# Coordinated Security & Privacy Disclosure, Final Report

## Leap Fitness: Arm Workout, Six Pack in 30 Days, Splits Training, Stretching Exercises, Height Increase Workout

Five-app fitness portfolio, one shared tracking template, no EU Art. 27 representative found

**PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, EIGHT WRITTEN NOTICES, NO RESPONSE OF ANY KIND**

| | |
|---|---|
| **Target** | Leap Fitness Group (developer account, no EU Art. 27 representative identified) |
| **Products audited** | Arm Workout, Six Pack in 30 Days, Splits Training, Stretching Exercises, Height Increase Workout, all built on the shared com.drojian.workout.framework |
| **Disclosure reference** | REF LEAP-FITNESS-BUNDLE-2026-R1 |
| **R1 sent** | 2026-06-22 |
| **Disclosure / embargo date** | 2026-09-19 |
| **Report published** | 2026-09-19 |
| **Severity** | CRITICAL (C2 TikTok Pangle / China routing, CVSS v4.0 8.7 High) |

rfi.irfos@gmail.com • rfi-irfos.com

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

## Contents

## Executive Summary

On 22 June 2026, RFI-IRFOS performed static analysis of five Android fitness applications published under the same developer account, Arm Workout, Six Pack in 30 Days, Splits Training, Stretching Exercises, and Height Increase Workout, and found all five built on an identical shared codebase, com.drojian.workout.framework, carrying identical findings across every app. Rather than five separate disclosures, RFI-IRFOS addressed all five in one bundled notice, since the underlying tracking architecture is shared, not coincidentally similar.

The Facebook Audience Network SDK, spanning 17,262 smali classes combined across the bundle, is undisclosed as a data recipient in any of the five apps' privacy policies. TikTok's Pangle SDK, operated by ByteDance, has confirmed active production endpoints routing to China with no EU adequacy decision, also undisclosed. Each app ships its own hardcoded Firebase API key, and two of the five apps feed the ACTIVITY_RECOGNITION permission directly into the advertising SDK stack.

Eight written notices were sent to support@leap.app, the only reachable inbox across all five apps, over 91 days. None produced a substantive reply, an acknowledgment, an automated ticket, or even a bounce. No data protection officer, privacy contact, or security contact was ever located for this developer, and no EU Art. 27 representative appears to be designated for a developer whose apps are distributed to EU users.

**Scope:** Static analysis of the publicly downloaded production Android APKs for five Leap Fitness apps, on an authorized test device, only. No backend, account, or infrastructure was accessed or tested.

**Disposition**

R1 sent 22 June 2026 to support@leap.app, covering all five apps at once, since all five share the identical com.drojian.workout.framework tracking template. Seven further written notices followed through 16 September 2026. Not one produced a substantive reply, an acknowledgment, an automated ticket, or a bounce. No data protection officer, privacy contact, or security contact was ever found reachable beyond the single support@leap.app inbox, across five separately published Play Store apps.

| ID | Severity | Title |
|---|---|---|
| C1 | CRITICAL | Facebook Audience Network: 17,262 combined smali classes, undisclosed as a data recipient in any of the five apps |
| C2 | CRITICAL | TikTok Pangle (ByteDance): active production endpoints routing to China, undisclosed |
| C3 | CRITICAL | Hardcoded Firebase API key in each app's binary, one project per app |
| H1 | HIGH | ACTIVITY_RECOGNITION permission feeding the advertising SDK stack |
| H2 | HIGH | Adjust SDK: undisclosed install attribution |

| ID | Severity | Title |
|---|---|---|
| H3 | HIGH | No EU Art. 27 representative identified for a developer distributing to EU users |

## Subject & Operator Analysis

The five audited apps are published under a developer account operating the shared com.drojian.workout.framework codebase, reachable only via support@leap.app. No corporate entity name, registered address, or EU representative is identifiable from any of the five apps' own privacy policies or Play Store listings, itself a finding relevant to GDPR Art. 13(1)(a)'s controller-identity disclosure requirement, independent of the six findings detailed below.

## Findings

### C1: Facebook Audience Network: 17,262 combined smali classes, undisclosed as a data recipient in any of the five apps

**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**

The Facebook Audience Network SDK is integrated across all five apps, totaling 17,262 smali classes combined. It is not named as a data recipient in any of the five apps' privacy policies.

No response was received naming this finding across eight written notices. GDPR Art. 13(1)(e) requires disclosure of recipients of personal data; a shared ad SDK integrated identically across a five-app portfolio, undisclosed in every single one, is a portfolio-wide transparency failure, not an isolated oversight.

**Impact:** Behavioral data from five fitness apps flows to Meta's advertising infrastructure without disclosure to users in any of the five privacy policies.

**Fix:** Disclose Facebook Audience Network as a data recipient under Art. 13(1)(e) across all five apps' privacy policies.

### C2: TikTok Pangle (ByteDance): active production endpoints routing to China, undisclosed

**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**

Pangle, ByteDance's ad monetization SDK, has confirmed active production endpoints in the shared framework, routing to Chinese infrastructure with no EU adequacy decision.

No response was received naming this finding. This data flow is undisclosed in any of the five apps' privacy policies, and no Art. 44-49 transfer mechanism is visible in any of the five binaries.

**Impact:** Fitness app usage data from five separately published apps is routed to Chinese ad infrastructure with no transfer safeguard and no user disclosure.

**Fix:** Remove Pangle or implement and disclose a verified Art. 44-49 transfer mechanism across all five apps.

### C3: Hardcoded Firebase API key in each app's binary, one project per app

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

Each of the five apps ships a distinct hardcoded Firebase API key, one project per app.

No response was received naming this finding, including the direct yes/no question of whether any of the five keys has been rotated.

**Impact:** Five separate exposed credentials enable FCM token enumeration and probing against five separate backend projects.

**Fix:** Rotate all five keys and restrict each to its production certificate fingerprint.

### H1: ACTIVITY_RECOGNITION permission feeding the advertising SDK stack

**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**

In two of the five apps, the ACTIVITY_RECOGNITION permission, ordinarily used for step-counting and workout-detection features, feeds directly into the advertising SDK stack rather than remaining scoped to fitness-tracking functionality.

No response was received naming this finding, including the direct yes/no question of whether this use has been assessed under GDPR Art. 9(1) given its adjacency to health-inference data on a fitness platform.

**Impact:** Physical activity data, collected under a fitness-tracking justification, is repurposed for advertising without a documented Art. 9 assessment.

**Fix:** Scope ACTIVITY_RECOGNITION data to on-device fitness features only, or obtain specific consent before any advertising use.

### H2: Adjust SDK: undisclosed install attribution

**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**

The Adjust SDK performs install attribution across the shared framework, undisclosed in any of the five apps' privacy policies.

No response was received naming this finding.

**Impact:** Install-level attribution data is collected and shared with Adjust without disclosure to users.

**Fix:** Disclose Adjust as a data recipient under Art. 13(1)(e) across all five apps.

### H3: No EU Art. 27 representative identified for a developer distributing to EU users

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L, 5.1**

No EU-based Article 27 representative could be identified for this developer across any public listing, privacy policy, or the developer's sole reachable contact channel, support@leap.app.

No response was received naming this finding. GDPR Art. 27 requires a non-EU controller offering goods or services to EU data subjects to designate an EU representative in writing; absent one, EU data subjects and supervisory authorities have no designated point of contact independent of the controller itself, which itself proved unreachable for any substantive purpose across eight written notices.

**Impact:** EU users and supervisory authorities have no designated Art. 27 representative to contact independent of a developer that did not respond to any of eight written notices over 91 days.

**Fix:** Designate and publish an EU Art. 27 representative across all five apps' privacy policies.

## Data Protection, Article by Article

| Finding | Provision | Concern |
|---|---|---|
| C1, H2 | GDPR Art. 13(1)(e) | Undisclosed third-party data recipients (Facebook Audience Network, Adjust) across all five apps |
| C2 | GDPR Art. 44-49 | Undisclosed routing to Chinese ad infrastructure with no transfer safeguard |
| C3 | GDPR Art. 32 | Five separate exposed backend credentials |
| H1 | GDPR Art. 9(1) | Fitness-tracking permission repurposed for advertising with no documented assessment |
| H3 | GDPR Art. 27 | No EU representative designated for a non-EU controller serving EU users |

## Disclosure Timeline & Outcome

| Date | Event |
|---|---|
| 2026-06-22 | R1 sent to support@leap.app, covering all five apps under the shared tracking template |
| 2026-07-17 / 07-27 | Follow-ups, no response of any kind |
| 2026-08-09 (twice) / 08-18 | Continued follow-ups, no response |
| 2026-09-04 | 76-day follow-up, three questions restated, deadline 11 September 2026 |
| 2026-09-12 | 11 September deadline passed; three questions restated again, deadline 16 September 2026 |
| 2026-09-16 | 16 September deadline reached; final notice, three days before embargo |
| 2026-09-19 | Embargo closes; this report publishes |

Eight written notices across 91 days produced no substantive reply, acknowledgment, automated ticket, or bounce, a rarer pattern than pure silence with at least an automated response,

since even a ticketing system never engaged. All six findings across five apps stand exactly as originally reported.

### Residual Risk & Recommendations

- Disclose Facebook Audience Network and Adjust as data recipients under Art. 13(1)(e) across all five apps.
- Remove Pangle or implement and disclose a verified Art. 44-49 transfer mechanism.
- Rotate all five exposed Firebase credentials.
- Scope ACTIVITY_RECOGNITION data away from the advertising stack absent a documented Art. 9 assessment.
- Designate and publish an EU Art. 27 representative across the portfolio.
- Establish a reachable privacy or security contact beyond the single generic support inbox.

**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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 9, 13, 27, 32, 44-49. REF LEAP-FITNESS-BUNDLE-2026-R1.