



Security & Privacy Disclosure, Final Report

Decathlon Android (com.decathlon.app)

A screen-recording SDK is configured at `initOrder=Integer.MAX_VALUE` so it starts before any other process in the app, including the consent screen, on a payment and loyalty app for one of the world's largest sporting-goods retailers, unresolved through 109 days and eight messages, every one of them answered only by an automated legal or press intake responder, never a human, now 19 days past embargo

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

Target	Decathlon SE, Villeneuve-d'Ascq, France (~EUR 17 billion revenue, 1,700+ stores, 60 countries)
Package	com.decathlon.app
Platform Audited	Android, static analysis of the production APK
Initial Disclosure (R1)	2026-06-30, to security@decathlon.com and dpo@decathlon.com, CC presse@decathlon.de, Austrian DSB, CERT.at, EDPS, CNIL
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (2 Critical, 2 High)
Correspondence	8 messages sent by RFI-IRFOS (2026-06-30, 07-06, 07-17, 07-23, 08-09, 08-21, 08-28, 09-11), met exclusively by automated legal-intake acknowledgments from dpo@decathlon.com and automated press-intake acknowledgments from presse@decathlon.de, 0 substantive replies ever received from security@decathlon.com, dpo@decathlon.com, or any named human
Authorities CC'd	Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · CERT.at · European Data Protection Supervisor (edps@edps.europa.eu) · CNIL (notifications@cnil.fr), lead supervisory authority for Decathlon SE, registered France

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	6
4.1	C1: Two hardcoded Firebase and Google Maps API keys extracted from the production binary	6
4.2	C2: Screen-recording SDK configured at initOrder=Integer.MAX_VALUE, architecturally the first process the app starts, ahead of the consent screen	6
4.3	H1: AltBeacon in-store BLE movement tracking linked to the customer's loyalty profile and purchase history	7
4.4	H2: Salesforce Marketing Cloud (1,859 classes) transfers data to US infrastructure with no Art. 44-49 mechanism identified	8
5	Impact Analysis	8
6	The Complete Chain: Eight Messages, Two Auto-Responders, Zero Human Replies	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

Decathlon SE is a France-headquartered sporting-goods retailer with roughly EUR 17 billion in annual revenue, operating 1,700+ stores across 60 countries. A static analysis of the production Android app, used for payment, loyalty, and in-store navigation, found four findings, two CRITICAL and two HIGH.

The app's Luciq screen-recording SDK is configured with `android:initOrder="2147483647"`, the literal value of `Integer.MAX_VALUE`, on its content provider. This is not a framework default and not a tooling artifact, it is a value someone typed deliberately, and its effect is to start the screen-recording infrastructure before any other process in the app, including the consent screen a user would see first. Two services declared with `foregroundServiceType="mediaProjection"` follow, one for screen video, one for screenshot capture, on an app that handles payment flows, a loyalty account, and a personal sports profile (C2). Two hardcoded Firebase and Google Maps API keys were extracted directly from the production binary, with no documented rotation or scoping found (C1). The app also runs AltBeacon, an open-source Bluetooth Low Energy beacon-scanning library, which Decathlon uses to track customers' movement through store departments via in-store beacons, linking that movement data to the same customer's loyalty profile and purchase history (H1). Finally, a Salesforce Marketing Cloud integration (1,859 classes) transfers data to United States infrastructure with no Art. 44 to 49 transfer mechanism identified anywhere in the app or its disclosures (H2).

RFI-IRFOS disclosed these findings on 30 June 2026 to security@decathlon.com and dpo@decathlon.com, CC.presse@decathlon.de, the Austrian Datenschutzbehoerde, CERT.at, the European Data Protection Supervisor, and the CNIL (France's own supervisory authority, given Decathlon's registration there). Across 109 days and eight messages sent (30 June, 6 July, 17 July, 23 July, 9 August, 21 August, 28 August, 11 September 2026), every single response came from an automated intake system, dpo@decathlon.com's Portuguese-language legal-request acknowledgment or presse@decathlon.de's German-language press-inquiry auto-reply, the same templated text each time, addressed to no specific finding. Not one message in eight was ever answered by a named human. The embargo, stated plainly in the original disclosure as 28 September 2026, passed with all four findings unaddressed, and this report publishes 19 days after that date.

ID	Severity	Title
C1	CRITICAL	Two hardcoded Firebase and Google Maps API keys extracted from the production binary
C2	CRITICAL	Screen-recording SDK configured at <code>initOrder=Integer.MAX_VALUE</code> , architecturally the first process the app starts, ahead of the consent screen
H1	HIGH	AltBeacon in-store BLE movement tracking linked to the customer's loyalty profile and purchase history
H2	HIGH	Salesforce Marketing Cloud (1,859 classes) transfers data to US infrastructure with no Art. 44-49 mechanism identified

Subject & Operator Context

Decathlon SE is a French multinational sporting-goods retailer, among the largest in the world by revenue, operating more than 1,700 stores across 60 countries. The Decathlon Android app (com.decathlon.app) is the group's primary consumer-facing app, used for product browsing, in-app and in-store payment, a loyalty program, and in-store navigation assistance, making it a repository of payment data, a loyalty identity, and a personal sports profile for its users.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to security@decathlon.com and dpo@decathlon.com, CC presse@decathlon.de, the Austrian Datenschutzbehoerde, CERT.at, the European Data Protection Supervisor, and the CNIL. The response was an automated Portuguese-language legal-intake acknowledgment from dpo@decathlon.com ("Agradecemos desde ja o seu contacto... este email destina-se exclusivamente para questoes [legais]") and, separately, a German-language automated press-inquiry acknowledgment from presse@decathlon.de. Both are templated auto-responders, not case-specific replies.

RFI-IRFOS followed up on 6 July, 17 July, 23 July, 9 August, 21 August, and 28 August 2026, each restating the open findings and the days elapsed, each addressed to security@decathlon.com and dpo@decathlon.com with presse@decathlon.de in CC (and the Austrian DSB, CERT.at, EDPS re-added in CC on the 9 August follow-up). Each follow-up triggered the identical pair of automated acknowledgments, in some cases from both dpo@decathlon.com and privacy.portugal@decathlon.com, a related legal-intake address that separately confirmed receipt with its own reference number, still automated, still unrelated to the substance of the findings. A final follow-up was sent on 11 September 2026, 73 days and eight messages into the correspondence, again answered only by the same two automated systems. No message from security@decathlon.com, dpo@decathlon.com, or any named human ever directly engaged with a single one of the four findings.

Findings

C1: Two hardcoded Firebase and Google Maps API keys extracted from the production binary

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.5) — unscoped backend and mapping credentials embedded directly in a payment and loyalty app for a global retailer

```
google_api_key: AIzaSyAwa0Dl6Ebqhe4R5HIwBYGmXqyeQKPNtLE
MAPS_API_KEY: AIzaSyAl-KAgLTmibJqrL40WajMaSGeJcklaxMS4
```

```
Rotation policy identified: none
Key scoping / referrer restriction identified: none
```

Impact: Two API keys were extracted directly from the production APK: a Google/Firebase key (google_api_key) and a separate Google Maps key (MAPS_API_KEY). No rotation policy, key-scoping restriction, or referrer/package restriction was identified for either. On an app that processes payment flows and a loyalty identity for a ~EUR 17 billion retailer, an unscoped backend key extracted from a public binary carries a quota-exhaustion and billing-abuse blast radius, and raises the question of what server-side rules, if any, constrain what the key can read or write. "Not a secret" does not mean "not a problem", the burden of demonstrating otherwise sits with the operator under Art. 5(2) GDPR.

C2: Screen-recording SDK configured at initOrder=Integer.MAX_VALUE, architecturally the first process the app starts, ahead of the consent screen

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — screen-video and screenshot capture infrastructure initializes before any consent interaction, on an app handling payment and loyalty data

```
<provider android:name="ai.luciq.apm.contentprovider.APMContentProvider"
  android:initOrder="2147483647"/> <!-- Integer.MAX_VALUE -->

<service android:name="ai.luciq.bug.internal.video.ScreenRecordingService"
  android:foregroundServiceType="mediaProjection"/>

<service android:name="ai.luciq.library.screenshot.ScreenshotCaptureService"
  android:foregroundServiceType="mediaProjection"/>

smali string: "start capture screenshot Using MediaProjection"
```

Impact: The Luciq APMContentProvider is declared with android:initOrder="2147483647", the literal integer value of Integer.MAX_VALUE. Android content providers initialize in ascending initOrder sequence, meaning this provider is set to start before every other content

provider in the app, by construction, as the very first process to run, before the user has seen a consent screen or any other app logic. Two services with `foregroundServiceType="mediaProjection"` follow directly from this SDK: `ai.luciq.bug.internal.video.ScreenRecordingService` (screen video) and `ai.luciq.library.screenshot.ScreenshotCaptureService` (screenshot capture), with small strings confirming "start capture screenshot Using MediaProjection". `Integer.MAX_VALUE` is not a value any build tool or framework writes automatically, it is a deliberate choice, and its only functional effect is to guarantee this SDK initializes ahead of anything else, including whatever gates user consent. This sits on an app with payment flows, a loyalty account, and a personal sports profile.

H1: AltBeacon in-store BLE movement tracking linked to the customer's loyalty profile and purchase history

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)
— physical movement through store departments becomes identity-linked behavioral data with no distinctly disclosed purpose

```
<service android:name="org.altbeacon.beacon.service.BeaconService"
  android:foregroundServiceType="location"/>
```

Library: `org.altbeacon.beacon` (AltBeacon BLE scanning)
 Linked identity: loyalty profile + purchase history

Impact: The app embeds `org.altbeacon.beacon.service.BeaconService`, declared with `android:foregroundServiceType="location"`. AltBeacon is an open-source library for scanning Bluetooth Low Energy beacons, and Decathlon places physical beacons inside its stores, meaning the app tracks a customer's movement path through store departments as they shop. This movement data is linkable to the same customer's loyalty profile and purchase history, turning a walk through a store into an identity-linked behavioral trace. Decathlon's disclosures do not separately name in-store BLE movement tracking as its own processing purpose distinct from general loyalty-program data collection.

H2: Salesforce Marketing Cloud (1,859 classes) transfers data to US infrastructure with no Art. 44-49 mechanism identified

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 large, undisclosed-transfer-basis marketing platform sits alongside the in-store movement data from H1

Salesforce Marketing Cloud: 1,859 smali classes
 MCInitContentProvider: initializes at app startup
 Transfer destination: United States
 Art. 44-49 mechanism identified: none

Impact: Salesforce Marketing Cloud is present as 1,859 smali classes, including an MCInitContentProvider that initializes as part of the app's normal startup sequence. Marketing Cloud data flows to United States infrastructure, and no Art. 44-49 GDPR transfer mechanism (Standard Contractual Clauses, adequacy decision, or equivalent) was identified for this flow in the app or its available disclosures. Combined with H1, this raises the specific question of what Art. 28 processing agreement and what transfer mechanism govern sending in-store movement profiles onward to a US-based marketing platform.

Impact Analysis

C2 is the most severe finding in this report not because screen-recording SDKs are inherently dangerous, but because of the specific, deliberate choice behind it: Integer.MAX_VALUE is not a value any build system writes on its own, it is typed by a person, and its only purpose is to guarantee this SDK starts before literally anything else in the app, including whatever would otherwise gate consent. C1 compounds the picture, an unscoped backend key sitting in the same binary as a payment and loyalty flow. H1 and H2 describe a second, separate data channel, in-store movement tracked via Bluetooth beacons and fed, through Salesforce, to US infrastructure with no documented transfer basis, which turns a shopping visit into identity-linked, internationally-transferred behavioral data.

What ties all four findings together procedurally is the nature of the correspondence itself: across 109 days and eight messages, Decathlon's own security and data-protection mailboxes never once produced a human response. Every single reply, from either address, every time, was an automated acknowledgment bearing no relationship to the specific findings raised.

The Complete Chain: Eight Messages, Two Auto-Responders, Zero Human Replies

Step 1 – Disclosure sent: RFI-IRFOS sends the full disclosure on 30 June 2026 to security@decathlon.com and dpo@decathlon.com, CC presse@decathlon.de, the Austrian Datenschutz zbehoerde, CERT.at, the EDPS, and the CNIL. dpo@decathlon.com's automated Portuguese-language legal-intake responder and presse@decathlon.de's automated German-language press responder both reply within the same window, neither referencing any finding.

Step 2 – 6 July 2026: First follow-up. Same two automated responses.

Step 3 – 17 July 2026: A further follow-up, sent directly to dpo@decathlon.com with presse@decathlon.de in CC, restating 17 days and two auto-replies with zero substantive response. Same automated pattern repeats.

Step 4 – 23 July 2026: Follow-up to security@decathlon.com and dpo@decathlon.com, CC the Austrian DSB. privacy.portugal@decathlon.com's related legal-intake auto-responder also replies separately, assigning its own reference number, still automated.

Step 5 – 9 August 2026: Follow-up restating 40 days, five messages, four automated replies at that point, CC presse@decathlon.de, the Austrian DSB, CERT.at, and the EDPS. Same automated pair responds again.

Step 6 – 21 August 2026: Follow-up restating 52 days, six messages, five automated replies. No change in response pattern.

Step 7 – 28 August 2026: Follow-up restating 59 days, seven messages, six automated replies. No change.

Step 8 – 11 September 2026: Final follow-up, 73 days and eight messages sent in total, restating all four findings. Answered, for the eighth time, only by the same two automated systems.

Step 9 – Embargo reached and passed: The embargo, stated plainly in the original disclosure as 28 September 2026, passes with all four findings unaddressed by any human at Decathlon.

Step 10 – Publication: This report publishes 19 days after the embargo date. Across 109 days and eight messages, the correspondence record shows exactly zero substantive replies.

Data Protection – Article by Article

Art. 5(1)(f), Art. 32(1)(b) GDPR – Integrity, confidentiality, and security of processing: C1's unscoped hardcoded keys and C2's pre-consent screen-recording infrastructure both fall short of the technical measures these provisions require.

Art. 6(1) GDPR – Lawfulness of processing: C2's screen-recording SDK initializes before any consent interaction is possible, and H1's in-store movement tracking is not clearly grounded in a distinct, disclosed legal basis.

Art. 13 GDPR – Information to be provided: Neither C2's screen-recording infrastructure nor H1's in-store BLE tracking is transparently described as its own distinct processing activity in Decathlon's available disclosures.

Art. 5(1)(c) GDPR – Data minimisation: H1 links physical in-store movement to a loyalty identity and purchase history, a combination broader than what loyalty-program participation alone would require.

Art. 44-49, Art. 28 GDPR – International transfers and processor agreements: H2's Sales-force Marketing Cloud transfer to the United States has no identified Art. 44-49 safeguard or disclosed Art. 28 processing agreement.

Regulatory & Legal Landscape

Decathlon SE is registered in France, placing it under the lead supervisory authority of the CNIL, CC'd on the original disclosure and again on this closure. The Austrian Datenschutzbehörde, CERT.at, and the European Data Protection Supervisor were also CC'd, given RFI-IRFOS's Austrian registration and the EU-wide scope of a retailer operating in 60 countries.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 6(1), 5(1)(c), and 13 issues in C2 and H1, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32(1)(b), 5(1)(f), 44-49, and 28 issues in C1 and H2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. For a retailer of Decathlon's scale, a screen-recording SDK deliberately configured to start before consent, on an app handling payment and loyalty data, is the kind of finding a supervisory authority is likely to treat as a substantive design choice rather than an oversight.

Indicators of Compromise

The following identifiers, SDK configurations, and manifest declarations were extracted from the production APK via static analysis only. No Decathlon servers, accounts, or infrastructure were probed.

```
C1 -- google_api_key: AIzaSyAwa0Dl6Ebqhe4R5HIwBYGmXqyeQKPNtLE
    MAPS_API_KEY: AIzaSyAl-KAgLTmibJqrL40WajMaSgeJcklaxMS4

C2 -- ai.luciq.apm.contentprovider.APMContentProvider,
    android:initOrder="2147483647" (Integer.MAX_VALUE)
    ai.luciq.bug.internal.video.ScreenRecordingService (mediaProjection)
    ai.luciq.library.screenshot.ScreenshotCaptureService (mediaProjection)

H1 -- org.altbeacon.beacon.service.BeaconService (foregroundServiceType=location)

H2 -- Salesforce Marketing Cloud, 1,859 smali classes, MCInitContentProvider
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to security@decathlon.com and dpo@decathlon.com, CC presse@decathlon.de, Austrian DSB, CERT.at, EDPS, CNIL. Automated legal-intake and press-intake acknowledgments received, no substantive reply.

2026-07-06 Follow-up sent. Same automated pattern.

2026-07-17 Follow-up sent to dpo@decathlon.com, CC presse@decathlon.de, restating 17 days, two auto-replies, zero substantive response. Same automated pattern.

2026-07-23 Follow-up sent to security@decathlon.com and dpo@decathlon.com, CC Austrian DSB. A related legal-intake address, privacy.portugal@decathlon.com, also auto-acknowledges separately.

2026-08-09 Follow-up sent, CC presse@decathlon.de, Austrian DSB, CERT.at, EDPS, restating 40 days, five messages, four automated replies. Same automated pattern.

2026-08-21 Follow-up sent, restating 52 days, six messages, five automated replies. Same automated pattern.

2026-08-28 Follow-up sent, restating 59 days, seven messages, six automated replies. Same automated pattern.

2026-09-11 Final follow-up sent, restating 73 days, eight messages, eight automated replies in total across the full correspondence. Same automated pattern, no human reply.

2026-09-28 Embargo date reached, as stated in the original disclosure. Correspondence record: eight RFI-IRFOS messages, exclusively automated acknowledgments in response, 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 both exposed keys, apply API-level scoping and referrer/package restrictions, and audit backend rules for anything the unscoped key could have read or written during its exposure window.

C2 – Immediate: remove Integer.MAX_VALUE as the Luciq SDK's initOrder, gate screen-recording and screenshot-capture initialization behind an explicit, pre-collection consent screen, and document the Art. 6(1) legal basis and Art. 35 DPIA for this configuration.

H1 – Near-term: disclose in-store BLE movement tracking as its own distinct processing purpose under Art. 13, separate from general loyalty-program data collection, and document its specific legal basis.

H2 – Near-term: document an Art. 44-49 transfer mechanism for the Salesforce Marketing Cloud data flow to the United States and confirm an Art. 28 processing agreement is in place.

Across all findings: route formal security and data-protection disclosures to a path that reaches a human reviewer, not exclusively an automated legal-request or press-inquiry intake system. Over 109 days and eight messages, every single response Decathlon's systems produced was a templated acknowledgment; the dedicated security and DPO mailboxes themselves never responded once.

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 Decathlon 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 COM.DECATHLON.APP.