) in the privacy policy at the granularity Art. 13 requires, and offer a specific opt-out for Custom Audience participation independent of general analytics consent.

H2 – Pre-consent initialization: Gate FirebaseInitProvider, the Adjust SystemLifecycleContentProvider, and the AppMeasurementReceiver's BOOT\_COMPLETED registration behind the consent decision, using the standard Android manifest-merger technique (tools:node="remove" or a conditional consent-mode default) rather than initializing unconditionally at process start.

H3 – Exported tracking receiver: Remove android:exported="true" from SendIntentBroadcastReceiver, or add an android:permission attribute scoped to idealo's own signing key, so that only idealo's own components can trigger this receiver.

Process-level: A reply that closes a submission with zero findings named individually does not meet the standard this campaign treats as a response. idealo's security contact channel would benefit from a documented per-finding acknowledgment process, consistent with how CERT.at, the BlnBDI, and comparable disclosure-handling bodies expect coordinated vulnerability disclosures to be triaged.

---

**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

de.ideal.android, the production APK as published on Google Play, analyzed 2026-06-30, using publicly available tools (apktool, jadx, jq). No idealo servers, accounts, or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the BlnBDI on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF DE.IDEALO.ANDROID.