Coordinated Security & Privacy Disclosure, Final Report

heyOBI for Android (de.obi.app, v26.5.8)

Ten written notices, one substantive point-by-point rebuttal disputing three of five findings, two findings never addressed, silence for the final ten weeks

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – TWO OF FIVE FINDINGS NEVER ADDRESSED, ONE UNILATERALLY DECLARED CLOSED

Target	OBI GmbH & Co. Deutschland KG, Wermelskirchen, Germany; OBI GmbH & Co. KG Oesterreich
Product audited	heyOBI for Android, de.obi.app, v26.5.8
Disclosure reference	REF HEYOBI-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 ContentSquare and Heap dual-layer session-replay capture initializing before any consent interaction, CVSS v4.0 8.7, never addressed by OBI)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production heyOBI Android application and identified two CRITICAL and three HIGH findings: a Firebase API key hard-coded in the public APK with no SHA-256 certificate-fingerprint restriction, a ContentSquare and Heap dual-layer behavioral and session-replay integration (517 combined smali classes) that auto-initializes on app launch before any consent interaction occurs, four overlapping advertising-tracking permissions (Privacy Sandbox Topics API, Advertising ID, and related ext.adservices permissions) declared alongside the Adjust SDK, precise location and Bluetooth Low Energy beacon scanning combined with loyalty purchase history for in-store product navigation, capable of building an in-store movement profile, and a Webtrekk/Mapp Digital integration whose linkage to Mapp Engage CRM marketing automation RFI-IRFOS's own correspondence characterized as reach-measurement analytics; OBI's own reply disputes the specific 'INFOnline' branding of that characterization, though not the presence or CRM linkage of Webtrekk itself.

OBI's data protection team replied substantively twice, on 27 June redirecting RFI-IRFOS to a vulnerability-disclosure portal (a channel intended for security vulnerabilities, not GDPR notices, which RFI-IRFOS declined as inapplicable), and on 2 July with a genuinely detailed, apparently human-authored rebuttal disputing the Firebase finding (characterizing an unrestricted key as 'public by design' for the Firebase SDK architecture, without addressing the specific finding that no SHA-256 fingerprint restriction was applied), disputing that the app accesses the Topics API despite the corresponding permission being declared in the manifest, and disputing that any INFOnline-branded reach-measurement component is integrated. OBI's 2 July reply did not address the ContentSquare/Heap pre-consent capture finding (C2) or the location/Bluetooth in-store profiling finding (H2) at all, and declared the matter closed regardless. A follow-up reply on 9 July reiterated the closure with no new content. No further reply of any kind was received across five subsequent written notices sent between 23 July and 11 September.

Scope: Static analysis of the publicly downloaded production heyOBI Android APK (v26.5.8), on an authorized test device, only. No OBI account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@obi.de and service@obi.at, bcc/cc the Landesbeauftragte für Datenschutz NRW, the Austrian Datenschutzbehörde, and CERT.at. OBI's data protection team replied twice substantively, first redirecting to a vulnerability-disclosure portal not suited to a GDPR notice, then on 2 July with a detailed point-by-point rebuttal disputing three of five findings and declaring the matter closed. OBI never addressed the two remaining findings and sent no further reply after 9 July, across five subsequent written notices over the following ten weeks.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded, no SHA-256 certificate-fingerprint restriction

ID	Severity	Title
C2	CRITICAL	ContentSquare and Heap dual-layer capture initializes before any consent interaction
H1	HIGH	Topics API and four overlapping advertising-tracking permissions declared
H2	HIGH	Precise location and Bluetooth beacon scanning combined with loyalty purchase history
H3	HIGH	Webtrekk/Mapp Digital reach-measurement integration linked to CRM marketing automation

Subject & Operator Analysis

OBI GmbH & Co. Deutschland KG is headquartered in Wermelskirchen, Germany, with OBI GmbH & Co. KG Oesterreich as its Austrian subsidiary. The Landesbeauftragte für Datenschutz NRW is OBI's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Firebase API key hardcoded, no SHA-256 certificate-fingerprint restriction

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

google_api_key AIzaSyD2KXb9T2t1I-92rYQiz5vYhTPcp0_7kAg, Firebase project hey-obi, storage bucket hey-obi.appspot.com, is not restricted by a SHA-256 certificate fingerprint.

OBI's 2 July reply characterized the Firebase key as 'public by design' for stability and crash monitoring, which is accurate as to the key's own visibility but does not address the specific finding: the key is not restricted to the app's package name and signing fingerprint, the standard hardening step Google's own documentation recommends regardless of the key's inherent visibility.

Impact: Without a SHA-256 fingerprint restriction, the exposed key can be used from any application, not only the legitimate heyOBI client, against the associated Firebase project.

Fix: Restrict the key to the correct package name and SHA-256 signing fingerprint in the Firebase console, and confirm deny-by-default security rules.

C2: ContentSquare and Heap dual-layer capture initializes before any consent interaction

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

425 smali classes implement ContentSquare and 92 implement Heap, 517 combined. CSQInitializer, registered via AndroidX Startup, and Heap's autocapture content providers initialize automatically on app launch, before any consent interaction occurs.

OBI's 2 July reply and its 9 July follow-up did not address this finding at all, despite it being explicitly restated in RFI-IRFOS's rejection of the 2 July closure. No reply of any kind has addressed it since.

Impact: Behavioral and session-replay data capture may begin before a user has made any consent decision, contrary to the consent-before-processing sequencing GDPR Art. 6/7 requires for non-essential tracking.

Fix: Gate both ContentSquare and Heap initialization behind an affirmative consent decision.

H1: Topics API and four overlapping advertising-tracking permissions declared

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, android.ext.adservices, and AD_ID permissions are declared in the manifest, alongside the Adjust SDK (203 smali classes).

OBI's 2 July reply states the app 'does not access the Topics API,' without addressing why the corresponding manifest permission is declared if genuinely unused.

Impact: A declared but allegedly unused ad-tracking permission leaves ambiguity about actual runtime behavior that static analysis alone, and OBI's own denial, do not fully resolve.

Fix: Remove manifest permissions for capabilities the app does not use, so declared permissions match actual behavior.

H2: Precise location and Bluetooth beacon scanning combined with loyalty purchase history

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

ACCESS_FINE_LOCATION and BLUETOOTH_SCAN, combined with in-store BLE beacon navigation assets (InstoreLocatorSVG), enable in-store product navigation that can be correlated with loyalty purchase history.

No OBI reply addressed this finding at any point in the correspondence.

Impact: Combined precise indoor location and purchase-history data could construct a granular in-store movement and shopping-behavior profile with no confirmed disclosure of that specific combination.

Fix: Disclose the combination of in-store location tracking and loyalty purchase history as a specific processing activity, with its own legal basis.

H3: Webtrekk/Mapp Digital reach-measurement integration linked to CRM marketing automation

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

webtrekk.android.sdk.integration.EngageIntegrationReceiver (17 smali classes) links Webtrekk-collected data to Mapp Engage CRM marketing automation.

OBI's 2 July reply states no INFOnline-branded reach-measurement component is integrated. RFI-IRFOS's own characterization of this finding as 'INFOnline reach measurement' is disputed by OBI on that specific branding point; the underlying presence of Webtrekk and its Mapp Engage CRM linkage is not itself disputed.

Impact: Analytics data collected under a reach-measurement framing may be linked to CRM marketing automation as a secondary purpose not separately disclosed.

Fix: Disclose the Mapp Engage CRM linkage as a distinct secondary purpose separate from analytics/reach measurement.

A Genuine Rebuttal, Two Findings It Never Reached

OBI's 2 July reply is, among every case in this disclosure wave, one of the few genuinely substantive, apparently human-authored rebuttals received: it engaged with three specific findings on their technical merits, disputing each. It did not, however, address the two remaining findings, the ContentSquare/Heap pre-consent capture (C2) and the location/Bluetooth in-store profiling (H2), at all, and it declared the entire matter closed regardless. RFI-IRFOS disputed that closure the same day and asked for a substantive answer on the two unaddressed findings and on whether an Art. 35 DPIA exists for the combined ContentSquare/Heap processing; OBI's 9 July reply reiterated its closure with no new content, and no further reply of any kind followed across five subsequent notices over the following ten weeks.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Firebase key not restricted by SHA-256 fingerprint
C2	GDPR Art. 6(1), Art. 7, Art. 25, Art. 35	Pre-consent behavioral/session-replay capture, never addressed by OBI
H1	GDPR Art. 5(1)(c), Art. 13(1)(c)	Declared but disputedly-unused advertising-tracking permissions
H2	GDPR Art. 5(1)(c), Art. 13(1)(e)	In-store location/Bluetooth profiling combined with purchase history, never addressed by OBI
H3	GDPR Art. 13(1)(e)	CRM marketing-automation linkage not separately disclosed

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@obi.de and service@obi.at, bcc LDI NRW/Austrian DSB/CERT.at; 2 CRITICAL + 3 HIGH findings; a EUR 75,000 figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-06-27	OBI redirects to a vulnerability-disclosure portal; RFI-IRFOS declines the redirect as inapplicable to a GDPR notice
2026-07-02	OBI sends a detailed rebuttal disputing three findings, does not address C2 or H2, declares the matter closed, declines the referenced figure
2026-07-02	RFI-IRFOS disputes the closure the same day, demands a substantive answer on C2/H2/DPIA by 9 July, moves regulators to visible cc
2026-07-09	OBI reiterates closure with no new content
2026-09-11	Latest follow-up on file; no OBI reply since 9 July
2026-09-19	Embargo, as calculated from R1's stated 90-day disclosure period, closes and this report publishes

Residual Risk & Recommendations

- Address the ContentSquare/Heap pre-consent capture finding specifically, which the 2 July rebuttal did not cover.
- Address the in-store location/Bluetooth profiling finding specifically, which was also not covered.
- Restrict the Firebase key by SHA-256 certificate fingerprint, the specific gap OBI's 'public by design' response did not resolve.
- Reconcile declared-but-disputedly-unused advertising permissions with actual runtime behavior.
- Publish an Art. 35 DPIA covering the combined ContentSquare/Heap processing if one exists, or conduct one.

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 Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 6, 7, 13, 25, 32, 35. REF HEYOBI-2026-R1.