Coordinated Privacy Disclosure, Final Report

Calm (com.calm.android)

Calm.com, Inc., San Francisco, California, USA

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 94 DAYS AFTER DISCLOSURE, NINE MESSAGES SENT, ZERO REPLY OF ANY KIND

Target	Calm, the market-leading meditation, sleep, and mental-wellness app, paid subscription product
Package	com.calm.android
Operator	Calm.com, Inc., San Francisco, California, USA
Initial Disclosure	2026-06-22
Original Embargo	2026-09-20 (90 days from disclosure)
Report Published	2026-09-24, four days after the embargo, an internal publishing gap, not a change in terms
Regulators in CC	Austrian DSB, European Data Protection Board (EDPB)
Total Outbound Messages	9, across 94 days
Inbound Replies	0. No acknowledgment of any kind, automated or human, was ever received from privacy@calm.com, security@calm.com, legal@calm.com, press@calm.com, the named Art. 27 EU representative, or the named UK representative.

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 disclosed to Calm.com, Inc. that its market-leading meditation and sleep app, a paid subscription product with a companion Health Connect integration, ships nine hardcoded third-party SDK credentials in its production binary, initializes Firebase before device unlock and before its own consent UI can run, and routes a structured mood check-in feature, a form of Art. 9-adjacent mental-health self-report, through an eight-vendor analytics fan-out architecture with no consent gate.

A deep-dive bytecode trace conducted during this disclosure, disassembling only the two dex files containing the relevant classes directly, confirmed the mood check-in finding at the instruction level: the shared analytics dispatcher (AnalyticsHelperImpl.track()) contains zero conditional branches on any consent, opt-out, or compliance flag between method entry and its unconditional fan-out loop over every registered AnalyticsClient. A compliance-flags helper exists in the same class but only tags outgoing events with flag values for the receiving vendor to interpret, it never gates the call. The trace also resolved an open question from the original disclosure in Calm's favor: the raw free-text content of a mood note is never transmitted, only its character count and a has-note boolean, a genuine, code-confirmed minimization measure, credited below.

Nine messages were sent to privacy@calm.com, security@calm.com, legal@calm.com, press@calm.com, the named Art. 27 EU representative (EURep@calm.com), and the named UK representative (ukrep@calm.com) across 94 days, cc'ing the Austrian DSB and the EDPB throughout. Not one reply, automated or human, was ever received from any of the six addresses. The 90-day embargo, set at first contact, elapsed on 20 September 2026. This report and the accompanying closure notice publish four days 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 Calm Android application (com.calm.android), covering the AndroidManifest, resource strings, and targeted dex-string and smali evidence, as pulled and reviewed on 6 September 2026 (base APK version 6.102, versionCode 4120456), with a follow-up deep-dive smali trace against the then-current production build (v7.0, versionCode 4120459) conducted the same day to resolve two open architectural questions at the bytecode level. Both APK versions and all extracted smali were deleted immediately after the relevant evidence was captured, per standing disk-discipline practice. No dynamic instrumentation, live traffic capture, or interaction with Calm's backend infrastructure was performed.

Disposition

Five findings were disclosed on 22 June 2026: one HIGH-severity credential-exposure finding (nine hardcoded third-party SDK credentials, including a live Datadog RUM token and eight internal Amplitude environment keys, shipped in the production binary), two findings escalated to HIGH under an explicit blast-radius justification (a Firebase bootstrap sequence that initializes before device unlock and before the app's own consent UI can run, contradicting a real TCF/DMA consent architecture built elsewhere in the same codebase; and a mood check-in feature carrying Art. 9-adjacent emotional-state data that a bytecode-level trace confirms fans out unconditionally to nine separate analytics vendors with no consent gate anywhere in the dispatch path), and two findings corrected down to MEDIUM and LOW respectively under CVSS v4.0 re-scoring. Nine messages were sent across 94 days. Not one reply, automated or human, was ever received from any of the six addresses contacted. This report closes and publishes the case on the terms disclosed from the first message.

ID	Severity	Title
C1	HIGH	Nine Hardcoded Third-Party SDK Credentials in the Distributed Binary, Including a Live Monitoring Token
C2	HIGH	Firebase Initializes Before Device Unlock and Before Consent, Contradicting the App's Own Consent Architecture
H1	HIGH	Mood Check-In Data, Art. 9-Adjacent Mental-Health Self-Report, Confirmed at the Bytecode Level to Fan Out Unconditionally to Nine Analytics Vendors
H2	MEDIUM	Paid Subscription App Still Ships the Full Ad-Attribution Stack; Health Connect Write Scope for Mindfulness Data
M1	LOW	Cloud Backup Includes All Local App Data Except Attribution-Fraud Stores

Subject & Operator Analysis

Calm (com.calm.android) is the market-leading meditation, sleep, and mental-wellness app, operated by Calm.com, Inc. of San Francisco, California. It is a paid subscription product with a companion Health Connect integration that writes mindfulness-session data into Android's system-wide health data store. Calm maintains six named contact points, privacy@calm.com, security@calm.com, legal@calm.com, press@calm.com, an Art. 27 EU representative (EURep@calm.com), and a UK representative (ukrep@calm.com). None replied at any point across nine messages and 94 days.

Several genuine positives are worth naming up front: a real DMA/IAB-TCF consent-state architecture exists in the codebase, well beyond what most apps in this program ship. firebase_analytics_collection_enabled and Facebook's AdvertiserIDCollectionEnabled and AutoLogAppEventsEnabled all default to false in the manifest. An Art. 27 EU representative and a UK representative are both named in the live privacy policy, most non-EU operators in this program have not done this. network_security_config.xml permits no cleartext domains. And, confirmed by the bytecode trace in H1, the raw free-text content of a mood note is never transmitted to any analytics vendor, only its character count and a has-note boolean, a genuine, code-confirmed minimization measure.

Architecture & Data Flow

Calm's own consent engineering exists and is real, a TCF/DMA consent-state column, a typed AppsFlyerConsent data class, and explicit collection-flag defaults of false. That effort is undermined at the one point that matters most for wellness data specifically: FirebaseInitProvider fires before device unlock and before any consent UI can render (C2), and the shared analytics dispatcher that carries the app's own mood check-in feature, a structured emotional self-report, has zero consent branching anywhere in its fan-out loop, confirmed at the bytecode level, not merely inferred from strings (H1). Nine hardcoded third-party credentials, including a live Datadog monitoring token, ship in the same production binary (C1).

Findings

C1: Nine Hardcoded Third-Party SDK Credentials in the Distributed Binary, Including a Live Monitoring Token

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N, 8.8.

Nine distinct third-party services are keyed directly in strings.xml of the shipped binary: Firebase/Google, Facebook, Datadog (RUM), Iterable, AppsFlyer, Amplitude, and Apptentive. Eight separate Amplitude Experiment keys, spanning prod, dev, dev_1 through dev_7, and local environments, are present together in the same production release, exposing Calm's internal environment naming and architecture to any party who downloads the public APK. The Datadog RUM token is a live monitoring credential, not a passive read key, a party holding it can inject synthetic Real User Monitoring events directly into Calm's own production observability dashboards.

```
res/values/strings.xml (excerpt)
google_api_key, google_crash_reporting_api_key: AIzaSyCrZbpLjgclFqhh2SZHOElOhB-
    _rSzD4_U
facebook_client_token: 68683bfae7023029efd1b48291cb7841
datadog_client_token: puba270bda402da475c862d5b302fa8ab38
iterable_key: aeaa602fbd3e4ec0b9f8341638bb8609
appsflyer_key: hHYWjEzLMtrFdxxFVcJLzG
amplitude_key: 800ded5ddeb6fb92371f2a6b0d86d7b5
amplitude_experiments_key_prod / _dev / _dev_1..._dev_7 / _local: 9 distinct keys, all
     present together
apptentive_api_key: f63174ed5efc0ac45fe156013cdfb650e9c8713afa098c9f1304c66f6e24e6b4
```

Impact: A live Datadog RUM token in a public binary lets any party pollute Calm's own production monitoring with synthetic events, and eight internal Amplitude environment keys shipped together expose the company's own dev/prod architecture boundaries to anyone who downloads the app.

Fix: Rotate all nine credentials, move Datadog RUM initialization behind a backend-issued short-lived token, and strip internal-environment (dev/local) keys from the production build configuration entirely. No confirmation that this has occurred was ever received.

C2: Firebase Initializes Before Device Unlock and Before Consent, Contradicting the App's Own Consent Architecture

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 Calm is the market-leading meditation and sleep app with a very large paying subscriber base, and this finding shows the one structural gate meant to govern collection of that mental-wellness data firing before it can ever apply.

FirebaseInitProvider is declared directBootAware="true" with android:initOrder="100", meaning it initializes before device unlock and before any Activity, including the consent UI the rest of the codebase was built to respect. This sits directly alongside real consent-engineering effort elsewhere in the same binary, a dma_consent_state database column, an AppsFlyerConsent(isUserSubjectToGDPR=...) data class, and a full IAB TCF purpose enum, none of which can gate a ContentProvider that has already fired. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because Calm is the market-leading meditation and sleep app with a very large paying subscriber base, and this finding shows the one structural gate meant to govern collection of that mental-wellness data firing before it can ever apply.

```
AndroidManifest.xml
<provider android:authorities="com.calm.android.firebaseinitprovider"
    android:directBootAware="true" android:exported="false"
    android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
```

Impact: Firebase's installation-identifier bootstrap begins at the earliest possible point in the app lifecycle, structurally ahead of the consent UI the same codebase was built to require, for every install of a market-leading wellness app.

Fix: Remove directBootAware and defer FirebaseInitProvider's initOrder until after the consent flow has run, or gate SDK bootstrap explicitly behind the existing dma_consent_state check. No confirmation that this has occurred was ever received.

H1: Mood Check-In Data, Art. 9-Adjacent Mental-Health Self-Report, Confirmed at the Bytecode Level to Fan Out Unconditionally to Nine Analytics Vendors

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because a bytecode trace confirms Art. 9-adjacent mood and emotional-state data reaches nine separate analytics vendors with no consent gate anywhere in the dispatch path, on a market-leading wellness app with a very large paying user base.

A smali trace of AnalyticsHelperImpl.track() (the shared dispatch chokepoint for all tracked events) shows exactly one call, enrichProperties, between method entry and an unconditional loop that invokes trackEvent() on every member of the injected analyticsClients set, with zero if/branch instructions on any consent, opt-out, or compliance flag. A separate compliance-flags helper exists but only tags the outgoing event with flag values for the receiving vendor to interpret, it never gates the call itself. Field-level tracing of putMoodCheckin() confirms the mood category name, all selected mood-tag IDs, tag count and presence, note presence and character count, and the log date are all attached to the outgoing event and fan out unconditionally to all nine registered clients (Firebase, Facebook, AppsFlyer, Amplitude, AmplitudeProxy, Segment, Iterable, Datadog, DataWarehouse). RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because this Art. 9-adjacent emotional-state data is confirmed, at the instruction level, to reach nine separate vendors unconditionally, on a market-leading wellness app with a very large paying user base.

```
smali_c4/com/calm/android/base/analytics/AnalyticsHelperImpl.smali, track()
# enrichProperties$base_release() called once, then:
:goto_10
invoke-interface {v0, p1, p2}, Lcom/calm/android/core/analytics/AnalyticsClient;->
    trackEvent(...)V
goto :goto_10
# zero consent/opt-out branch instructions present between entry and this loop
```

Impact: A user logging ”anxious” or ”grateful” inside a wellness app has that structured emotional-state data, mood category, tags, note presence and length, and timestamp, fanned out to nine third-party analytics vendors through the identical unconditional pipe used for ordinary screen-view events, confirmed at the bytecode level, not merely inferred from strings.

Fix: Add an explicit consent check to the shared track() dispatcher, or route Art. 9-adjacent events (mood check-ins) through a separately gated code path before the fan-out loop. No confirmation that this has occurred was ever received.

H2: Paid Subscription App Still Ships the Full Ad-Attribution Stack; Health Connect Write Scope for Mindfulness Data

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.

Calm is a subscription product with Play Billing 8.0.0 and a Stripe Financial Connections SDK, users already pay directly, yet the binary still carries a full install-attribution and ad-identifier stack (AppsFlyer, Facebook Ads AD_ID plumbing, and Android Privacy Sandbox ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID). Separately, android.permission.health.WRITE_MINDFULNESS and health.WRITE_EXERCISE write session data into Android's system-wide Health Connect store, a shared cross-app data layer outside Calm's own consent flow once data lands there.

```
AndroidManifest.xml
<uses-permission android:name="android.permission.health.WRITE_EXERCISE"/>
<uses-permission android:name="android.permission.health.WRITE_MINDFULNESS"/>
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
```

Impact: A paying subscriber's mental-wellness session data is written into a shared, cross-app Android data layer while the app retains a full advertising-attribution stack it has no free-tier justification to keep.

Fix: Remove the ad-attribution stack for a fully paid product, and document the Health Connect recipient pathway explicitly in the privacy policy. No confirmation that this has occurred was ever received.

M1: Cloud Backup Includes All Local App Data Except Attribution-Fraud Stores

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

allowBackup="true" is set at the application level, and the only paths excluded from Android's Auto Backup and Device Transfer are three AppsFlyer-owned stores whose purpose is attribution and purchase-fraud bookkeeping, not user content. Nothing excludes the local mood check-in database, journal or session history, or the Auth0 session store from the backup scope. The exclusion list shows the engineering team knows how to scope backup content precisely, they did it for three specific paths, which makes the absence of an equivalent exclusion for mood and journal data a minimization gap, not an oversight born of not knowing the mechanism exists.

```
res/xml/appsflyer_data_extraction_rules.xml, full contents
<data-extraction-rules>
  <cloud-backup>
    <exclude domain="sharedpref" path="appsflyer-data" />
    <exclude domain="sharedpref" path="appsflyer-purchase-data" />
    <exclude domain="database" path="afpurchases.db" />
  </cloud-backup>
</data-extraction-rules>
# no equivalent exclusion for the mood check-in or journal database
```

Impact: A user's local mental-wellness data history, mood logs and journal entries, rides along with Android's general-purpose cloud backup mechanism, while only unrelated attribution bookkeeping was deliberately scoped out.

Fix: Extend the existing data-extraction-rules exclusion list to cover the mood check-in and journal databases and the Auth0 session store. No confirmation that this has occurred was ever received.

Impact Analysis

C2 and H1 compound, they do not sit side by side: C2 establishes that Firebase's bootstrap fires ahead of the app's own consent gate, and H1 shows that once a user does interact with the app's most sensitive first-party feature, a structured mood check-in, that data enters a dispatch pipe with no consent branch of its own either, confirmed by direct instruction-level tracing, not string inference alone. C1's nine hardcoded credentials, including a live monitoring token, sit at the operational-security layer underneath both.

Total Silence, Nine Messages, 94 Days

This case's correspondence record is total silence, not deflection, not an automated acknowledgment, nothing. Nine messages were sent to six separately named Calm contact points, privacy@calm.com, security@calm.com, legal@calm.com, press@calm.com, EU-Rep@calm.com, and ukrep@calm.com, across 94 days, cc'ing the Austrian DSB and the EDPB throughout. No bounce, no auto-reply, no human reply was ever received from any of them. Calm names an EU representative and a UK representative in its own privacy policy, addresses that exist specifically to receive exactly this kind of contact, and both remained silent.

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. 32(1)(b), Art. 25, Art. 5(2)	C1	Nine hardcoded third-party credentials, including a live monitoring token, ship in the production binary.
Art. 7(1), Art. 5(1)(a), Art. 25	C2	Consent-gated SDK bootstrap fires before the consent UI it was built to respect can ever run.
Art. 9, Art. 5(1)(c), Art. 35	H1	Art. 9-adjacent mental-health self-report data fans out to nine vendors with no consent gate, confirmed at the bytecode level.
Art. 5(1)(b), Art. 13(1)(e), Art. 9	H2	Full ad-attribution stack retained on a paid product; undisclosed Health Connect recipient pathway for mindfulness data.
Art. 5(1)(c), Art. 32(1)(a)	M1	Cloud backup scope broader than necessary, mood and journal data not excluded despite the technical capability being demonstrated elsewhere in the same manifest.

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. Any such escalation is always stated explicitly in the finding itself, never left implicit, as C2 and H1 are escalated and C1 is corrected down and H2 and M1 are corrected down in this report. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: com.calm.android.