Coordinated Security & Privacy Disclosure, Final Report

Flo Period & Pregnancy Tracker for Android (org.iggymedia.periodtracker)

A legal letter disputing one finding of five, citing a letter RFI-IRFOS never sent, then ten weeks of silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – EIGHTY-NINE DAYS, ONE FINDING ANSWERED OF FIVE, TEN WEEKS OF SILENCE SINCE

Target	Flo Health Ltd., United Kingdom
Product audited	Flo Period & Pregnancy Tracker for Android, org.iggymedia.periodtracker
Disclosure reference	REF FLO-C1-R1
R1 sent	2026-06-22
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 TikTok SDK / C2 Facebook SDK, CVSS v4.0 8.7)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Positive Observations 4

4 Findings 4

4.1 C1: TikTok Business SDK active alongside menstrual and sexual-activity Health Connect permissions 4

4.2 C2: Facebook SDK active in the same binary the 2021 FTC consent order specifically addressed 5

4.3 H1: Oura Ring OAuth integration alongside 29 total Health Connect permissions 5

4.4 H2: DETECT_SCREEN_CAPTURE implemented with no stated purpose on a fertility-tracking app 6

4.5 H3: Hardcoded Firebase key, mParticle routing to AppsFlyer, zero certificate pinning on any domain 6

5 Flo's Response, Recorded in Full 7

6 Data Protection, Article by Article 7

7 Disclosure Timeline & Outcome 8

8 Residual Risk & Recommendations 9

Executive Summary

On 22 June 2026, RFI-IRFOS performed static analysis of the production Flo Health Android application, a menstrual and fertility tracking app reporting over 370 million downloads, and identified five findings, two CRITICAL, three HIGH. The most significant: a compiled TikTok Business SDK operates alongside Health Connect permissions covering menstruation, sexual activity, ovulation, cervical mucus, and basal body temperature, whether the app's consent state propagates to the SDK layer or only to the event-sending layer could not be confirmed from static analysis alone, and ByteDance's exposure to China's National Intelligence Law compounds the transfer question.

Separately, a Facebook SDK (214 classes) remains active in the same binary that Flo Health's own 2021 US FTC consent order specifically addressed, concerning health data shared with Facebook and Google for advertising despite the company's privacy policy stating otherwise. Three further findings raise separate concerns: Oura Ring OAuth integration alongside 29 total Health Connect permissions, an unusually broad aggregation of health signals; a screenshot-detection permission with no stated purpose on a fertility-tracking app; and a hardcoded Firebase key with zero certificate pinning on any domain, securing the consent-synchronization channel for Art. 9 special-category data.

Nine written notices were sent over 89 days. A Zendesk reply declined engagement without technical content. Flo's Privacy Counsel then sent a formal legal letter addressing only the TikTok finding, citing a letter RFI-IRFOS never sent, and citing ISO certification and an unnamed external security firm as evidence without providing either. The other four findings were never addressed, and no reply of any kind followed across five further written notices and ten weeks through the close of the embargo.

Scope: Static analysis of the publicly downloaded production Flo Health Android APK, on an authorized test device, only. No Flo account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 22 June 2026 to privacy@flo.health, security@flo.health, and dpo@flo.health, cc the UK ICO as Flo's lead supervisory authority and the Austrian DSB. A Zendesk support reply on 27 June declined engagement without addressing any finding. Flo's Privacy Counsel sent a formal legal letter on 8 July disputing only the report's TikTok finding, citing a 29 June letter RFI-IRFOS never sent, and leaving the other four findings, including a Facebook SDK the company's own 2021 FTC consent order specifically addressed, entirely unaddressed. No further reply of any kind was received across five subsequent written notices and ten weeks.

ID	Severity	Title
C1	CRITICAL	TikTok Business SDK active alongside menstrual and sexual-activity Health Connect permissions
C2	CRITICAL	Facebook SDK active in the same binary the 2021 FTC consent order specifically addressed

ID	Severity	Title
H1	HIGH	Oura Ring OAuth integration alongside 29 total Health Connect permissions
H2	HIGH	DETECT_SCREEN_CAPTURE implemented with no stated purpose on a fertility-tracking app
H3	HIGH	Hardcoded Firebase key, mParticle routing to AppsFlyer, zero certificate pinning on any domain

Subject & Operator Analysis

Flo Health Ltd. (United Kingdom) operates a menstrual and fertility tracking application reporting over 370 million downloads globally, with the UK ICO as lead GDPR supervisory authority and subject to a 2021 US FTC consent order concerning health data sharing with Facebook and Google.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: TikTok Business SDK active alongside menstrual and sexual-activity Health Connect permissions

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

com.tiktok.TikTokBusinessSdk and related event-tracking classes, including a persistent cross-session anonymous identifier, are compiled into the same binary declaring READ_MENSTRUATION, READ_SEXUAL_ACTIVITY, WRITE_SEXUAL_ACTIVITY, READ_OVULATION_TEST, READ_CERVICAL_MUCUS, and READ_BASAL_BODY_TEMPERATURE.

The disputed question, verbatim from R1: whether Flo's consent infrastructure correctly propagates opt-out state to the TikTok SDK at the SDK layer, rather than merely at the event-sending layer, cannot be verified from static analysis alone. ByteDance is subject to China's National Intelligence Law (2017) and Data Security Law (2021), with no GDPR Art. 45 adequacy decision for China. Flo's 8 July legal letter stated its own testing "strongly refutes the assertion that sensitive health-related data is transmitted via Flo's TikTok SDK," citing ISO 27001, ISO 27701 certification and an unnamed "accredited external security firm." Neither the security firm's name nor its report was provided despite five repeated requests through 4 September.

Impact: Special-category menstrual, sexual-activity, and reproductive health data may reach a PRC-exposed advertising SDK, with the disputed consent-propagation question left unresolved by evidence neither party could independently verify.

Fix: Name the external security firm and provide its report, or publish the specific technical mechanism confirming consent state is enforced at the SDK layer, not only the event-sending layer.

C2: Facebook SDK active in the same binary the 2021 FTC consent order specifically addressed

---

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

214 Facebook SDK classes, Facebook App ID 2278022672520157, remain compiled into the production binary.

Flo Health's 2021 FTC consent order specifically concerned sharing health data with Facebook and Google for advertising despite the privacy policy stating otherwise. This finding was never confirmed or disputed by Flo; the 8 July legal letter addressed only the TikTok finding above and left this finding, and all three HIGH findings below, entirely unaddressed.

Impact: An advertising SDK named specifically in the company's own prior FTC consent order remains active in the current production binary, with no response confirming or disputing its current data-sharing configuration.

Fix: Confirm the Facebook SDK's current data-sharing configuration and its compliance with the 2021 FTC consent order's terms, in writing.

H1: Oura Ring OAuth integration alongside 29 total Health Connect permissions

---

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

An OAuth module connects to Oura Ring wearables, alongside 29 total declared Health Connect permissions spanning menstruation, sexual activity, sleep, heart rate variability, and body weight.

Not confirmed or disputed by Flo despite repeated requests for a documented Art. 35 DPIA covering the Oura Ring integration specifically.

Impact: An unusually broad aggregation of health signals across 29 permission categories operates with no confirmed DPIA specific to the wearable-device integration.

Fix: Publish the Art. 35 DPIA covering the Oura Ring integration and the full scope of Health Connect data it can access.

H2: DETECT_SCREEN_CAPTURE implemented with no stated purpose on a fertility-tracking app

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

android.permission.DETECT_SCREEN_CAPTURE is implemented, notifying the app whenever a user screenshots while it is foregrounded.

Not confirmed or disputed by Flo. RFI-IRFOS's framing, verbatim: why does Flo need to know when a user screenshots their own menstrual data, their own cycle predictions, their own sexual activity records?

Impact: Screenshot behavior on menstrual, cycle, and sexual-activity data screens is monitored with no disclosed purpose.

Fix: Disclose the specific purpose of screenshot detection or remove the permission.

H3: Hardcoded Firebase key, mParticle routing to AppsFlyer, zero certificate pinning on any domain

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

A hardcoded Firebase API key is extracted from the production binary. mParticle's AppsFlyerKit routes health signals to AppsFlyer. cleartextTrafficPermitted is set to false, but no certificate pins are configured for any domain, including the Firebase channel through which consent state for Art. 9 special-category data is synchronized.

```
google_api_key:  AIzaSyAkPZESterELxrlGkfBpx9dVQCH7L0Q0U4
google_app_id:   1:154016399017:android:fdc758dd051ecb9740b3b8
```

Not confirmed or disputed by Flo. Consent-sync architecture routes through Firebase, meaning the consent state for special-category health data depends on a third-party connection with zero certificate pinning.

Impact: The channel synchronizing consent state for special-category health data has no certificate pinning, and health signals are routed to an additional undisclosed attribution recipient via mParticle.

Fix: Rotate the Firebase key, implement certificate pinning for the consent-sync channel specifically, and disclose AppsFlyer as a recipient of health-adjacent signals via mParticle.

Flo’s Response, Recorded in Full

On 27 June 2026, a Zendesk support reply signed ”Kate” stated, in full: ”Having reviewed the technical points of your preliminary review, we remain satisfied that our operation of SDKs meet legal and compliance requirements. We therefore do not agree with your suggested conclusions. While we appreciate your interest and the services you have offered, we do not require external consultancy services in relation to the matters raised.” This addressed no specific finding.

On 8 July 2026, Alexandre Rajagopalan, Privacy Counsel, sent Flo’s only formal reply, a covering email attaching a legal letter. The letter opened by referencing ”your correspondence dated 22 June and 29 June 2026”, RFI-IRFOS sent nothing on 29 June, a citation to correspondence that does not exist. The letter’s substantive content, as quoted in RFI-IRFOS’s own same-day rebuttal: ”our own testing… strongly refutes the assertion that sensitive health-related data is transmitted via Flo’s TikTok SDK,” citing ISO 27001, ISO 27701 certification and an unnamed ”accredited external security firm” whose name and report were never subsequently provided despite five repeated requests. The letter characterized the disclosure, alongside RFI-IRFOS’s standard optional paid-engagement tier and its regulator CC practice, as using ”the regulatory process” as ”commercial leverage,” and argued that publishing the findings risks ”deterring people from tools that support their wellbeing, which is a real harm.” The letter addressed only the TikTok finding; the Facebook SDK finding, specifically implicated in Flo’s own 2021 FTC consent order, and all three HIGH findings, were not mentioned.

No reply of any kind was received from Flo Health after 8 July 2026, across five subsequent written notices and ten weeks through the close of the embargo.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 9(1), Art. 5(1)(b), Art. 44	Disputed consent propagation to a PRC-exposed advertising SDK
C2	GDPR Art. 9(1), Art. 26; FTC Consent Order 2021	Advertising SDK named in a prior US consent order, current status unaddressed
H1	GDPR Art. 9(1), Art. 5(1)(c)	Broad wearable-device health-data aggregation, no confirmed DPIA
H2	GDPR Art. 5(1)(a)	Undisclosed screenshot-detection purpose
H3	GDPR Art. 32(1)(b)	Hardcoded credential, no certificate pinning on the consent-sync channel

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent to privacy@/security@/dpo@flo.health, cc UK ICO (lead SA) and Austrian DSB, 5 findings
2026-06-27	Zendesk reply (”Kate”) declines engagement, addresses no finding
2026-07-08	Alexandre Rajagopalan (Privacy Counsel) sends formal legal letter addressing only C1, citing a nonexistent 29 June letter; RFI-IRFOS rebuts same day, flags 4 of 5 findings unaddressed
2026-07-27 / 08-04 / 08-12 / 08-25	Follow-ups restate all five findings and five standing questions; a_rajagopalan@flo.health confirmed bounced, correspondence re-routed
2026-09-04	Final follow-up, day 74, weekly SHA-256 re-diffing confirmed for remaining embargo period
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Nine written notices across 89 days produced two real replies: a support-macro decline and a formal legal letter addressing one of five findings while citing correspondence RFI-IRFOS never sent. No reply of any kind followed after 8 July across five further written notices and ten weeks.

Residual Risk & Recommendations

- Name the external security firm cited in the 8 July letter and provide its report, or publish the specific technical mechanism confirming SDK-layer consent enforcement for the TikTok integration.
- Confirm the Facebook SDK's current data-sharing configuration against the terms of the 2021 FTC consent order.
- Publish the Art. 35 DPIA covering the Oura Ring integration.
- Implement certificate pinning specifically for the Firebase consent-synchronization channel.
- Respond to the four findings the 8 July legal letter did not address.

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, 26, 32, 35, 44-49; FTC Consent Order 2021. REF FLO-C1-2026-R1.