Coordinated Security & Privacy Disclosure, Final Report

Pokemon GO for Android (com.nianticlabs.pokemongo, v0.415.2)

Ten written notices, ninety-one days, four identical automated ticket acknowledgements, zero human replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL EIGHT FINDINGS UNADDRESSED AFTER TEN NOTICES, ZERO HUMAN REPLY

Target	Niantic, Inc., San Francisco, USA – control chain: Scopely, Inc. / Savvy Games Group / Saudi Public Investment Fund
Product audited	Pokemon GO for Android, com.nianticlabs.pokemongo, v0.415.2 (versionCode 2026061202)
Disclosure reference	REF POKEMONGO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C2 GeoUploader/Titan.Uploader undisclosed defense-contractor downstream use, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Pokemon GO Android application and identified two CRITICAL and six HIGH findings: a Firebase project key hardcoded in a distributed asset file, an undisclosed downstream data pipeline (GeoUploader/Titan.Uploader) whose recipient list was found to include Vantor, a US defense contractor holding an NGA contract, persistent background GPS collection through the Adventure Sync feature, a bundled Facebook SDK and a 420-class AppsFlyer ad-attribution stack absent a documented lawful basis, non-consenting third-party contact processing through an address-book import feature, an anomalous privileged telephony permission, and a Google Fit health-data integration framed only as an in-game egg-hatching mechanic.

Across ten written notices over ninety-one days, cc'd across the sequence to the Austrian DSB, CERT.at, and the Irish Data Protection Commission, the only inbound correspondence in this case was four identical automated ticketing-system acknowledgements from two support addresses, each quoting the sender's own message back in full. Three of the five originally-tried recipient addresses (security@, legal-privacy@, info@nianticlabs.com) bounced as nonexistent, and the cc address niantic@lionheartsquared.eu bounced on every attempt across the sequence. No named Data Protection Officer was ever identified, and none of RFI-IRFOS's six standing questions, on Vantor licensing, Art. 5(1)(b) purpose disclosure, internal DPO awareness given the dead security@ address, the legal basis for the GeoUploader/Titan transfer, COPPA-relevant pre-consent collection, or Art. 33 notification to the lead supervisory authority, ever received a reply.

A separate, distinct thread concerning Pokemon Champions (jp.pokemon.pokemonchampions, published by The Pokemon Company, not Niantic) was opened on 25 June 2026 under its own reference and carries its own later embargo of 23 September 2026. That case is not yet due and is not covered by this report; it will be reported separately on its own embargo date.

Scope: Static analysis of the publicly downloaded production Pokemon GO Android APK (v0.415.2), on an authorized test device, only. No Niantic account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to security@nianticlabs.com (bounced), legal@nianticlabs.com, legal-privacy@nianticlabs.com (bounced), info@nianticlabs.com (bounced), and privacy@nianticlabs.com, cc press@nianticlabs.com and niantic@lionheartsquared.eu (bounced on every attempt), bcc/cc across the sequence to the Austrian DSB, CERT.at, and the Irish Data Protection Commission. Across ten written notices over ninety-one days, the only inbound correspondence of any kind was four identical automated ticketing-system acknowledgements from two support addresses. No named Art. 37 DPO, no substantive reply, and no acknowledgment of any finding was ever received.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in a distributed APK asset file

ID	Severity	Title
C2	CRITICAL	GeoUploader / Titan.Uploader pipeline – undisclosed downstream defense-contractor use of civilian geospatial data
H1	HIGH	Adventure Sync – persistent background GPS tracking when the app is closed
H2	HIGH	Facebook SDK (three assemblies) bundled without a documented lawful basis
H3	HIGH	AppsFlyer (420 classes) and Privacy Sandbox custom-audience permissions – ad attribution absent a documented lawful basis
H4	HIGH	Address Book Import – processing of non-consenting third parties
H5	HIGH	READ_PRIVILEGED_PHONE_STATE – anomalous privileged permission
H6	HIGH	FOREGROUND_SERVICE_HEALTH and Google Fit integration – health data framed as a game mechanic

Subject & Operator Analysis

Pokemon GO is developed and operated by Niantic, Inc., San Francisco, USA. Following the March 2025 acquisition described in RFI-IRFOS's correspondence, Niantic's games division sits under Scopely, Inc., itself owned by Savvy Games Group, a subsidiary of the Saudi Public Investment Fund. The GeoUploader/Titan.Uploader finding (C2) concerns processing that predates and continues independently of that ownership change.

Findings

C1: Firebase API key hardcoded in a distributed APK asset file

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

Plaintext Firebase credential in assets/google-services-desktop.json shipped in every distributed APK: API key AIzaSyB5tOqHEH2QrGnSGxmj5ai9o7z_umdLjoo, project_id prodholoholo, database_url https://prodholoholo.firebaseio.com, storage prodholoholo.appspot.com.

No reply of any kind, substantive or otherwise, addressed this finding across ten notices.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm Firestore/RTDB security rules are deny-by-default, and enforce App Check for this project.

C2: GeoUploader / Titan.Uploader pipeline – undisclosed downstream defense-contractor use of civilian geospatial data

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

The APK ships Niantic.Lightship.GeoUploader.dll, Niantic.Titan.Uploader.dll, Niantic.Titan.GeoClient*.dll, and Niantic.Lightship.AR.dll (Visual Positioning System). In-app consent text describes processing only as occurring 'during your AR session' and does not name Vantor, a US defense contractor holding an NGA (National Geospatial-Intelligence Agency) contract, as a downstream recipient, does not disclose player-captured photogrammetry contributing to drone-navigation model training, and does not disclose the Scopely / Savvy Games Group / Saudi Public Investment Fund control chain.

This finding concerns disclosure, not the legality of the underlying commercial arrangement: RFI-IRFOS asked six times whether this secondary use is licensed, whether it is disclosed to EU players as a specific processing purpose distinct from 'improving our services,' and whether the lead supervisory authority has been notified. No reply of any kind answered any of these questions.

Impact: Civilian AR-session geospatial data captured by consumer players may be repurposed for defense-adjacent model training without a matching Art. 13(1)(e) disclosure of the recipient or purpose.

Fix: Name Vantor explicitly as a downstream recipient with the applicable legal basis and transfer mechanism, or discontinue the transfer pending disclosure.

H1: Adventure Sync – persistent background GPS tracking when the app is closed

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

AdventureSync.Android.dll, nia-advsync-location.dll, LocationForegroundService, GeofenceController, and UpdateBulkPlayerLocationResponseProto, combined with ACCESS_BACKGROUND_LOCATION, FOREGROUND_SERVICE_LOCATION, and ACTIVITY_RECOGNITION permissions, enable continuous background location reporting for the egg-hatching game mechanic.

No reply of any kind addressed this finding.

Impact: Players opting into a single game mechanic are enrolled in continuous background location collection with no independent minimization boundary observed.

Fix: Bound Adventure Sync's background collection to the minimum sampling interval the mechanic requires, and document the retention period separately from other location processing.

H2: Facebook SDK (three assemblies) bundled without a documented lawful basis

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

Facebook.Unity.dll, Facebook.Unity.Android.dll, and Facebook.Unity.Settings.dll are present and capable of social-graph construction and shadow profiling; Meta Platforms, Inc. is not disclosed as a named recipient with an applicable transfer safeguard.

No reply of any kind addressed this finding.

Impact: Social-graph data may be constructed and transferred to a third party without a documented Art. 13(1)(e)/(f) basis covering that specific recipient.

Fix: Name Meta Platforms, Inc. explicitly as a processor or recipient with the applicable legal basis and transfer mechanism, or remove the SDK if unused.

H3: AppsFlyer (420 classes) and Privacy Sandbox custom-audience permissions – ad attribution absent a documented lawful basis

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

420 smali classes from com.appsflyer, combined with the ACCESS_ADSERVICES_CUSTOM_AUDIENCE and ACCESS_ADSERVICES_TOPICS permissions, enable ad-attribution profiling with no documented consent mechanism found in the binary.

No reply of any kind addressed this finding.

Impact: Ad-attribution profiling operates without a demonstrable lawful-basis consent gate.

Fix: Deploy a recognized consent-management platform gating AppsFlyer and Privacy Sandbox attribution collection.

H4: Address Book Import – processing of non-consenting third parties

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

AddressBookImport.dll, Niantic.Platform.AddressBookImport.Android.dll, and the READ_CONTACTS permission process contact data belonging to non-users, with no consent flow for those third parties observed in the binary.

No reply of any kind addressed this finding.

Impact: Personal data of individuals who never installed or agreed to Pokemon GO's terms may be processed without a lawful basis specific to them.

Fix: Restrict address-book processing to on-device matching that never transmits non-user contact data off-device, or obtain a documented basis covering non-users specifically.

H5: READ_PRIVILEGED_PHONE_STATE – anomalous privileged permission

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 declared READ_PRIVILEGED_PHONE_STATE permission normally requires OEM or system-level privilege and grants access to SIM serial, IMEI, and telephony state beyond what a consumer application ordinarily needs.

No reply of any kind addressed this finding.

Impact: Device-identifying telephony data may be collected beyond the minimum needed for the app's stated purpose.

Fix: Remove the privileged permission declaration unless a specific, documented feature requires it, and disclose that feature if retained.

H6: FOREGROUND_SERVICE_HEALTH and Google Fit integration – health data framed as a game mechanic

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

nia-advsync-fitness.dll and a GoogleFitWorker class, combined with the FOREGROUND_SERVICE_HEALTH permission, continuously synchronize step counts and activity-recognition data from Google Fit. The consent interface frames this exclusively as an egg-hatching mechanic, not as Art. 9 special-category health data processing.

No reply of any kind addressed this finding.

Impact: Special-category health data may be processed under a general game-mechanic consent rather than the explicit consent Art. 9 requires.

Fix: Present a distinct, explicit consent flow naming Google Fit and the health-data category before enabling the fitness-sync mechanic.

Ten Notices, Four Automated Acknowledgements, Zero Humans

The only inbound correspondence this case ever produced was four identical automated ticketing-system acknowledgements from two support addresses (legal@support.nianticlabs.com, privacy@support.nianticlabs.com), each quoting RFI-IRFOS's own message back in full. No named Data Protection Officer was ever identified. Three of the five originally-tried recipient addresses bounced outright as nonexistent, and the cc address niantic@lionheartsquared.eu bounced on every attempt across the sequence. Ten notices over ninety-one days produced no human reply of any kind.

A Related, Separately-Timed Case: Pokemon Champions

A separate thread concerning Pokemon Champions (jp.pokemon.pokemonchampions), published by The Pokemon Company rather than Niantic, was opened on 25 June 2026 under REF POKEMONCHAMPIONS-2026-R1 and carries its own embargo of 23 September 2026, not yet due. Both primary addresses used for that case, privacy@pokemon.co.jp and press@pokemon.co.jp, bounced, and no reply of any kind was ever received on that thread either. It will be reported on its own embargo date rather than folded into this one.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key in every distributed APK
C2	GDPR Art. 5(1)(b), Art. 13(1)(a), Art. 13(1)(e)	Undisclosed defense-contractor downstream recipient for civilian geospatial data
H1	GDPR Art. 5(1)(b)(c)	Persistent background location collection for a single game mechanic
H2	GDPR Art. 8, Art. 13(1)(e)(f)	Undisclosed social-graph SDK recipient
H3	GDPR Art. 8, ePrivacy Directive	Ad-attribution profiling absent a documented consent mechanism
H4	GDPR Art. 6(1), Art. 13	Non-consenting third-party contact data processing
H5	GDPR Art. 5(1)(c)	Anomalous privileged telephony permission
H6	GDPR Art. 9	Health data processed under a general game-mechanic consent

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@nianticlabs.com (bounced), legal@, legal-privacy@ (bounced), info@ (bounced), privacy@nianticlabs.com, bcc Austrian DSB/CERT.at/Irish DPC; 2 CRITICAL + 6 HIGH findings; under the R1 policy then in force, a EUR 75,000 NDA remediation engagement was offered as an alternative to public disclosure – historical record only, not a currently open offer
2026-06-27	Follow-up resent; legal-privacy@ and info@ bounced outright; automated ticket ack #41975782 from legal@support.nianticlabs.com
2026-07-17	First message reaching a working address, privacy@nianticlabs.com, after 27 days of silence; automated ticket ack #42586502
2026-07-27	Day-10 follow-up restating three yes/no questions on Vantor licensing and internal DPO awareness; automated ticket ack #42794595
2026-08-18	Follow-up sets deadline of 25 August 2026, cc press@ and niantic@lionheartsquared.eu (bounced); automated ticket ack #43241160
2026-09-06	'Three Dead Addresses, Two Ticket Numbers, Zero Humans, 41 Days of Silence' – full chronology restated, new deadline 13 September 2026, staged Art. 33(4) regulatory notification referenced as available
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name an Art. 37 Data Protection Officer and a functional escalation path beyond a ticketing system that auto-acknowledges and never routes to a human.
- Name Vantor explicitly as a downstream recipient of GeoUploader/Titan-collected geospatial data, with the applicable legal basis and transfer mechanism, or discontinue the transfer.
- Deploy a consent-management platform gating AppsFlyer, Privacy Sandbox, and Facebook SDK data collection.
- Present a distinct, explicit Art. 9 consent flow before enabling the Google Fit fitness-sync mechanic.
- Rotate the exposed Firebase key and confirm deny-by-default security rules with App Check enforced.

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, 8, 9, 13, 25, 32. REF POKEMONGO-2026-R1.