



Security & Privacy Disclosure, Final Report

IKEA Android App (com.ingka.ikea.app) v5.4.0

A hardcoded IndoorAtlas API Secret exposes the in-store positioning infrastructure behind IKEA's own KompassMap navigation system across every installed copy of the app, a production Firebase database URL and key sit alongside it, two Optimizely receivers and an Adjust content provider begin behavioural tracking at device boot before the app is ever opened, and a furniture shopping app fires a callback every time a customer screenshots it, unresolved through 92 days since the first confirmed delivery and a 19-day-overdue embargo, after the original disclosure itself bounced outright at all three addresses it was sent to

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

Target	Ingka Group / Inter IKEA Systems B.V.
Package	com.ingka.ikea.app
Version Audited	v5.4.0
Platform Audited	Android, static analysis of the production APK
Initial Disclosure Attempt	2026-06-30, to security@ingka.com and privacy@ingka.com, CC press@ingka.com — all three bounced (address not found)
First Confirmed Delivery (Resend)	2026-07-17, to dpo.ikea.se@ikea.com, CC privacidade@ikea.com, the Austrian DSB and the EDPS
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (2 Critical, 2 High)
Correspondence	6 messages sent by RFI-IRFOS (1 bounced routing attempt, 1 resend, 4 follow-ups), 1 automated routing acknowledgment received, 0 substantive replies ever received from Ingka Group or Inter IKEA Systems
Authorities CC'd	Austrian Datenschutzbehörde (DSB), European Data Protection Supervisor (EDPS), Swedish Authority for Privacy Protection (IMY), CERT.at

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: IndoorAtlas API Key and API Secret hardcoded, exposing the in-store positioning infrastructure behind IKEA's own KompassMap system	6
4.2	C2: Firebase API Key and production Realtime Database URL hardcoded alongside it	6
4.3	H1: Two Optimizely receivers and an Adjust content provider begin behavioural tracking at device boot, before the app is ever opened	7
4.4	H2: DETECT_SCREEN_CAPTURE on a furniture shopping app: IKEA is notified every time a customer screenshots the app	8
5	Impact Analysis	8
6	The Complete Chain: A Disclosure That Bounced at Every Address It Was Sent To	9
7	Data Protection – Article by Article	10
8	Regulatory & Legal Landscape	10
9	Indicators of Compromise	11
10	Disclosure Timeline & Outcome	11
11	Residual Risk & Recommendations	12

Executive Summary

Ingka Group operates the IKEA Android app (com.ingka.ikea.app) at a scale of more than 170 million IKEA Family members. A static analysis of the production binary (v5.4.0) found four findings, two CRITICAL and two HIGH.

The IndoorAtlas API Key and the accompanying 512-bit API Secret, both explicitly private credentials per IndoorAtlas's own documentation, are hardcoded in AndroidManifest.xml in every installed copy of the app. These credentials power KompassMap, IKEA's in-store navigation and department-level analytics system, and provide access to floor plans, magnetic field maps, and positioning session data across the company's store network (C1). A Google API key and a production Firebase Realtime Database URL are hardcoded alongside it; the database itself becomes reachable if its Security Rules are misconfigured, and quota or billing denial-of-service applies regardless of that configuration (C2). Separately, two Optimizely A/B-testing receivers registered on RECEIVE_BOOT_COMPLETED, together with an Adjust lifecycle content provider, begin collecting behavioural data at device boot, before the app is opened and before any consent screen can appear (H1). Finally, the app declares the DETECT_SCREEN_CAPTURE permission and fires a callback every time a customer screenshots the app, a permission designed for credential protection in financial apps or piracy prevention in DRM media, applied here to a furniture catalog with no disclosed lawful basis (H2).

RFI-IRFOS's original disclosure, sent 30 June 2026 to security@ingka.com and privacy@ingka.com, CC press@ingka.com, bounced outright at all three addresses the same day, address not found. RFI-IRFOS resent the full disclosure on 17 July 2026 to dpo.ikea.se@ikea.com, CC privacidade@ikea.com, the Austrian Datenschutzbehoerde and the European Data Protection Supervisor, which is the first confirmed delivery in this case. A single automated routing acknowledgment arrived from privacidade@ikea.com confirming receipt into IKEA's data-subject-request queue. Four further follow-ups were sent on 15 August, 24 August, 3 September, and 12 September 2026, each restating the open findings and the days elapsed, with the embargo date, stated as 28 September 2026 from the first message onward, confirmed unchanged in every subsequent message. Across 92 days since the first confirmed delivery and six messages in total, not one substantive reply was ever received from Ingka Group or Inter IKEA Systems.

ID	Severity	Title
C1	CRITICAL	IndoorAtlas API Key and API Secret hardcoded, exposing the in-store positioning infrastructure behind IKEA's own KompassMap system
C2	CRITICAL	Firebase API Key and production Realtime Database URL hardcoded alongside it
H1	HIGH	Two Optimizely receivers and an Adjust content provider begin behavioural tracking at device boot, before the app is ever opened
H2	HIGH	DETECT_SCREEN_CAPTURE on a furniture shopping app: IKEA is notified every time a customer screenshots the app

Subject & Operator Context

Ingka Group is the largest IKEA franchisee, operating the majority of IKEA retail stores worldwide under franchise from Inter IKEA Systems B.V., the Netherlands-based franchisor that owns the IKEA concept and brand. The IKEA Android app (package com.ingka.ikea.app) is the primary consumer-facing shopping and in-store navigation app, used by a stated 170 million plus IKEA Family members. This audit covers v5.4.0 of the production Android binary.

Engagement Summary

RFI-IRFOS sent the original disclosure on 30 June 2026 to security@ingka.com and privacy@ingka.com, CC press@ingka.com, also BCC the Austrian Datenschutzbehörde, CERT.at, and the Swedish Authority for Privacy Protection (IMY). All three addresses bounced the same day, address not found, meaning the disclosure never reached a live inbox on this first attempt, a mail-infrastructure failure on Ingka Group's side rather than an addressing error.

RFI-IRFOS resent the full disclosure on 17 July 2026 to dpo.ikea.se@ikea.com, CC privacidad@ikea.com, the Austrian Datenschutzbehörde, and the European Data Protection Supervisor, explicitly flagging that the prior delivery had bounced. This resend is the first confirmed successful delivery in the case; a single automated acknowledgment arrived from privacidad@ikea.com the same day the follow-up of 15 August was sent, confirming the message had reached IKEA's data-subject-request queue, but offering no substantive engagement with any finding. RFI-IRFOS sent further follow-ups on 15 August, 24 August, 3 September, and 12 September 2026, each restating the four open findings and the days elapsed since confirmed delivery. The embargo date, stated as 28 September 2026 in the 17 July resend, was confirmed unchanged in every one of the four follow-ups that came after it. Not one message across this record ever received a substantive reply.

Findings

C1: IndoorAtlas API Key and API Secret hardcoded, exposing the in-store positioning infrastructure behind IKEA's own KompassMap system

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.7) — floor plans, magnetic field maps, and positioning session data reachable across the company's entire store network

```
com.indooratlas.android.sdk.API_KEY: [REDACTED, disclosed to Ingka Group 2026-06-30]
com.indooratlas.android.sdk.API_SECRET: [REDACTED, 512-bit, disclosed to Ingka Group
2026-06-30]
```

Powers: KompassMap, in-store navigation and department-level analytics
 Secret classification per IndoorAtlas docs: private, not a public identifier
 Shipped in: every installed copy of com.ingka.ikea.app v5.4.0

Impact: An IndoorAtlas API Key and the accompanying 512-bit API Secret are hardcoded in AndroidManifest.xml in every installed copy of the production app. Per IndoorAtlas's own documentation, the API Secret is an explicitly private credential, not a public identifier meant to ship inside a client binary. These credentials power KompassMap, IKEA's in-store navigation and department-level behavioural analytics system, and anyone extracting them with a tool as basic as apktool gains access to the floor plans, magnetic field maps, and positioning session data IndoorAtlas holds for IKEA's stores. For a public disclosure, the literal credential value is withheld here and available to Ingka Group's security team on request; it was named in full in the original private disclosure sent 30 June 2026.

C2: Firebase API Key and production Realtime Database URL hardcoded alongside it

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N, 7.9) — database reachable if Security Rules are misconfigured, quota and billing denial-of-service applies regardless

```
google_api_key: [REDACTED, disclosed to Ingka Group 2026-06-30]
firebase_database_url: https://ikea-mobile-app-release2.firebaseio.com
```

Reachability of the database itself: depends on Security Rules configuration, not tested by RFI-IRFOS (static analysis only, no live backend probing)
 Confirmed regardless of Security Rules: quota/billing DoS exposure from the hardcoded key, and a project identifier now public via the database URL

Impact: A Google API key and the production Firebase Realtime Database URL are hardcoded in the production app alongside the IndoorAtlas credentials. Whether the database itself is reachable depends on how its Security Rules are configured, a condition RFI-IRFOS cannot verify through static analysis alone and does not claim to have tested; what is confirmed is that the credential and the production URL both ship in the binary, and that quota or billing denial-of-service risk applies to a hardcoded key regardless of the Security Rules question. GDPR Art. 32(1)(b) asks whether technical measures are appropriate to the risk,

and a hardcoded production key plus database URL, unverifiable from the outside as to what it actually permits, does not meet that standard on its own. As with C1, the literal key value is withheld from this public report and was named in full in the original private disclosure.

H1: Two Optimizely receivers and an Adjust content provider begin behavioural tracking at device boot, before the app is ever opened

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, 5.3)
— A/B-testing and attribution data collected before any consent interaction, before the user has even launched the app

```
<receiver android:name="com.optimizely.ab.android.datafile_handler.DatafileRescheduler"
">
  <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></intent
-filter>
</receiver>
<receiver android:name="com.optimizely.ab.android.event_handler.EventRescheduler">
  <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></intent
-filter>
</receiver>
<provider android:name="com.adjust.sdk.SystemLifecycleContentProvider"
  android:authorities="com.ingka.ikea.app.AdjustProvider" android:exported="false"/>
```

Trigger: device boot (Optimizely) and process start (Adjust), both pre-consent

Impact: Two Optimizely A/B-testing components, `com.optimizely.ab.android.datafile_handler.DatafileRescheduler` and `com.optimizely.ab.android.event_handler.EventRescheduler`, are registered to receive the `BOOT_COMPLETED` broadcast, meaning they wake and begin operating the moment the device starts, independent of whether the user has ever opened the IKEA app. An Adjust lifecycle content provider (`com.adjust.sdk.SystemLifecycleContentProvider`) initialises at app start, again before any consent screen is shown. Consent management configured inside the app itself is meaningless if the data collection it is meant to gate has already begun at boot or at process start.

H2: DETECT_SCREEN_CAPTURE on a furniture shopping app: IKEA is notified every time a customer screenshots the app

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, 5.3)
—a permission designed for financial-credential protection or DRM piracy prevention, applied here with no disclosed lawful basis or stated purpose

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

Established legitimate use cases for this permission: financial-app credential protection, DRM-licensed media piracy prevention

Applies to this app: no (furniture shopping catalog)

Disclosed purpose in app's privacy information: none identified

Impact: The app declares `android.permission.DETECT_SCREEN_CAPTURE`, which fires a callback to the app every time the user takes a screenshot. This permission exists for two established purposes, protecting credential-entry screens in financial apps and enforcing DRM in licensed media, neither of which applies to a retail furniture-shopping catalog. IKEA can determine exactly which product listing, price, or cart state a customer chose to capture, a behavioural signal never disclosed as a processing purpose in the app's privacy information, and with no lawful basis stated anywhere for its collection. A furniture shopping app that knows when its own customers are trying to save a price or a product photo for later, and knows it well enough to fire a callback the instant it happens, is not disclosure-matched to any legitimate purpose currently stated for the data.

Impact Analysis

C1 and C2 share the same structural root cause: both are credentials that should never have shipped inside a client-distributed binary in the first place, found side by side in the same manifest, suggesting a build-time secrets-handling gap rather than two unrelated oversights. C1 is the more severe of the two because the data it protects, in-store positioning infrastructure spanning IKEA's retail network, has no equivalent anywhere else; a leaked Firebase key is a known, well-documented risk category with established mitigation playbooks, while a leaked IndoorAtlas secret powering a company's own proprietary in-store navigation system is a far less common, far less immediately mitigable exposure.

H1 and H2 are a different category of finding, not credential exposure but undisclosed pre-consent behavioural collection. Taken together with C1 and C2, the picture is a shopping app that collects positioning-relevant and behavioural data before the user has consented to anything, protected by credentials that were never meant to be public, in a company whose own dedicated security and privacy mailboxes could not even receive the report telling them so.

The Complete Chain: A Disclosure That Bounced at Every Address It Was Sent To

Step 1 – First attempt, outright failure: RFI-IRFOS sends the full disclosure on 30 June 2026 to security@ingka.com and privacy@ingka.com, CC press@ingka.com. All three addresses bounce the same day, address not found. The disclosure never reaches a live inbox on this attempt.

Step 2 – Resend, first confirmed delivery: RFI-IRFOS resends the complete disclosure on 17 July 2026 to dpo.ikea.se@ikea.com, CC privacidade@ikea.com, the Austrian Datens chutzbehoerde, and the European Data Protection Supervisor, explicitly flagging the prior bounce. This is the first confirmed successful delivery, and it states the embargo date of 28 September 2026.

Step 3 – Twenty-nine days, automated acknowledgment only: On 15 August 2026, RFI-IRFOS follows up, restating all four findings. The same day, an automated routing acknowledgment arrives from privacidade@ikea.com, confirming the message reached IKEA's data-subject-r equest queue but engaging with none of the findings.

Step 4 – Fifty-five days, embargo reconfirmed: On 24 August 2026, RFI-IRFOS follows up a second time, restating the findings and the unchanged embargo date. No substantive reply.

Step 5 – Sixty-five days, third follow-up: On 3 September 2026, RFI-IRFOS follows up again, noting twenty-five days since the previous message and reconfirming the embargo. No reply.

Step 6 – Seventy-four days, final follow-up: On 12 September 2026, RFI-IRFOS sends a final follow-up, restating the complete chronology from the original bounce onward and all four findings, confirming the embargo remains 28 September 2026. No reply follows.

Step 7 – Embargo reached and passed: The embargo, stated identically in every message from the 17 July resend onward, passes on 28 September 2026 with all four findings unad-dressed.

Step 8 – Publication: This report publishes 19 days after the embargo date. Across 92 days since the first confirmed delivery, and 109 days since the original bounced attempt, six mes-sages were sent. The only response received across the entire record was one automated routing acknowledgment.

Data Protection – Article by Article

Art. 32(1)(b) GDPR – Security of processing: C1's IndoorAtlas secret and C2's Firebase key, both hardcoded in a client-distributed binary, do not meet the appropriate-technical-measures standard this article requires.

Art. 25 GDPR – Data protection by design and by default: C1's positioning infrastructure, built on a credential never meant to leave IndoorAtlas's own server-side configuration, is the opposite of privacy by design.

Art. 7 GDPR – Conditions for consent: H1's Optimizely and Adjust components begin collecting data before any consent interaction, at boot or at process start respectively.

Art. 5(1)(b), Art. 5(1)(c) GDPR – Purpose limitation and data minimisation: H2's screenshot-detection callback collects a behavioural signal with no stated, disclosed purpose connecting it to any of the app's actual functions.

Art. 13 GDPR – Information to be provided: neither H1's pre-consent tracking components nor H2's screenshot monitoring are named as processing activities anywhere identified in the app's privacy information.

Regulatory & Legal Landscape

Ingka Group and Inter IKEA Systems B.V. operate across the EU with significant presence in the Netherlands, Sweden, and Austria, among others; this disclosure placed the Austrian Datenschutzbehörde, the European Data Protection Supervisor, the Swedish Authority for Privacy Protection (IMY), and CERT.at in BCC or CC across its lifecycle.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32(1)(b) and Art. 25 security-and-design issues in C1 and C2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 7, Art. 5(1)(b,c), and Art. 13 issues in H1 and H2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. For a company operating at the scale Ingka Group does, with more than 170 million IKEA Family members and store-level positioning infrastructure spanning its entire retail network, a hardcoded secret protecting that infrastructure is the kind of finding a supervisory authority is likely to treat as substantive, not cosmetic.

Indicators of Compromise

The following identifiers, SDK packages, and manifest declarations were extracted from the production APK via static analysis only. No Ingka Group servers, accounts, or infrastructure were probed. Literal credential values are withheld from this public report per RFI-IRFOS's standing practice for unremediated, exploitable secrets; they were disclosed in full to the responsible parties in the original private communication.

```
C1 -- com.indooratlas.android.sdk.API_KEY + API_SECRET (hardcoded,
      values withheld, disclosed privately 2026-06-30)

C2 -- google_api_key (withheld) + firebase_database_url:
      https://ikea-mobile-app-release2.firebaseio.com

H1 -- com.optimizely.ab.android.datafile_handler.DatafileRescheduler,
      com.optimizely.ab.android.event_handler.EventRescheduler (BOOT_COMPLETED),
      com.adjust.sdk.SystemLifecycleContentProvider (pre-consent)

H2 -- android.permission.DETECT_SCREEN_CAPTURE
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to security@ingka.com and privacy@ingka.com, CC press@ingka.com, BCC Austrian DSB, CERT.at, and IMY. All three addresses bounce the same day, address not found. Never reaches a live inbox.

2026-07-17 Full disclosure resent to dpo.ikea.se@ikea.com, CC privacidade@ikea.com, Austrian DSB, and EDPS, flagging the prior bounce. First confirmed delivery. Embargo stated as 2026-09-28.

2026-08-15 Follow-up sent, 29 days since confirmed delivery. Same day, an automated routing acknowledgment arrives from privacidade@ikea.com, confirming receipt only.

2026-08-24 Follow-up sent, 55 days since confirmed delivery, embargo reconfirmed unchanged. No reply.

2026-09-03 Follow-up sent, 65 days since confirmed delivery, 25 days since the previous message. No reply.

2026-09-12 Final follow-up sent, 74 days since confirmed delivery, full chronology and all four findings restated, embargo reconfirmed unchanged. No reply.

2026-09-28 Embargo date reached (stated identically in every message from the resend onward). Correspondence record: six RFI-IRFOS messages, one bounced attempt, one automated routing acknowledgment, zero substantive replies.

2026-10-17 This report published, 19 days after the embargo date. All four findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 – Immediate: rotate the IndoorAtlas API Key and API Secret, move the secret server-side behind a token-exchange flow rather than shipping it in the client binary, and audit IndoorAtlas-side logs for any unauthorised use during the exposure window.

C2 – Immediate: rotate the Firebase API key, verify and harden the Realtime Database's Security Rules, and move any sensitive read/write paths behind authenticated, server-mediated access rather than direct client access to the database URL.

H1 – Near-term: gate Optimizely and Adjust initialisation behind an explicit consent check, and review whether BOOT_COMPLETED registration is actually necessary for either SDK's stated function.

H2 – Near-term: either remove DETECT_SCREEN_CAPTURE entirely, since no disclosed purpose in a furniture shopping app justifies it, or disclose the exact purpose, lawful basis, and data use in the privacy policy if a legitimate internal reason exists.

Across all findings: review the mail-routing configuration that caused the original disclosure to bounce outright at three separately maintained addresses (security@, privacy@, press@ingka.com) rather than reaching any human inbox, since the same failure would equally have blocked a report from a customer, a researcher, or a regulator attempting to reach Ingka Group's own published contact points.

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 analysis of the published application using publicly available tooling. No Ingka Group servers, accounts, or infrastructure were probed. Literal credential values are withheld from this public report and were disclosed in full to the responsible parties in the original private communication. 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 COM.INGKA.IKEA.APP.