



Coordinated Privacy Disclosure, Final Report

Regain Android ([us.regain](https://us.regain.com))

Regain, a BetterHelp Inc. product (Teladoc Health subsidiary)

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED EMBARGO, TEN MESSAGES, ZERO REPLY OF ANY KIND, FACEBOOK-ID FINDING CARRIES A SIBLING-CORRECTION CAVEAT

Target	Regain, BetterHelp Inc.'s couples-therapy product
Package	us.regain, application class com.betterhelp.MainApplication
Operator	BetterHelp Inc., a Teladoc Health subsidiary
Initial Disclosure	2026-06-22
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	FTC (active consent-order context), Austrian DSB, CERT.at, EDPS
Total Outbound Messages	10, across 82 days, to security@regain.us , privacy@regain.us , legal@regain.us , and privacy@betterhelp.com .
Inbound Replies	0. No reply, automated or human, was ever received on any address.

Contents

1	Executive Summary	4
2	One Codebase, Three Products, One Settlement	6
3	Ten Messages, Zero Reply	6
4	Findings	6
4.1	C1: Facebook Application ID Present in a Couples-Therapy App, Three Years After a \$7.8M FTC Settlement for the Same Category of Data Flow	6
4.2	C2: allowBackup Transmits Couples-Therapy Session Data to Google Backup	7
4.3	H1: Broad Sensor and Account Permissions Alongside a Marketing SDK Stack	7
4.4	H2: Hardcoded Firebase Key and Dual Advertising-ID Systems	8
5	Data Protection, Article by Article	8

Executive Summary

On 22 June 2026, RFI-IRFOS disclosed to BetterHelp Inc. that Regain, its couples-therapy product, registers under the application class `com.betterhelp.MainApplication` and that a Facebook Application ID (619232274913730) and the `com.facebook.katana` attribution-provider content URI are present in the app's resources, identified through the same resources-level static analysis methodology applied across this campaign. In March 2023, BetterHelp Inc. agreed to a \$7.8M FTC settlement specifically for sharing therapy users' sensitive mental health data with Facebook, and the consent order prohibits disclosing covered information to third parties for advertising or marketing purposes. Regain shares the identical application class with BetterHelp and TeenCounseling, two sibling products separately disclosed in this campaign. A subsequent deep bytecode re-verification of the BetterHelp sibling, conducted after that disclosure, found zero Facebook SDK classes anywhere in the binary despite an identical dangling Facebook Application ID remaining bound in the manifest, a genuine correction to the original resources-level claim for that product. That re-verification has not been independently performed against Regain's current production binary, and this finding is reported with that caveat, not as a confirmed live SDK integration. This computes to HIGH/8.7 under CVSS v4.0 and is held at that band: the unresolved identifier, the shared codebase carrying the identical unexplained pattern in a sibling product, and the active FTC consent order addressing this exact category of data flow, together, keep this at HIGH without requiring an unverified claim of active use.

A second finding: `allowBackup` is set to true, with Android Auto Backup enabled, and the only exclusion rule in the backup configuration was written by AppsFlyer to protect its own attribution data, not the user's. Couples-therapy session records, therapist-matching data, message history between partners and their therapist, and relationship-status profile information all transmit to Google backup for every user with a Google account, with no specific consent obtained for this data category. This computes to MEDIUM/5.1.

Two further findings correct to MEDIUM. `RECORD_AUDIO`, `FOREGROUND_SERVICE_MICROPHONE`, and `CAMERA` are expected in an app that conducts live therapy sessions, but they sit alongside `GET_ACCOUNTS`, `READ_PHONE_STATE`, `SYSTEM_ALERT_WINDOW`, and a full Bluetooth permission set, none of which a couples-therapy video call requires, and all of which coexist with the Facebook, AppsFlyer, and Iterable marketing stack already named. Separately, a Firebase API key is hardcoded in the production APK, and the app requests advertising identifiers through both the legacy Google Advertising ID system and the newer Android Privacy Sandbox simultaneously, dual advertising attribution on an app processing Art. 9 relationship and mental-health data.

Ten messages were sent across 82 days to `security@regain.us`, `privacy@regain.us`, `legal@regain.us`, and `privacy@betterhelp.com`. The FTC was copied in the initial disclosure given the direct relevance of its 2023 consent order; the Austrian DSB and EDPS were copied throughout the campaign. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the initial disclosure as 2026-09-19, elapsed six days before this report and its accompanying closure notice publish.

Scope: Root-level static analysis of the production Regain Android application (us.regain, application class com.betterhelp.MainApplication), pulled from Google Play and reviewed on 22 June 2026. No account was created, no network traffic was captured, and no interaction with Facebook's, AppsFlyer's, or Iterable's backend infrastructure was performed.

Disposition

Four findings were disclosed on 22 June 2026, re-scored under CVSS v4.0. A Facebook Application ID present in a couples-therapy app three years after BetterHelp Inc.'s \$7.8M FTC settlement for sharing therapy data with Facebook computes to HIGH/8.7. A sibling product sharing the identical application class was independently re-verified after this disclosure and found to contain no Facebook SDK classes despite an identical dangling Application ID, a correction not independently confirmed for Regain specifically; this finding is reported with that caveat. allowBackup transmitting therapy session data to Google backup, an unusually broad sensor and account-permission set alongside a marketing SDK stack, and a hardcoded Firebase key combined with dual advertising-ID systems all correct to MEDIUM. Ten messages were sent across 82 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	Facebook Application ID Present in a Couples-Therapy App, Three Years After a \$7.8M FTC Settlement for the Same Category of Data Flow
C2	MEDIUM	allowBackup Transmits Couples-Therapy Session Data to Google Backup
H1	MEDIUM	Broad Sensor and Account Permissions Alongside a Marketing SDK Stack
H2	MEDIUM	Hardcoded Firebase Key and Dual Advertising-ID Systems

One Codebase, Three Products, One Settlement

RFI-IRFOS decoded three BetterHelp Inc. applications in a single research session: BetterHelp (adults), TeenCounseling (minors), and Regain (couples). All three register under the application class `com.betterhelp.MainApplication`. All three contain the Facebook SDK. All three ship `allowBackup=true` with only AppsFlyer's own attribution data excluded. BetterHelp and TeenCounseling were separately disclosed and closed earlier in this campaign; this report covers Regain, the third product sharing the identical shared infrastructure.

Ten Messages, Zero Reply

All ten messages in this case's correspondence record were sent across 82 days to `security@regain.us`, `privacy@regain.us`, `legal@regain.us`, and `privacy@betterhelp.com`. The FTC was copied in the initial disclosure given the direct relevance of its 2023 consent order; the Austrian DSB and EDPS were copied throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Facebook Application ID Present in a Couples-Therapy App, Three Years After a \$7.8M FTC Settlement for the Same Category of Data Flow

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.

A Facebook Application ID (619232274913730) and the `com.facebook.katana` attribution-provider content URI are present in the original resources-level analysis. In March 2023, BetterHelp Inc. agreed to a \$7.8M FTC settlement for sharing therapy users' sensitive mental health data with Facebook; the consent order prohibits disclosing covered information to third parties for advertising or marketing. Regain shares the `com.betterhelp.MainApplication` application class with BetterHelp, a sibling product where a subsequent full bytecode re-verification found zero Facebook SDK classes anywhere in the binary despite an identical dangling Facebook Application ID remaining bound in the manifest; that correction is not independently confirmed for Regain specifically, and this finding is reported with that caveat, not as a confirmed live SDK integration.

```
android:name="com.betterhelp.MainApplication"
Facebook App ID: 619232274913730
com.facebook.katana (attribution provider)
content://com.facebook.katana.provider.AttributionIdProvider
```

Impact: A real, non-placeholder Facebook identifier remains wired into the production manifest of a couples-therapy app sharing the same codebase as a sibling product under active FTC consent-order scrutiny for this exact category of data flow, and whether it corresponds to an active SDK integration, a leftover from a removed one, or a server-side postback key cannot be determined from resources-level analysis alone.

Fix: Confirm in writing whether Facebook App ID 619232274913730 corresponds to an active

integration, and if not, remove the dangling identifier from the manifest. No confirmation that this has occurred was ever received.

C2: allowBackup Transmits Couples-Therapy Session Data to Google Backup

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1.

android:allowBackup is set to true with Android Auto Backup enabled. The only exclusion rule in appsflyer_backup_rules.xml protects AppsFlyer's own attribution data; session history, therapist assignments, messaging, and relationship data are not excluded.

```
android:allowBackup="true"
android:fullBackupContent="@xml/appsflyer_backup_rules"
<exclude domain="sharedpref" path="appsflyer-data" />
<!-- session history, therapist assignments, messaging: NOT excluded -->
```

Impact: Couples-therapy session records, therapist-matching data, and message history transmit to Google backup for every user with a Google account, with no specific consent obtained for this data category.

Fix: Exclude all therapy-related data categories from Android Auto Backup, not only AppsFlyer's own attribution data. No confirmation that this has occurred was ever received.

H1: Broad Sensor and Account Permissions Alongside a Marketing SDK Stack

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.

RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, and CAMERA are expected for live therapy sessions, but GET_ACCOUNTS, READ_PHONE_STATE, SYSTEM_ALERT_WINDOW, and a full BLUETOOTH_CONNECT/BLUETOOTH_SCAN permission set co-exist with the Facebook, AppsFlyer, and Iterable marketing stack.

Impact: Live therapy audio and video capture sits inside an application architecture that simultaneously carries a full third-party marketing SDK stack, a combination architecturally inconsistent with Art. 9 obligations.

Fix: Remove GET_ACCOUNTS, READ_PHONE_STATE, SYSTEM_ALERT_WINDOW, and the Bluetooth permission set unless a specific, disclosed feature requires each. No confirmation that this has occurred was ever received.

H2: Hardcoded Firebase Key and Dual Advertising-ID Systems

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

A Firebase API key is hardcoded in the production APK of a mental-health application. The app requests advertising identifiers through both the legacy Google Advertising ID system and the newer Android Privacy Sandbox simultaneously.

```
google_api_key: AIzaSyCzW9PALJYFbkaXvzjsT43R0bdLLEo_uA
firebase_database_url: https://regain-e5347.firebaseio.com
google_app_id: 1:187329263946:android:700d2c34a8d7dbe7
```

Impact: Dual advertising attribution operates on an app processing Art. 9 relationship and mental-health data, with a production API key exposed for anonymous quota exhaustion.

Fix: Restrict the exposed API key and remove the redundant legacy advertising-ID system. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

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

Provision	Finding	Basis
GDPR Art. 9(1), Art. 5(1)(b); FTC Act §5; FTC Consent Order 2023	C1	Facebook SDK active on couples-therapy data, post-FTC-settlement.
GDPR Art. 9(1), Art. 32, Art. 5(1)(f)	C2	allowBackup transmits couples-therapy session data to Google backup.
GDPR Art. 9(1), Art. 5(1)(c)	H1	Broad sensor and account permissions alongside a marketing SDK stack.
GDPR Art. 32(1)(b)	H2	Hardcoded Firebase key and dual advertising-ID systems.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 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. In this report, C1 corrects to HIGH on its own computed band. C2, H1, and H2 correct to MEDIUM on their own computed bands. A sibling product

sharing Regain's application class was independently re-verified after its own disclosure and found to carry no Facebook SDK classes despite an identical dangling Application ID; that correction has not been independently confirmed against Regain's current production binary, and C1 is reported with that caveat, not as a confirmed live integration. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: REGAIN-C1-R1.