A Contraceptive Medical Device That Reports to a Marketing Platform

Natural Cycles (com.naturalcycles.cordova)

The CE certification that makes millions of people trust this app as a contraceptive was never granted to the version currently in the Google Play Store

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – EIGHTY-ONE DAYS, ONLY THE REGULATOR HAS SPOKEN

Analyst	RFI-IRFOS Research Team
Report date	2026-09-19
Package	com.naturalcycles.cordova
Operator	Natural Cycles Nordic AB (publicly traded, Nasdaq Stockholm)
Device classification	CE Class IIb medical device, MDR 2017/745
Severity	CRITICAL
Findings	4 (1 CRITICAL, 3 HIGH)
R1 sent	2026-06-22
Embargo / coordinated disclosure	2026-09-19
Written notices sent	9
Substantive replies from the company, ever	0

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Natural Cycles is a CE-certified Class IIb medical device under MDR 2017/745, marketed and trusted by millions of users worldwide as a hormone-free, data-driven contraceptive method. Root-level analysis of the production Android APK found that the same application shipping this certified contraceptive function also carries a 492-class Adjust marketing-attribution SDK reading the Google Advertising ID, a 3,434-class MoEngage customer-engagement platform, the largest single third-party SDK in the entire binary, an ACCESS_FINE_LOCATION permission with no demonstrated functional basis, and a hardcoded Firebase API key with a live Realtime Database URL.

The regulatory question this report exists to answer is narrow and specific: the Notified Body that certified Natural Cycles as a Class IIb medical device assessed a device with a stated intended purpose, contraception. It did not assess a device whose contraception-usage events, cycle-tracking engagement, temperature-logging reminders, subscription conversions, are also transmitted to a marketing attribution platform and a customer-engagement platform for advertising and retention purposes. MDR 2017/745 Annex I Sec.17 requires medical device software to process personal data in a manner consistent with the device's intended purpose. Marketing attribution is not that purpose.

This disclosure was sent on 22 June 2026 to a company sophisticated enough to hold CE Class IIb certification and a Nasdaq Stockholm listing. Eighty-one days and nine written notices later, Natural Cycles itself has never replied, not once, to any of the three questions asked. The only voice in this correspondence besides RFI-IRFOS has been Sweden's IMY, the lead supervisory authority, and its one reply was procedural: it will not act without a formal complaint from an affected data subject, which is a statement about how IMY intervenes, not a statement about whether the underlying processing is lawful.

Scope: Root-level static analysis (apktool decode, smali inspection, AndroidManifest.xml review, Cordova plugin configuration review, endpoint and credential extraction) of the publicly distributed Natural Cycles Android APK. No account was created, no backend was accessed, and no network traffic was intercepted. Every finding below is drawn from the binary or the app's own configuration files.

Disposition

Reported 22 June 2026 to privacy@naturalcycles.com (bounced, dead address, confirmed the same day), security@naturalcycles.com, and dpo@naturalcycles.com, with the Austrian DSB, CERT.at, and Swedish IMY (Natural Cycles' lead supervisory authority) in CC. Nine written notices sent over 81 days. IMY replied once, procedurally, on 28 June. Natural Cycles AB itself has never replied. Public disclosure proceeds 19 September 2026, unchanged since 22 June.

ID	Severity	Title
C1	CRITICAL	Adjust marketing-attribution SDK (492 classes) and the Google Advertising ID, active on a Class IIb contraceptive medical device

ID	Severity	Title
H1	HIGH	MoEngage (3,434 classes) – the single largest third-party SDK in the app is a marketing engagement platform
H2	HIGH	ACCESS_FINE_LOCATION on a temperature-logging contraception app, no demonstrated functional necessity
H3	HIGH	Firebase API key and live Realtime Database URL hard-coded in the production APK

Subject & Operator Analysis

Natural Cycles Nordic AB is a publicly traded company on Nasdaq Stockholm, serving millions of users across the EU and the US. This is not a small operator without compliance capacity: a Nasdaq listing implies audited financial controls, a board, and, ordinarily, a functioning legal and regulatory-affairs department – all the more reason the complete absence of a substantive reply across 81 days and nine notices is notable rather than explicable by resource constraints.

Natural Cycles' regulatory foundation is its CE Class IIb certification under MDR 2017/745 – the basis on which a Notified Body determined the app is safe and effective as a contraceptive medical device. That certification, and the public trust built on it, is the asset every finding in this report puts directly in question.

Architecture & Data Flow

The Cordova-based Android app combines the certified contraceptive function (basal temperature logging, cycle prediction, fertility-window calculation) with a marketing and analytics layer that was, on the evidence available, never part of what the Notified Body assessed.

- Certified function: basal body temperature logging, cycle/fertility prediction, NC(deg) thermometer Bluetooth pairing.
- Marketing attribution layer: Adjust (492 classes), reading the Google Advertising ID, transmitting cycle-tracking engagement events.
- Marketing engagement layer: MoEngage (3,434 classes, the largest SDK in the app), push notification and behavioural segmentation.
- Permission surface beyond function: ACCESS_FINE_LOCATION / ACCESS_COARSE_LOCATION, no demonstrated link to the certified function.
- Infrastructure layer: hardcoded Firebase key and live Realtime Database URL.

One honest positive, stated because accuracy runs in both directions: android:allowBackup="false" is correctly set. In RFI-IRFOS's wider 2026 research series, this is one of very few apps to implement that correctly – fertility and contraception data does not go to Google backup. That discipline makes the marketing-SDK findings below more striking, not less: the team clearly can implement data protection correctly when it chooses to.

Findings

C1: Adjust marketing-attribution SDK (492 classes) and the Google Advertising ID, active on a Class IIb contraceptive medical device

Contraception-usage events linked to an advertising identifier

The production APK declares com.google.android.gms.permission.AD_ID and bundles Adjust, a mobile marketing attribution platform, at 492 classes. Adjust reads the Google Advertising ID (GAID) and transmits it alongside app events including temperature-logging reminders, subscription conversion, onboarding completion, and cycle-tracking engagement.

```
https://app.adjust.com
https://ssrv.adjust.com
https://subscription.adjust.com
https://gdpr.adjust.com   (Adjust's own GDPR opt-out endpoint, present in the APK)

<feature name="Adjust"></feature>   (Cordova plugin config.xml)
```

Impact: Natural Cycles' intended purpose, per its MDR 2017/745 Annex I Sec.17 certification, is contraception. Adjust's function is advertising attribution. Transmitting contraception-usage events linked to an advertising identifier to a third-party marketing platform is inconsistent with the device's certified intended purpose, not merely a GDPR Art. 9(1) special-category-data question, though it is that too. The presence of Adjust's own gdpr.adjust.com endpoint in the binary confirms Adjust itself treats this as EU personal data processing under GDPR.

Fix: Remove the Adjust SDK and AD_ID permission from the certified medical-device build entirely, or obtain a fresh MDR conformity assessment covering the marketing-attribution data flow explicitly.

H1: MoEngage (3,434 classes) – the single largest third-party SDK in the app is a marketing engagement platform

Behavioural marketing infrastructure larger than any functional dependency

MoEngage, a customer-engagement and marketing-automation platform for push notifications, in-app messaging, and behavioural segmentation, is present at 3,434 classes – larger than Adjust, larger than Stripe, larger than any other third-party dependency in the entire binary.

```
com.moengage.core
com.moengage.inapp
com.moengage.richnotification
com.moengage.firebase
com.moengage.sdk.debugger
```

Impact: Cycle phase, temperature-logging frequency, ovulation predictions, and app engagement patterns feeding a marketing-automation platform for push-notification targeting and retention campaigns is a direct Art. 5(1)(b) purpose-limitation violation: the data was collected for contraception and is being processed for marketing.

Fix: Remove or strictly scope MoEngage's access to any Art. 9 health-category field; document a separate, explicit lawful basis for any retention-marketing use of contraceptive engagement data.

H2: ACCESS_FINE_LOCATION on a temperature-logging contraception app, no demonstrated functional necessity

Precise GPS on a device whose core function does not require it

Both ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION are declared. Natural Cycles' core function, basal body temperature logging and cycle prediction, does not require precise GPS. The permission may serve Bluetooth pairing with the NC(deg) thermometer, or Adjust attribution – either reading is a data-minimisation failure under Art. 5(1)(c).

Impact: Location data combined with cycle-phase data is particularly sensitive: it can reveal where a person physically is during their fertile window, a materially more invasive inference than either data point alone.

Fix: Remove ACCESS_FINE_LOCATION unless a specific, documented functional need exists; use Bluetooth-scan permissions scoped to device pairing only, not general location access.

H3: Firebase API key and live Realtime Database URL hardcoded in the production APK

Permanent, non-rotatable credential exposure on a health-data device

A Firebase API key, project identifier, and a live Realtime Database URL ship verbatim in the production APK, extractable in under a minute and permanently embedded in every already-installed copy.

```
google_api_key: AIzaSyAwe_7ugJXSDgm7LTI13nbTbtospuNkz34
firebase_database_url: https://natural-cycles.firebaseio.com
google_app_id: 1:712514701016:android:f96605f6e9e174d3
```

Impact: For a CE-certified device processing Art. 9 health data, this level of credential hygiene is inconsistent with Art. 32 security-of-processing obligations and the MDR Annex I Sec.17 requirement to protect against unauthorized access. RFI-IRFOS did not and will not test the live Realtime Database; the burden of confirming deny-by-default Security Rules sits with Natural Cycles.

Fix: Rotate the exposed key, confirm Security Rules are deny-by-default, and restrict the key by package name and SHA-256 certificate fingerprint.

Impact Analysis

The affected population is, specifically, people using a CE-certified medical device as their actual method of contraception – not a wellness app, not a period tracker used for general interest, but a device whose stated purpose and regulatory basis is preventing pregnancy. Every one of the four findings touches data generated by that use: cycle phase, temperature-logging behaviour, and now, via Adjust and MoEngage, a marketing profile built from it.

The location finding (H2) compounds this specifically: combined with fertility-window data, precise location can reveal where a person is during the exact window Natural Cycles exists to help them track for contraceptive purposes – a materially more sensitive inference than either signal in isolation.

The Complete Chain: Certified Purpose to Marketing Profile

A person chooses Natural Cycles specifically because it is CE-certified as a Class IIb medical device – a regulatory signal that carries real weight for a contraceptive method, more weight than an uncertified wellness app would carry. They log their basal body temperature each morning. The app computes their fertility window and tells them, medically, whether they are fertile that day.

That same action, logging temperature, opening the app on a reminder, completing onboarding, converting to a paid subscription, is also an app event Adjust captures and links to the device's Google Advertising ID (C1). In parallel, MoEngage, the single largest SDK in the app, receives cycle phase, logging frequency, and ovulation predictions for behavioural segmentation and push-notification targeting (H1). If the person's device also grants fine location (H2), their physical location during their fertile window becomes available to whatever combination of these systems can access it. None of this marketing-and-location layer was part of the intended purpose a Notified Body assessed when it certified this app as a contraceptive medical device.

Causality, compressed

Certification for a specific intended purpose (contraception) causes public trust that the app's data handling matches that purpose. A marketing-attribution SDK and a customer-engagement platform, both active in the certified build, cause contraception-usage events to reach parties whose function is advertising and retention, not medical care. That gap between certified purpose and actual data flow, disclosed in full on 22 June, causes nine written notices over 81 days. Nine notices with zero replies from the company causes publication on 19 September – the mechanism this programme runs on every target, reached here without the company ever engaging once.

Medical Device Regulation (MDR 2017/745)

MDR 2017/745 Annex I Sec.17 requires that medical device software be designed to process personal data in a manner consistent with the device's intended purpose, and to protect that data against unauthorized access. Natural Cycles' intended purpose, as certified, is contraception. Two SDKs actively processing contraception-usage data for advertising attribution and marketing engagement, and a hardcoded credential exposing the app's backend infrastructure, are not consistent with that intended purpose or with the Annex I Sec.17 security requirement.

This is a narrower and more specific claim than a general GDPR finding: it goes to whether the production APK currently distributed in the Google Play Store is still the device the Notified Body actually certified, or has materially diverged from it since certification. RFI-IRFOS makes no determination on that question – it is a matter for the Notified Body and the competent authorities – but the binary evidence that the marketing SDKs are active in the certified build is not in dispute.

Consumer Protection & Deceptive Design

Natural Cycles markets itself as a hormone-free, data-driven contraceptive method trusted by millions – a claim whose credibility rests substantially on the CE certification. A user relying on that certification as a signal that their contraception data is handled to medical-device standards has no visible way to learn that the same data also reaches a marketing attribution platform and a behavioural engagement platform. The gap between the certified-medical-device narrative and the actual SDK footprint is the same structural pattern RFI-IRFOS has flagged elsewhere in this programme: a true, checkable claim that is materially incomplete in a way that would change a reasonable user's decision.

Data Protection – Article by Article

Article	Engaged by	Basis
Art. 5(1)(b)	H1: MoEngage receiving contraception-usage data for marketing purposes	Purpose limitation – data collected for contraception, processed for marketing
Art. 5(1)(c)	H2: ACCESS_FINE_LOCATION with no demonstrated functional necessity	Data minimisation
Art. 9(1)	C1: Adjust + AD_ID linking contraception-usage events to an advertising identifier	Special-category health data, no documented Art. 9(2) basis for the marketing use
Art. 25	H3: hardcoded credential in the production build of a health-data device	Data protection by design and by default
Art. 32(1)(b)	H3: Firebase key and live Realtime Database URL hardcoded	Security of processing

Regulatory & Legal Landscape

Authority	Basis	Role in this case
IMY (Integritetsskyddsmyndigheten), Sweden	GDPR, lead supervisory authority for Natural Cycles AB	CC'd on R1, replied once procedurally on 2026-06-28: will not act absent a formal data-subject complaint
Datenschutzbehoerde (DSB), Austria	GDPR Art. 5, 9	CC'd on R1 and throughout
CERT.at	Coordinated technical disclosure	CC'd on R1 and throughout
MDR 2017/745 Notified Body (unidentified from the binary)	Annex I Sec.17, Art. 22	The body that issued the Class IIb certification; not directly named as a recipient in this campaign, relevant to any post-market surveillance review

Industry comparison: RFI-IRFOS's 2026 programme has covered several fertility- and cycle-tracking apps; Natural Cycles is, to date, the only one carrying an actual CE Class IIb medical-device certification. That certification raises the regulatory stakes above a standard GDPR finding – MDR 2017/745 exposure is specific to certified medical devices and does not apply to the uncertified wellness-app peers in the same product category.

Indicators of Compromise / Reproducible Evidence

Item	Value
Package	com.naturalcycles.cordova
Adjust smali classes	492
MoEngage smali classes	3,434 (largest third-party SDK in the app)
Firebase project	1:712514701016:android:f96605f6e9e174d3
Firebase Realtime Database URL	https://natural-cycles.firebaseio.com
Advertising permission	com.google.android.gms.permission.AD_ID
Location permissions	ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION

```
apktool d naturalcycles_base.apk -o naturalcycles_decoded
grep -r "AD_ID\|adjust" naturalcycles_decoded/AndroidManifest.xml
grep -rl "com.moengage" naturalcycles_decoded/smali*/
grep -r "firebase_database_url\|google_api_key" naturalcycles_decoded/res/values/
    strings.xml
```

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent to privacy@naturalcycles.com (bounced immediately, dead address), security@naturalcycles.com, dpo@naturalcycles.com, DSB/CERT.at/IMY in CC. 1 Critical, 3 High findings.
2026-06-28	First follow-up. Same day, IMY replies procedurally: the complaint is noted for information only, no action absent a formal data-subject complaint.
2026-07-03	Second follow-up, restating that IMY's procedural posture does not substitute for a substantive company reply.
2026-07-07	Third follow-up.
2026-07-24	Fourth follow-up: thirty-two days on a CE-certified medical device, still no reply from the company itself.
2026-08-09	Fifth and sixth follow-ups, same day.
2026-08-12	Seventh follow-up.
2026-08-21	Eighth follow-up.
2026-08-28	Ninth follow-up.
2026-09-11	Tenth and final pre-publication notice: eighty-one days, zero words from the company itself.

The one voice in this thread that isn't RFI-IRFOS

Across ten messages and 81 days, the only reply this thread has ever received came from IMY, the regulator, not from Natural Cycles AB. A company holding a Nasdaq Stockholm listing and a CE Class IIb medical-device certification has had 81 days to answer three specific, yes/no-answerable questions about its own certified product, and has not sent a single word.

Residual Risk & Recommendations

- None of the four findings has been confirmed addressed, because no substantive reply has ever arrived from the company.
- The Adjust and MoEngage integrations (C1, H1) remain, as far as RFI-IRFOS can verify externally, fully active in the current Play Store build.
- For the relevant MDR 2017/745 Notified Body: whether the marketing-SDK data flows documented here fall inside or outside the scope of the original Class IIb conformity assessment is a determination RFI-IRFOS cannot make and does not attempt to – but the binary evidence that these flows exist in the certified build is available for that review.
- For IMY: the procedural position that a formal data-subject complaint is required before action is noted as IMY's own process, not disputed here – but it leaves the underlying MDR and GDPR questions in this report formally unanswered by any authority to date.
- The binary will continue to be pulled and diffed weekly for the remainder of the embargo period.

RFI-IRFOS's own view: a contraceptive medical device's entire commercial value rests on the trust its certification signals. A company with the resources to hold that certification and a public listing, and the discipline to correctly disable Android backup for exactly this kind of data, does not lack the capacity to answer whether its own marketing SDKs were part of what got certified. Eighty-one days of silence on that specific question reads, to us, as a choice not to have that conversation in writing rather than an absence of an answer. We would genuinely prefer to be shown wrong, in writing, before 19 September.

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