Security & Privacy Disclosure, Final Report

kGoal Boost for Android (com.minnalife.boost)

An intimate-health app that asked for no consent, and an operator that now reports changes in writing.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026, STATED IN OUR MESSAGE OF 15 NOVEMBER. OPERATOR REPLIED 18 NOVEMBER 2026, FIXES STATED BY THE OPERATOR, NOT VERIFIED.

Target	Therapy Holdings, Inc., 1816 SE 22nd Ave, Portland, OR 97214, USA (kGoal, Minna Life)
Versions Audited	2.1.51 (versionCode 246), analysed 2026-08-22. Operator states 2.1.60 (Android) and 2.88.5 (iOS) of 2026-11-11, not analysed.
Supervisory Authority	None designated (operator outside the EU). Representative: PelviCoach GmbH, Mannheim, per policy 2.0. Policy 2.1 of 2026-11-16 is stated by the operator and was not read by RFI-IRFOS.
Notice / Publication	2026-08-22 / 2026-11-21 (91 days after the notice)
Findings	6: 1 High, 3 Medium, 2 Low (all six from the first notice, re-assessed)
Status	OPERATOR ANSWERED IN WRITING ON 11 AND 18 NOVEMBER 2026. FIXES STATED BY THE OPERATOR, NOT VERIFIED BY RFI-IRFOS, AS OF 21 NOVEMBER 2026.
SHA-256 (base APK)	`111786aa2f68d27fbf9491e5070b57173ae63cddea6de638d1e8157d28f9db39`

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1 Executive Summary 4

2 Finding Status at a Glance 6

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 7

5 Findings 7

5.1 C1: No consent step for health-related workout data, and Firebase starts at process start in version 2.1.51 . . . 7

5.2 C2: The Google Play Data Safety label said no data is shared with third parties while the Privacy Policy reserved the right to share stripped data for advertising, marketing and analytics . . . 9

5.3 H1: Firebase API key hardcoded in res/values/strings.xml . . . 10

5.4 H2: No EU representative, no stated legal basis and no transfer information in the version 2.1.51 Privacy Policy for a US operator offering the app in the EU . 11

5.5 M1: PEGI 3 content rating on an adult intimate device, with no age gate in version 2.1.51 . . . 12

5.6 L1: Privacy Policy and Terms of Service links ship as plain http in version 2.1.51 13

6 Impact Analysis 13

7 The Complete Chain 14

8 Health Data, the Biometric Question & Operator Rebuttal 14

9 Data Protection: Article by Article 15

10 Regulatory & Legal Landscape 16

11 Indicators of Compromise & Reproducible Evidence 16

12 Disclosure Timeline & Outcome 17

13 What kGoal Got Right 18

14 Residual Risk & Recommendations 18

Executive Summary

kGoal Boost is the companion app of a Bluetooth pelvic-floor biofeedback trainer, published on Google Play by Therapy Holdings, Inc. of Portland, Oregon. On 22 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF KGOALBOOST-2026-R1 after a root level code analysis of version 2.1.51. It described two Critical and two High findings, one Medium and one Low, and asked three written questions.

Two findings carry the case. In version 2.1.51 users were never asked for consent before their workout data, which comes from an intimate device and is tied to an email address, went to the operator's Firebase project, and the operator's own policy said that no opt-out existed (C1). The Google Play label said nothing is shared with third parties while the policy reserved the right to share stripped data for advertising (C2).

The operator answered in writing three times. A COO acknowledged the notice on 16 September 2026, sent a point-by-point follow-up on 11 November 2026 and replied again on 18 November 2026 to our message of 15 November. The 11 November message states a consent step, analytics and crash reporting off by default, no advertising identifier, https links, an adult target audience, a rewritten Privacy Policy and a named EU representative, in Android version 2.1.60 and iOS version 2.88.5. It also disputes three points of the notice: the data is not biometric within the meaning of Art. 4(14) GDPR, no workout data goes to Firebase Analytics, and the Firebase key is not a secret.

This report is stricter than the notice and gives the operator's corrections their weight. The two Critical labels are reduced to High and Medium, the two High labels to Medium and Medium, the Medium to Low and the Low stays Low. On 15 November 2026 we withdrew the word biometric as a legal classification, narrowed the Art. 44 to 46 point and asked three remaining questions. The Privacy Policy version 2.0 on the live site confirmed the wording changes, the named representative and the removal of the stripped-data passage.

The reply of 18 November 2026 answers the three questions. The operator states that it processes the workout data on the basis of explicit consent under Art. 9(2)(a), through a separate unticked checkbox. It states that Privacy Policy version 2.1, published on 16 November 2026, names the legal bases, the right to withdraw consent and the right to lodge a complaint, and that the consent-by-use transfer sentence is removed. On the Firebase key it states that every request to Firestore is checked against security rules and that it publishes no further details of its server-side configuration.

The app itself (versions 2.1.60 and 2.88.5), the consent screen, the Data Safety form, the Play rating, Privacy Policy version 2.1 and the Firestore rules were not examined by RFI-IRFOS. Every fix to the app and every statement of 18 November is recorded as stated by the operator, not verified by RFI-IRFOS. No severity changes on the strength of these statements.

Scope: Root level code analysis of kGoal Boost 2.1.51 (versionCode 246, package com.minnalife.boost), a base APK of about 90 MB and an arm64-v8a XAPK bundle of about 100 MB: apktool resource and manifest decode, and dex string analysis across six classes dex files with about 30,199 class definitions. A full smali decompile was not run, so every statement that would need method bodies is marked UNVERIFIED. The APK came from the APKPure mirror because no audit device was connected, and the developer name and version were checked against the live Google Play listing. The mirror listed 2026-08-08 for 2.1.51 while Google Play showed an update on 2026-08-17, so the Play build at the date of the notice may differ from the audited build. The operator's public Privacy Policy at kgoal.com was read by plain HTTP GET, first on the analysis day and again before the report of 15 November 2026 (version 2.0). Version 2.1 of 16 November 2026 was not read. No account was created, no kGoal or Firebase server was called and no key was tested. CVSS v4.0 measures exploitability. Most findings here are data-governance findings with no attacker, so the printed scores are low and three findings carry an explicit blast-radius escalation.

ID	Severity	Title
C1	HIGH	No consent step for health-related workout data, and Firebase starts at process start in version 2.1.51
C2	MEDIUM	The Google Play Data Safety label said no data is shared with third parties while the Privacy Policy reserved the right to share stripped data for advertising, marketing and analytics
H1	MEDIUM	Firebase API key hardcoded in res/values/strings.xml
H2	MEDIUM	No EU representative, no stated legal basis and no transfer information in the version 2.1.51 Privacy Policy for a US operator offering the app in the EU
M1	LOW	PEGI 3 content rating on an adult intimate device, with no age gate in version 2.1.51
L1	LOW	Privacy Policy and Terms of Service links ship as plain http in version 2.1.51

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Operator states explicit consent under Art. 9(2)(a), separate unticked checkbox, in 2.1.60. Stated by the operator, not verified.
C2	CRITICAL	MEDIUM	Policy passage removed, confirmed on the live page (version 2.0). Label statement not re-checked.
H1	HIGH	MEDIUM	Operator states access runs through Firestore security rules and publishes no further details. Stated by the operator, not verified. Restrictions not examined.
H2	HIGH	MEDIUM	Representative named, confirmed on the live page (2.0). Operator states policy 2.1 of 16 November adds legal bases and complaint right. Stated by the operator, not verified.
M1	MEDIUM	LOW	Adult target audience stated by the operator. Not verified.
L1	LOW	LOW	https links stated by the operator. Not verified.

Subject & Operator Analysis

The operator is Therapy Holdings, Inc., trading as Minna Life and kGoal, 1816 SE 22nd Ave, Portland, OR 97214, USA. It is a US company with no establishment in the Union. The notice went to privacy@kgoal.com, boost-help@kgoal.com and customerservice@kgoal.com. The reply came from Jonathan Thomas, COO, with privacy@kgoal.com as the channel.

Because the operator has no establishment in the Union, there is no lead supervisory authority under Art. 56 GDPR and each national authority is competent for its own residents. The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the first notice for transparency. The operator names PelviCoach GmbH of Mannheim as its Art. 27 representative in Privacy Policy version 2.0.

Architecture & Data Flow

- Device link: Bluetooth Low Energy to the trainer. BLUETOOTH_SCAN carries neverForLocation and ACCESS_FINE_LOCATION is capped at maxSdkVersion 30.
- Account: email login through Firebase Auth. default_web_client_id is present.
- Storage: workout data in Google Firebase (Firestore and Realtime Database), project boost-76f95, hosted in the United States per the operator.
- Start-up: FirebaseInitProvider with initOrder 100 and directBootAware (C1).
- Analytics path: Firebase Analytics, Crashlytics, App Check and Messaging are bundled. Endpoints app-measurement.com/a and app-measurement.com/s/d are in the dex strings (C1).
- Consent: no consent management platform. A bundled tickbox gates account creation (C1).
- Paid feature: Workout Analysis (kGoal+) derives strength, endurance and control scores from the raw readings.
- Network configuration: no network_security_config.xml override, so the Android default blocks cleartext traffic (L1).

What this report does not show is any payload that leaves the phone. Where a statement depends on it, the finding says UNVERIFIED.

Findings

C1: No consent step for health-related workout data, and Firebase starts at process start in version 2.1.51

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), reassessed from CRITICAL in the first notice. Operator states a fix in Android 2.1.60 and, on 18 November 2026, explicit consent under Art. 9(2)(a). Stated by the operator, not verified by RFI-IRFOS

The operator's own Privacy Policy, as captured on 22 August 2026, stated that users have no option to opt out of any collection, use, sharing or retention. The package contains no consent management platform. FirebaseInitProvider is declared with initOrder 100 and directBootAware true, so Firebase Analytics, Crashlytics, App Check and Messaging are constructed when Android binds the process, before any activity or splash screen. The only consent-adjacent string gates account creation.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the data is health-related workout data from an intimate device tied to an email-linked account, the operator's own policy stated that no opt-out existed, and the operator's own description of its new consent step confirms that no consent step existed before. CRITICAL, as disclosed on 22 August 2026, is withdrawn because the transmitted analytics content was not measured and the data-protection classification of the readings as biometric is contested.

```
<provider android:authorities="com.minnalife.boost.firebaseinitprovider"
    android:directBootAware="true" android:exported="false"
    android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<receiver android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measurement.AppMeasurementReceiver"/>
<service android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measurement.AppMeasurementService"/>
```

Policy wording captured on 22 August 2026, verbatim: ”At this time, The Company does not provide users of the App any options to selectively opt out of our collection, use, sharing or retention of any data.” Search for OneTrust, Didomi, Usercentrics and IABTCF markers across resources and all six classes dex files returned no match. The string please_agree_terms_first (”You must agree with our Terms of Service and Privacy Policy to create an account”) gates sign-up with a bundled tickbox. The manifest also declares com.google.android.gms.permission.AD_ID and android.permission.ACCESS_ADSERVICES_AD_ID, and the dex strings contain the analytics endpoints app-measurement.com/a and app-measurement.com/s/d.

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): new users must accept the revised Terms of Use and Privacy Policy and ”separately consent to the processing of their workout data” to create an account, and existing users are asked for the same on opening the update. The consent box is unticked by default and acceptance is recorded with date and policy version. Analytics and crash reporting are off by default and run only if the user turns them on in the consent prompt or in Settings. These changes are stated for Android version 2.1.60 and iOS version 2.88.5, released on 11 November 2026. RFI-IRFOS has not analysed version 2.1.60 and records this as the operator’s statement.

The operator also corrects the notice on three points. First, it states that no workout, pressure or health data is sent to Firebase Analytics, and that the app logs two Analytics events, a selection on the welcome screen (including which kGoal product the user says they own, with Google Play install-referrer parameters) and the install-referrer campaign. The notice asserted that the Analytics pipeline initializes before any consent step, not that workout data reaches Analytics, and the operator’s description is consistent with the first statement. Second, it states that workout data is stored in the user’s own account so that history and progress work. The Privacy Policy version 2.0 lists it as collected data. Third, it disputes that the data is biometric. That point is addressed in the section on health data below.

Observed fact: in version 2.1.51 no consent step for workout data existed before the data was uploaded to the operator’s Firebase project boost-76f95, and the operator’s newly described consent step confirms the absence of an earlier one. Not shown: the content of what version 2.1.51 sent to Firebase Analytics before sign-up, which depends on call order in code that the dex string analysis does not decide. That is UNVERIFIED. The first notice rated this CRITICAL. This report rates it HIGH because the workout data is health-related data of an intimate device, the missing consent step is confirmed by both sides, and the transmitted analytics content was not measured.

Operator statement of 18 November 2026 (Jonathan Thomas, COO), answering our question on Art. 9: it applies the Art. 9 standard to the workout data and processes it ”on the basis of explicit consent under Art. 9(2)(a).” The consent is a separate, unticked checkbox, distinct from acceptance of the Terms and Privacy Policy and from the optional analytics setting. An account cannot be created without it, existing users are asked on opening the updated app with signing out as the only alternative, and it is recorded with date and policy version. Withdrawal is by deleting the account in the app. Stated by the operator, not verified by

RFI-IRFOS. The reply names no position on whether the readings are data concerning health under Art. 9(1) beyond applying that standard.

GDPR: Art. 7(1), Art. 9(2)(a), Art. 6(1), Art. 5(1)(a), Art. 5(2), ePrivacy Directive Art. 5(3)

Impact: A person who bought an intimate pelvic-floor trainer and installed its app was never asked whether the readings of their body, tied to their email address, may be stored on a US server. The operator's own policy told them there was nothing to decide.

Fix: Keep the new consent step, record the policy version with every acceptance, and verify in the shipped build that Firebase Analytics and Crashlytics stay disabled until the user opts in. Re-collect consent from existing users on the new text.

C2: The Google Play Data Safety label said no data is shared with third parties while the Privacy Policy reserved the right to share stripped data for advertising, marketing and analytics

---

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from CRITICAL in the first notice. Policy wording changed on 11 November 2026, confirmed on the live page

Two public statements by the same operator about the same app disagreed. The Data Safety page captured on 22 August 2026 said "No data shared with third parties." The Privacy Policy said the company may strip personally identifying information and share the data with third parties "for various purposes, including advertising, marketing, and analytics" with no obligation to seek permission.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the label is the disclosure most users read first, the device is an intimate one, and for the length of version 2.1.51 the operator's own two statements gave opposite answers. CRITICAL, as disclosed on 22 August 2026, is withdrawn because the package shows no advertising or attribution recipient and sharing was not demonstrated.

Google Play Data Safety page, captured 22 August 2026, verbatim: "No data shared with third parties. The developer says this app doesn't share user data with other companies or organizations." Privacy Policy captured the same day, verbatim: "we may strip your data of any personally identifying information and share it with third parties for various purposes, including advertising, marketing, and analytics. In such instances, we have no obligation to seek your permission or provide you with the ability to opt-out of such disclosures."

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): the Data Safety declaration "is accurate" and the operator does not share user data with third parties. The passage on sharing de-identified data has been removed from the Privacy Policy.

Check against the live page: the Privacy Policy at kgoal.com now reads "Version 2.0, updated and effective November 11, 2026". The stripped-data passage is gone. Section 3 says "We do not sell personal information collected through the App, and we do not sell or share de-identified, individual-level data with third parties for their own independent use", and section 4 says "The App does not collect your device's advertising identifier, and we do not use data collected through the App for advertising". Section 3 still allows the company to "share or license aggregate statistics about our users as a whole" that do not identify any individual. Google appears as the storage provider through Firebase.

Observed fact: in version 2.1.51 the label and the policy contradicted each other. The pack-

age supports the label more than the policy. Its SDK inventory contains no ad network, no attribution SDK and no session-replay tool, only Google and Firebase components, a game engine and an image loader. The policy passage therefore looks like reserved rights that the package does not show in use. Not shown: whether any stripped data was ever shared. That is UNVERIFIED. The first notice rated this CRITICAL. This report rates it MEDIUM because what is demonstrated is a documentary contradiction that the operator reports as resolved, and the live policy page confirms the changed wording.

GDPR: Art. 5(1)(a), Art. 13(1)(e), Art. 5(2)

Impact: A person reading the Play label before installing an intimate-health app was told nothing is shared, while the legal text they accepted at sign-up reserved the right to share data for advertising.

Fix: Keep label and policy aligned on every release, and state in the policy which recipients are processors and which receive only aggregate statistics.

H1: Firebase API key hardcoded in res/values/strings.xml

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), reassessed from HIGH in the first notice. Operator answered 18 November 2026, stated by the operator, not verified

The Firebase client configuration is readable from any copy of the package. The same value is stored twice, as google_api_key and as google_crash_reporting_api_key.

```
<string name="google_api_key">AIzaSyCbNxUjT72CG9WchMClU0EAys-RsCz4l3o</string>
<string name="google_crash_reporting_api_key">AIzaSyCbNxUjT72CG9WchMClU0EAys-RsCz4l3o
    </string>
<string name="google_app_id">1:140450854339:android:e55711c448dc5a0daa7976</string>
<string name="project_id">boost-76f95</string>
<string name="default_web_client_id">140450854339-u36tio8q5b3ohv3qare9iau9a50ugfsi.
    apps.googleusercontent.com</string>
```

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): ”The Firebase API key in the app is not a secret. As Google documents, it identifies the Firebase project and is placed in every Firebase Android app by Google’s own build tooling.”

Observed fact: the operator is right that Google documents these keys as project identifiers and that every Firebase Android app carries one. The value is unchanged in the audited package. What matters is the restriction on the key and the access rules and App Check enforcement of the Firestore and Realtime Database in project boost-76f95. No key was tested and no Google or kGoal service was called, so the restrictions are UNVERIFIED. The manifest shows that App Check is bundled, which is a mitigating fact only if it is enforced. The first notice rated this HIGH. This report rates it MEDIUM because the key is a public identifier by design and the exposure depends on server-side settings that were not examined.

Operator statement of 18 November 2026: ”Access to user data does not depend on the key. Every request to Firestore is checked against our security rules.” The project, sender and app identifiers are ”public configuration values by design.” The operator adds: ”We do not publish further details of our server-side security configuration.” Stated by the operator, not verified by RFI-IRFOS. The reply gives no answer on quota limits, key restrictions or App Check enforcement, so the five vectors named in our message of 15 November 2026 stay

open as questions. The finding keeps its grade.

GDPR: Art. 32(1)(b), Art. 25

Impact: If the project is not locked down, anyone holding the key can exhaust its quota. For a connected trainer that interrupts the sync of a user's own workout history.

Fix: Restrict the key to the package name and signing certificate, restrict it to the required APIs, enforce App Check on Firestore and the Realtime Database, and review the security rules of project boost-76f95.

H2: No EU representative, no stated legal basis and no transfer information in the version 2.1.51 Privacy Policy for a US operator offering the app in the EU

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from HIGH in the first notice. Representative named in policy 2.0, confirmed on the live page

The policy captured on 22 August 2026 said data is "stored and processed on servers located in the United States of America" and that "by using our Services, you consent to the transfer". It did not name the GDPR or the CCPA, an EU representative or a data protection officer. The app was listed on the Austrian and EU Google Play store with a PEGI rating, which shows EU distribution.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the processor is a US company with no EU presence offering an intimate health-related device in the EU, and the missing representative removed the only local route for a user's requests. HIGH, as disclosed on 22 August 2026, is withdrawn because the representative is now named and the Chapter V point does not carry for direct collection.

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): personal data "is collected directly from users by Therapy Holdings, Inc. and stored in the United States on Google Cloud (Firestore), with Google acting as our processor under its data processing terms", and "as a controller outside the EU, we have appointed PelviCoach GmbH as our representative under Art. 27, as set out in our Privacy Policy."

Check against the live page: Privacy Policy version 2.0 names the representative in section 6, "PelviCoach GmbH, Franz-Volhard-Straße 5, 68167 Mannheim, Germany, contact@pelvicoach.com". The page still contains the sentence "By using our Services, you consent to the transfer of your personal information to the United States." It does not name an Art. 6 legal basis, a right to lodge a complaint with a supervisory authority or a data protection officer. Section 7 says the company "may, at its discretion, delete or anonymize" the data of an account inactive for more than two years and "is not obligated to do so on any particular schedule".

Observed fact: the Art. 27 element is addressed on the live page. The Art. 44 to 46 element of the first notice is narrowed here. The operator states that it collects the data directly from users, and the European Data Protection Board's Guidelines 05/2021 treat direct collection by a controller outside the Union as a case that is not a Chapter V transfer. The operator's answer names no Art. 46 mechanism, and the first notice asked for one, so the question as posed does not carry. What remains is the Art. 13 information duty. The policy gives no legal basis, no complaint right and a consent-by-use transfer sentence, and consent by mere use is not valid consent under Art. 7. The Art. 37 point in the first notice is not maintained as a finding, because a data protection officer is required only where the Art. 37(1) conditions

are met and the operator's scale is UNVERIFIED. The first notice rated this HIGH. This report rates it MEDIUM because the main gap was closed on 11 November 2026 on the operator's account and the live page, and what remains is incomplete information.

Operator statement of 18 November 2026: Privacy Policy version 2.1, "published at kgoal.com on 16 November 2026," states the legal bases for the processing, the right to withdraw consent and the right to lodge a complaint with a supervisory authority, and the sentence that use of the Services constitutes consent to the transfer "has been removed and is not relied on." Stated by the operator, not verified by RFI-IRFOS, because version 2.1 was not read for this report. The observations above describe version 2.0 as read on 11 November 2026. The finding keeps its grade until version 2.1 has been read.

GDPR: Art. 27, Art. 13(1)(c), Art. 13(2)(d), Art. 7, Art. 44

Impact: For the months version 2.1.51 was on sale in the EU, a user who wanted to exercise a data right had no EU address to turn to and no statement of the legal basis. The device is intimate and the operator sits in another jurisdiction.

Fix: State the legal basis for each purpose in the policy, add the right to complain to a supervisory authority, remove the consent-by-use sentence for the US storage, and publish a fixed retention period instead of a discretionary one.

M1: PEGI 3 content rating on an adult intimate device, with no age gate in version 2.1.51

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), reassessed from MEDIUM in the first notice. Operator reports adult rating, not verified

The Google Play listing showed PEGI 3, and the APKPure mirror showed "Everyone". Search for date-of-birth, age-gate and parental-control strings in resources and dex returned no app-specific age mechanism. The one match, ERROR_CODE_PARENTAL_CONTROL_RESTRICTED, is a generic Play Billing and Play Core constant.

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): the Google Play content rating questionnaire was re-run and the target audience is set to adults, 18 and over.

Check against the live page: Privacy Policy version 2.0 says "The App and our services are not directed to, or intended to be used by, children under 18 years of age." The current Play rating and the app flow were not re-checked, so the rating change is UNVERIFIED. RFI-IRFOS has not analysed version 2.1.60 and records this as the operator's statement.

Observed fact: the mismatch was a labelling gap for a product that is plainly for adults. It is not a processing finding by itself. The first notice rated it MEDIUM. This report rates it LOW because the harm is the rating label and the operator reports that it was corrected.

GDPR: Art. 8, Art. 25

Impact: A parent who relies on PEGI 3 to decide what a child may install is given the wrong signal for an app that pairs with an intimate device.

Fix: Confirm the adult rating on Google Play and the App Store, and add an age statement to the sign-up flow.

L1: Privacy Policy and Terms of Service links ship as plain http in version 2.1.51

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), unchanged from the first notice. Operator reports https links, not verified

Both legal-document links are hardcoded with the http scheme. The destination page redirects to https today, so the exposure is the first request only.

```
<string name="privacy_and_policy">http://www.kgoal.com/privacy?lang=en</string>
<string name="terms_of_service">http://www.kgoal.com/terms?lang=en</string>
```

Operator statement of 11 November 2026 (Jonathan Thomas, COO, Therapy Holdings, Inc.): ”Policy links use https and point to kgoal.com in every language.” RFI-IRFOS has not analysed version 2.1.60 and records this as the operator’s statement.

Observed fact: no network_security_config.xml override was found, so the Android default of blocking cleartext traffic applies to the app’s own API calls on targetSdk 37. This is a hygiene finding about two links and not an interception path for workout data. Unchanged rating from the first notice.

GDPR: Art. 32(1)(a)

Impact: A user on a hostile network who taps the policy link could be shown a forged policy page for the first request.

Fix: Use https links in every language build and check them in release testing.

Impact Analysis

- Account holders. They use an intimate device whose readings, scores and workout history are tied to an email address and stored on US servers. In version 2.1.51 they were not asked for consent and the policy said they had no choice (C1).
- Readers of the Play label. They were told no data is shared, while the policy reserved sharing for advertising (C2).
- EU users who want to exercise a right. They had no EU representative and no stated legal basis until the 11 November 2026 policy (H2).
- Parents. PEGI 3 told them the app suits any age (M1).

Scale: the notice records live distribution on the Austrian and EU Play store. No install count was verified for this report.

The Complete Chain

- 1. A person buys the trainer and installs kGoal Boost. At process start Firebase initializes before any screen (C1).
- 2. The person creates an account with an email address. The tickbox covers the Terms and the Privacy Policy and nothing narrower (C1).
- 3. The trainer sends pressure readings by Bluetooth. The app computes scores and uploads the history to the operator's Firebase project in the United States (C1).
- 4. The Play label says nothing is shared. The policy reserves the right to share stripped data (C2).
- 5. The person has no EU representative to address and no stated legal basis (H2).
- 6. The operator's written position of 11 and 18 November 2026 is that a consent step under Art. 9(2)(a), opt-in analytics, a named representative and Privacy Policy 2.1 with legal bases are in place. These are stated changes. RFI-IRFOS has not verified them in a shipped build or on the live page for version 2.1.

Each later section of this report refers to one of these six links. The harm is a processing chain that began for an intimate product without a consent step and without a way to refuse.

Health Data, the Biometric Question & Operator Rebuttal

The first notice called the workout readings biometric data. The operator disputes this. Art. 4(14) GDPR defines biometric data as personal data from specific technical processing of physical characteristics that allows or confirms the unique identification of a person. Pressure readings from a trainer are processed to score exercise, not to identify anyone, so the operator's reading is the better one for the term biometric. This report accepts that point and withdraws the word biometric as a legal classification.

The classification that remains open is Art. 4(15), data concerning health, which Art. 9(1) places among the special categories. A pelvic-floor strength and control score computed from readings of a body and tied to an email address relates to the physical condition of a person. The operator's Privacy Policy itself said, in the version captured in August, that the app processes "biometric data from wearable devices", and describes exercise data collected from a wearable device. Whether the readings are health data for the purpose of Art. 9 is a legal question the operator has to answer in its Data Protection Impact Assessment. This report treats it as likely and not as settled, which is why C1 is rated on the demonstrated absence of consent and not on the category label.

Two further points of the operator are recorded. The operator says the two Analytics events do not contain workout data and that workout data is stored in the user's account to run the service. Both statements are consistent with the package. The content of the events was not measured.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a)	Transparency. Label and policy contradicted each other (C2). The policy gives no legal basis (H2).
Art. 5(2)	Accountability. A design with no consent step cannot demonstrate consent (C1).
Art. 6(1)	Legal basis. The policy 2.0 names none (H2). The operator states that policy 2.1 names them.
Art. 7	Consent. A bundled tickbox at sign-up and consent by mere use of the service are not specific consent (C1, H2).
Art. 8	Age of the user. Rating and audience label (M1).
Art. 9(1), 9(2)(a)	Data concerning health, if the readings qualify. Explicit consent required (C1).
Art. 13(1)(c), 13(1)(e), 13(2)(d)	Purposes and legal basis, recipients, right to complain (C2, H2).
Art. 25	Data protection by design (C1, M1).
Art. 27	EU representative. Named on 11 November 2026 (H2).
Art. 32(1)	Security of processing. Key hygiene and link scheme (H1, L1).
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.
Art. 35	DPIA for the health-data question.
ePrivacy Directive Art. 5(3)	Access to information on the terminal device (C1).

Regulatory & Legal Landscape

A US operator with no Union establishment answers to each national supervisory authority for its residents and must have an Art. 27 representative where Art. 3(2) applies. The Datenschutzbehörde and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: consent for workout data separate from acceptance of the Terms, recorded with the policy version and unticked by default, is the pattern the operator now describes. Analytics that stay off until the user turns them on is the standard design for apps in this category.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The package came from the APKPure mirror and the developer name kGoal.com was checked against the Google Play listing. The signing certificate was verified with apksigner and matches the fingerprint published on the mirror.

```
Package       com.minnalife.boost
Version       2.1.51 / versionCode 246 (analysed 2026-08-22)
base.apk      SHA-256 111786aa2f68d27fbf9491e5070b57173ae63cddea6de638d1e8157d28f9db39
XAPK bundle   SHA-256 19b39fa51ca300e977554026ed2c17f9a8b4d61f375ac7106310cd95fdaed095
Signing cert  SHA-1 4a8c20585d0db1bfcbcd88a7872e13e997714823 (Google Play App Signing)
Firebase      project boost-76f95, app 1:140450854339:android:e55711c448dc5a0daa7976
              google_api_key AIzaSyCbNxUjT72CG9WchMClU0EAys-RsCz4l3o
              default_web_client_id 140450854339-u36tio8q5b3ohv3qare9iau9a50ugfsi.apps
    .googleusercontent.com
```

```
http://www.kgoal.com/privacy?lang=en
http://www.kgoal.com/terms?lang=en
https://play.google.com/store/apps/datasafety?id=com.minnalife.boost
app-measurement.com/a
app-measurement.com/s/d
```

```
Operator contacts  privacy@kgoal.com, boost-help@kgoal.com, customerservice@kgoal.com,
     jon@kgoal.com
Support ticket     Zendesk request 9541 (automated acknowledgment, 2026-08-22)
```

Disclosure Timeline & Outcome

Date	Event
2026-08-22	Analysis of version 2.1.51. Notice REF KGOALBOOST-2026-R1 sent to privacy@kgoal.com, boost-help@kgoal.com and customerservice@kgoal.com, copied to the Datenschutzbehörde and the EDPS. Three written questions. Same day: automated Zendesk acknowledgment, request 9541.
2026-09-12	Follow-up on the same thread. Findings restated unchanged. Answers requested by 22 September 2026.
2026-09-16	Reply from Jonathan Thomas, COO. A review had been completed, changes were in progress and a point-by-point response would follow before 21 November 2026. The reply says it is an acknowledgment and not agreement with the notice.
2026-09-18	RFI-IRFOS reply logging the 16 September message as an acknowledgment and restating the three questions.
2026-10-17	Reminder, 35 days before publication. Three questions unchanged.
2026-11-11	Follow-up from Jonathan Thomas. Reports changes in Android 2.1.60 and iOS 2.88.5 of the same day and in Privacy Policy and Terms of Use version 2.0. Answers all three questions in writing. States three corrections and asks that the report reflect them.
2026-11-14	No bounce received for any message.
2026-11-15	RFI-IRFOS answers the message of 11 November (13:02 UTC, from s.kepp@rfi-irfos.com). It withdraws biometric as a legal classification, narrows the Art. 44 to 46 point, records the operator statements as such, confirms the policy changes of version 2.0 on the live page and asks three questions on Art. 9, Art. 13 and the Firebase key. Embargo date 21 November 2026 restated.
2026-11-16	Privacy Policy version 2.1 published at kgoal.com, as stated by the operator on 18 November 2026. Not read by RFI-IRFOS.
2026-11-18	Reply from Jonathan Thomas, COO (19:27 UTC). Answers the three questions: explicit consent under Art. 9(2)(a), policy 2.1 with legal bases, withdrawal and complaint right, Firestore security rules without further detail. The reply refers to our message as 'of 16 November'; our message carries 15 November 2026, 13:02 UTC. It asks that the publication reflect the answers, which this report does as the operator's statements.
2026-11-21	Publication of this final report. Embargo date reached. No request to extend the embargo was received.

The operator received the same embargo date in every message. No request to extend it was made and none was granted.

What kGoal Got Right

- Bluetooth permission handling is textbook correct: BLUETOOTH_SCAN carries neverForLocation and location is capped at API level 30.
- allowBackup is false, so workout data is not swept into Android Auto Backup.
- The SDK inventory is clean: no ad network, no attribution SDK, no session-replay tool and no SDK from a sanctioned or high-risk jurisdiction.
- No RECORD_AUDIO and no CAMERA permission is requested.
- targetSdk is 37, tracking current Android.
- A COO answered personally, and the operator reports a concrete set of changes with version numbers.
- Privacy Policy version 2.0 is versioned, lists the data collected, offers account deletion in the app and names a representative.

Residual Risk & Recommendations

Most of the reported fixes rest on the operator's statement of 11 and 18 November 2026, and the findings describe version 2.1.51. Versions after 2.1.51, Privacy Policy version 2.1 and the Firestore rules are not covered by this report, and the status of each finding will change once a shipped build and the new policy have been examined.

- Verify in the shipped build that no Firebase Analytics or Crashlytics data leaves the device before the user opts in.
- Read Privacy Policy version 2.1 against the operator's statement that it holds the legal bases, the complaint right and no consent-by-use sentence.
- Restrict the Firebase key and enforce App Check on the project.
- Run a Data Protection Impact Assessment on the classification of the readings as health data.
- Publish a fixed retention period.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published application plus the operator's public Privacy Policy. No kGoal or Firebase servers or accounts were probed and no key was tested. Severity per CVSS v4.0 (CVSS-B) with explicit blast-radius escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF KGOALBOOST-2026-R1.