# Coordinated Privacy Disclosure, Final Report

## ChatGPT Android (com.openai.chatgpt)

OpenAI, San Francisco, California, USA

**SILENT ON SUBSTANCE · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 89 DAYS AFTER DISCLOSURE, FOUR SUPPORT CASE NUMBERS, ZERO SUBSTANTIVE REPLY, ONE WRITTEN ADMISSION**

| | |
|---|---|
| **Target** | ChatGPT for Android, OpenAI's consumer AI assistant application |
| **Package** | com.openai.chatgpt |
| **Operator** | OpenAI, San Francisco, California, USA |
| **Initial Disclosure** | 2026-06-28 |
| **Original Embargo** | 2026-09-24 (90 days from disclosure, as stated in the original notice) |
| **Report Published** | 2026-09-25, one day after the embargo, an internal publishing gap, not a change in terms |
| **Regulators in BCC** | Austrian DSB, CERT.at |
| **Total Outbound Messages** | 7+, across 89 days, cycling through four distinct OpenAI support case numbers (10550708, 12912668, 13070657, 13694445) |
| **Inbound Replies** | Multiple automated support-queue replies and two auto-closures via customer-satisfaction survey. One reply, in a Support Summary auto-generated on case 10550708, contained a written admission: "Your Android app initializes tracking and analytics before users can provide consent." No reply from a human privacy, legal, or DPO function was ever received. |

rfi.irfos@gmail.com • rfi-irfos.com

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

## Contents

## Executive Summary

On 28 June 2026, RFI-IRFOS disclosed to OpenAI that ChatGPT for Android initializes Firebase analytics via a directBootAware ContentProvider before any consent screen can render, processes biometric identity-verification data (facial liveness and document scanning) through the Persona SDK with no disclosed Art. 9(2) legal basis, routes conversation-adjacent data to Segment, monitors when a user takes a screenshot via an onScreenCaptured callback, and integrates Plaid Link for financial account access alongside a READ_CONTACTS permission, none of the latter three disclosed under Art. 13(1)(e).

What makes this case unusual in this campaign is not the findings themselves, comparable pre-consent and undisclosed-recipient patterns recur across dozens of targets, but the correspondence record. On 30 June 2026, an OpenAI automated support system generated a case summary whose first bullet point read, verbatim: "Your Android app initializes tracking and analytics before users can provide consent." That is not RFI-IRFOS's characterization of the finding. That is OpenAI's own system, in writing, confirming it. Under GDPR Art. 83(2)(b), an organization's documented awareness of an infringement is an aggravating factor in determining any subsequent fine, and this is now part of the written record regardless of what OpenAI's privacy or legal function does or does not say afterward.

Across 89 days, correspondence cycled through four distinct OpenAI support case numbers (10550708, 12912668, 13070657, 13694445), each producing automated ticket-routing replies, and twice auto-closed via a customer-satisfaction survey asking whether the support experience was easy, not whether the underlying findings were addressed. A reply on case 13694445 dated 14 September 2026 explicitly declined to confirm or deny that the Firebase, Persona, Segment, or screen-capture behaviors described occurred as alleged, while providing no technical rebuttal of any kind. No reply from a human privacy, legal, or Data Protection Officer function was ever received. The 90-day embargo, set at first contact, elapsed on 24 September 2026. This report and the accompanying closure notice publish one day later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

**Scope:** Root-level static analysis of the production ChatGPT Android application (com.openai.chatgpt, version 1.2026.167), covering the AndroidManifest, resource strings, and decompiled dex/smali, as pulled and reviewed on 28 June 2026. No dynamic instrumentation, live traffic capture, or interaction with OpenAI's backend infrastructure was performed.

**Disposition**

Five findings were disclosed on 28 June 2026, later re-scored under CVSS v4.0. One finding, Persona biometric identity verification processed with no disclosed Art. 9(2) legal basis, reaches HIGH on the computed CVSS score alone, no editorial escalation applied or needed. A second finding, Firebase analytics initializing before any consent screen can appear, is held at HIGH under an explicit, stated blast-radius escalation, not primarily for scale, though ChatGPT's user base is counted in the hundreds of millions, but because OpenAI's own automated support system produced, in writing, the sentence "Your Android app initializes tracking and analytics before users can provide consent," a documented admission that under GDPR Art. 83(2)(b) constitutes an aggravating factor in its own right. Three further findings, undisclosed Segment analytics routing, screen-capture monitoring, and undisclosed Plaid financial-account-linking plus contacts access, correct to or remain at MEDIUM. Across 89 days and four separate support case numbers, the only written engagement with the substance of any finding was that one admission, produced by an automated system, never followed up on by a human.

| ID | Severity | Title |
|---|---|---|
| C1 | HIGH | Firebase Analytics Initializes Before Any Consent Screen, a Fact OpenAI's Own Support System Confirmed in Writing |
| H1 | MEDIUM | Undisclosed Segment Analytics Pipeline on Conversation-Adjacent Data |
| H2 | HIGH | Persona Biometric Identity Verification, No Disclosed Art. 9(2) Legal Basis |
| H3 | MEDIUM | Screen Capture Monitoring via onScreenCaptured, No Disclosed Purpose or Legal Basis |
| H4 | MEDIUM | Plaid Link Financial Account Integration and READ_CONTACTS, No Art. 13 Disclosure |

## Subject & Operator Analysis

ChatGPT for Android is OpenAI's consumer AI assistant application, with a user base counted in the hundreds of millions. RFI-IRFOS disclosed five findings on 28 June 2026 and pursued the case across 89 days and four separate OpenAI support case numbers.

A genuine positive is worth naming plainly: OpenAI's automated support system, whatever the limitations of an AI-generated case summary as a substitute for human review, produced a factually accurate, unprompted, and specific admission on the central finding in this case (C1), one clearer and more direct than most human-drafted responses RFI-IRFOS has received across this entire campaign. That accuracy is credited here even though no human function ever followed up on it.

## Four Case Numbers, One Written Admission, Zero Human Engagement

This case's correspondence record cycled through four distinct OpenAI support case numbers (10550708, 12912668, 13070657, 13694445) across 89 days, each generating automated ticket-routing replies, and was auto-closed via a customer-satisfaction survey on at least two occasions, a survey asking whether the support experience was easy to use, not whether the underlying GDPR findings had been addressed. A reply on the final case number, dated 14 September 2026, explicitly declined to confirm or deny that the specific Firebase, Persona, Segment, or screen-capture behaviors described had occurred as alleged, providing no technical rebuttal of any kind in either direction. At no point across 89 days did a reply arrive from a human privacy, legal, or Data Protection Officer function.

## Findings

### C1: Firebase Analytics Initializes Before Any Consent Screen, a Fact OpenAI's Own Support System Confirmed in Writing

**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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because OpenAI's own automated support system produced, in writing, the sentence "Your Android app initializes tracking and analytics before users can provide consent," a documented admission that under GDPR Art. 83(2)(b) is itself an aggravating factor, on an application with a user base in the hundreds of millions.**

FirebaseInitProvider is declared with android:directBootAware="true" in the public APK manifest, meaning it initializes before any Activity, and therefore before any consent screen, can render. On 30 June 2026, an OpenAI automated support system (case 10550708) generated a Support Summary whose first bullet read, verbatim: "Your Android app initializes tracking and analytics before users can provide consent." This is not RFI-IRFOS's interpretation of the finding, it is OpenAI's own system stating the underlying fact directly. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because this written admission constitutes a documented awareness of the infringement, an Art. 83(2)(b) aggravating factor in its own right, on an application with a user base in the hundreds of millions.

```
AndroidManifest.xml
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
    android:directBootAware="true" android:exported="false"/>

OpenAI automated Support Summary, case 10550708, 30 June 2026 (verbatim):
"Your Android app initializes tracking and analytics before users can
provide consent."
```

**Impact:** App-open telemetry begins for every user before they have seen a single privacy notice, a fact OpenAI's own support infrastructure has independently confirmed, not merely something RFI-IRFOS alleges.

**Fix:** Defer FirebaseInitProvider's initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

### H1: Undisclosed Segment Analytics Pipeline on Conversation-Adjacent Data

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

The Segment (Twilio) analytics SDK is present and routes conversation-adjacent behavioral data, session events, feature usage, timing patterns around actual chat sessions, to a third-party analytics processor. Segment is not individually named as a data recipient with a stated Art. 28 processing basis in OpenAI's privacy documentation reviewed for this disclosure.

**Impact:** Behavioral data adjacent to a user's actual conversations with the model is routed to a named third-party analytics processor without individual disclosure of that specific data flow.

**Fix:** Name Segment individually as a data recipient with a stated Art. 28 processing basis and Art. 13(1)(e) disclosure. No confirmation that this has occurred was ever received.

### H2: Persona Biometric Identity Verification, No Disclosed Art. 9(2) Legal 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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.**

The Persona identity-verification SDK is integrated, providing facial liveness detection and government-document scanning, special category biometric data under GDPR Art. 9(1) when processed for the purpose of uniquely identifying a person. No Art. 9(2) legal basis for this specific processing, and no confirmation of an Art. 35 Data Protection Impact Assessment, was located in OpenAI's privacy documentation as reviewed, nor was one provided across 89 days and four support case numbers.

**Impact:** Facial biometric and government-identity-document data, among the most sensitive categories of personal data under GDPR, is processed through a named third-party SDK with no disclosed lawful basis specific to that processing.

**Fix:** Document an Art. 9(2) legal basis and, if not already completed, an Art. 35 DPIA for the Persona identity-verification flow specifically. No confirmation that this has occurred was ever received.

### H3: Screen Capture Monitoring via onScreenCaptured, No Disclosed Purpose or Legal Basis

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

The binary confirms an onScreenCaptured callback, monitoring when a user takes a screenshot within the app. No disclosed purpose, Art. 6(1) legal basis, or user-facing notice for this monitoring was located in OpenAI's privacy documentation as reviewed.

**Impact:** A user's decision to screenshot a conversation, itself potentially revealing what content they found notable enough to capture, is monitored by the app with no disclosed purpose or legal basis for that specific signal.

**Fix:** Disclose the purpose and legal basis for screen-capture monitoring, or remove the callback if it serves no disclosed product function. No confirmation that this has occurred was ever received.

### H4: Plaid Link Financial Account Integration and READ_CONTACTS, No Art. 13 Disclosure

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

Plaid Link, a financial account-linking SDK, and the READ_CONTACTS permission are both present in the binary. Neither the specific purpose of the financial-account integration nor the contacts access is individually disclosed under Art. 13(1)(e) in the privacy documentation reviewed for this disclosure.

**Impact:** Financial account-linking capability and contact-list access both exist in a general-purpose AI assistant application with no individually disclosed purpose for either, in a product context where neither function is self-evidently necessary for the app's stated purpose.

**Fix:** Disclose the specific purpose and legal basis for the Plaid Link integration and the READ_CONTACTS permission individually under Art. 13(1)(e), or remove either if not load-bearing for a documented feature. No confirmation that this has occurred was ever received.

## Impact Analysis

C1 and H2 are the two findings that reach HIGH severity, and they reach it by different routes: H2 reaches HIGH purely on its computed CVSS v4.0 score, biometric identity data with no disclosed legal basis is serious on its technical merits alone. C1 reaches HIGH through an explicit blast-radius escalation grounded specifically in OpenAI's own written admission, a category of evidence CVSS's technical vector was never built to weigh, but GDPR Art. 83(2)(b) treats as an aggravating factor in its own right.

## Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

| Article | Finding | Basis |
|---|---|---|
| Art. 6(1), Art. 7(1), Art. 83(2)(b) | C1 | Pre-consent SDK initialization, with a documented written admission constituting an aggravating factor. |
| Art. 13(1)(e), Art. 28 | H1 | Undisclosed third-party analytics recipient on conversation-adjacent data. |
| Art. 9(1), Art. 9(2), Art. 35 | H2 | Biometric identity-verification data, no disclosed legal basis or confirmed DPIA. |
| Art. 6(1), Art. 5(1)(b) | H3 | Undisclosed screen-capture monitoring, no stated purpose or legal basis. |
| Art. 13(1)(e) | H4 | Undisclosed financial-account integration and contacts access. |

**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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, C1 is escalated from MEDIUM/6.9 to HIGH specifically because the target's own written support-system output independently confirmed the

finding, a real-world circumstance CVSS's technical vector does not capture; H2 reaches HIGH on its computed score alone. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF #CGPT-2026-001.