Security & Privacy Disclosure, Final Report

GlucoCoachAI (com.glucocoachai.app)

A diabetes coaching app whose store label and privacy policy contradict each other, with analytics that start before consent.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	GlucoCoachAI LLC (Aliso Viejo, California, United States)
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	1.0.12 / 1010012 (analysed 2026-08-21)
Findings	8: 4 High, 3 Medium, 1 Low (C1 reassessed from Critical, M2 from Medium)
Status	NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`573a412f213c2090457176a1db0c15f7f487fdf8a654077497f7403c82fec589`

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Findings 6

5.1 C1: Firebase Analytics starts before any consent screen, with all four Consent Mode defaults set to granted, in a diabetes coaching app . . . 6

5.2 H1: Google Play Data Safety says no data is shared with third parties, the privacy policy says data may be shared . . . 7

5.3 H2: No EU representative and no named Data Protection Officer for a US company processing health data of EU users . . . 8

5.4 H3: Microphone, contacts and precise location permissions with no traceable feature or disclosure . . . 9

5.5 M1: Date of birth is collected with no age check, the store rating is PEGI 3 and the policy says the app is not for under 18 . . . 10

5.6 M2: allowBackup is true on an app that stores glucose logs, meal photos and chat history locally . . . 10

5.7 M3: No network security configuration and no certificate pinning for the production API . . . 11

5.8 M4: Privacy policy contradicts itself and a staging backend reference to an external agency domain shipped in the production bundle . . . 11

6 Impact Analysis 12

7 The Complete Chain 12

8 Special-Category Health Data: Why the Setting Matters 13

9 Data Protection: Article by Article 13

10 Consumer Protection & Platform Disclosures 14

11 Regulatory & Legal Landscape 14

12 What GlucoCoachAI Got Right 14

13 Indicators of Compromise & Reproducible Evidence 15

14 Disclosure Timeline & Outcome 15

15 Residual Risk & Recommendations 16

Executive Summary

GlucoCoachAI is an Android coaching app for people with Type 2 diabetes, built around an AI chat persona called Kai that gives food, glucose and lifestyle guidance. It is published on Google Play under the package com.glucocoachai.app by GlucoCoachAI LLC, a US company, and shows 10+ installs. The privacy policy describes collection of diabetes type, diagnosis date, A1C values, glucose logs, medications, date of birth, meal photos and location. This is special-category health data under Art. 9 GDPR.

On 21 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF GLUCOCOACHAI-2026-R1 to the support address the company publishes, copying the Austrian Datenschutzbehörde and the European Data Protection Supervisor. It reported eight findings from a root level code analysis of version 1.0.12 and asked three written questions. A follow-up on 12 September 2026 and a final reminder on 17 October 2026 restated them. As of 14 November 2026 no reply of any kind has arrived, not even an automated acknowledgement.

The governing thesis of this report is that the app tells people three different things about their data. The store label says nothing is shared (H1). The privacy policy says data may be shared with unnamed partners, names a data category that cannot apply to a digital product, and offers no EU contact (H2, M4). The binary starts analytics before any consent screen with every Consent Mode signal set to granted, on a product where the fact of using it is itself a health inference (C1). The same build requests a microphone and address book access that nothing explains (H3).

The report is also specific about limits. The Google advertising ID is blocked and no advertising SDK is present, which keeps the analytics finding below Critical, the rating used in the first notice. No traffic was captured, so no health field is shown leaving the device. What happens on api.glucocoachai.com, and whether the AI persona is custom or a pass-through to a third-party language model, cannot be seen from the client and is not claimed.

Scope: Root level code analysis of the Google Play release 1.0.12 (versionCode 1010012): manifest, resources, the Expo app.config, the seven dex files and the Hermes JavaScript bundle. Public web pages read by plain HTTP GET: the Play Store listing and Data Safety page and the privacy policy. No backend was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. Report prepared for the publication date. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89.

ID	Severity	Title
C1	HIGH	Firebase Analytics starts before any consent screen, with all four Consent Mode defaults set to granted, in a diabetes coaching app
H1	HIGH	Google Play Data Safety says no data is shared with third parties, the privacy policy says data may be shared
H2	HIGH	No EU representative and no named Data Protection Officer for a US company processing health data of EU users
H3	HIGH	Microphone, contacts and precise location permissions with no traceable feature or disclosure
M1	MEDIUM	Date of birth is collected with no age check, the store rating is PEGI 3 and the policy says the app is not for under 18
M2	LOW	allowBackup is true on an app that stores glucose logs, meal photos and chat history locally
M3	MEDIUM	No network security configuration and no certificate pinning for the production API
M4	MEDIUM	Privacy policy contradicts itself and a staging backend reference to an external agency domain shipped in the production bundle

Finding Status at a Glance

ID	Disclosed	This report	Status on 14 November 2026
C1	CRITICAL	HIGH	No reply. Reassessed on the evidence: initialisation order and defaults demonstrated, no health field observed in transit.
H1	HIGH	HIGH	No reply. Both statements read live on 21 August 2026.
H2	HIGH	HIGH	No reply. No representative named.
H3	HIGH	HIGH	No reply. Permissions as declared in 1.0.12.
M1	MEDIUM	MEDIUM	No reply.
M2	MEDIUM	LOW	No reply. Reassessed: the adb route is restricted on Android 12 and later.
M3	MEDIUM	MEDIUM	No reply.
M4	MEDIUM	MEDIUM	No reply.

Subject & Operator Analysis

The developer named on Google Play and in the privacy policy is GlucoCoachAI LLC, a US limited liability company with a single listed postal address in Aliso Viejo, California. The privacy policy footer lists one support address and states that the person behind it reads every email. The Play listing publishes a developer contact address and two telephone numbers, which differ. RFI-IRFOS did not establish why two numbers are listed.

The pattern is a very small operator rather than an organisation with a data protection function. The policy names no Data Protection Officer and no EU representative. The binary points to an external build: the bundled JavaScript carries a staging reference under the namespace of a development studio, and the app uses stock Expo managed workflow modules (expo-router, expo-sqlite, expo-image-picker, expo-iap and the React Native Firebase packages) with no custom native code found. Who is responsible under Art. 4(7) GDPR is not in doubt, since the policy names GlucoCoachAI LLC. Whether the studio acts as a processor under Art. 28 is not documented anywhere the analysis could read.

This operator receives the same treatment as every other target of the programme. Size and download count do not change the questions, they only change the proportionate answers.

Architecture & Data Flow

The client is a React Native application on the Expo SDK 54 managed workflow. Application logic is Hermes bytecode in assets/index.android.bundle. Seven classes dex files hold mostly Firebase, Google Play services, the ML Kit barcode scanner and React Native scaffolding. The app declares targetSdkVersion 36 and minSdkVersion 24.

Data flow as far as the client shows it: the user completes an onboarding profile (date of birth, diabetes type, diagnosis date, A1C, medications), logs glucose and meals with photos, and chats with Kai. The production API host api.glucocoachai.com is configured in assets/app.config and the stack is tRPC. A dashboard host, dashboard.glucocoachai.com, appears in the same file. Analytics flow to Google through Firebase from process start. Purchases run through Apple and Google, so no card data reaches the controller.

What the client does not show: how the backend stores and forwards health data, which language model answers Kai, and what the dashboard host does. These are stated as outside the analysis and no claim is made about them.

Findings

C1: Firebase Analytics starts before any consent screen, with all four Consent Mode defaults set to granted, in a diabetes coaching app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 21 August 2026, reassessed in this report

FirebaseInitProvider is a ContentProvider with directBootAware="true" and initOrder="100". Android instantiates it at process start, before any Activity and before device unlock, so no consent screen can run first. The manifest also declares the Google Analytics defaults analytics_storage, ad_storage, ad_user_data and ad_personalization_signals, all set to true. A search of all seven dex files and the JavaScript bundle for OneTrust, Didomi, Usercentrics, consentmanager.net and any ConsentInformation or UserMessagingPlatform class found nothing. The IABTCF key names present in classes4.dex are string constants of a bundled dependency with no implementing class beside them. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the app is a Type 2 diabetes coaching product, so even the fact that a device runs it is a health inference, and because the manifest sets all four Google Consent Mode signals to granted, which is the opposite of the denied-by-default pattern Google recommends. The mitigations the notice recorded (advertising ID blocked, no ad mediation SDK) keep this below Critical.

```
<provider android:authorities="com.glucocoachai.app.firebaseinitprovider"
          android:directBootAware="true" android:exported="false"
          android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<provider android:authorities="com.glucocoachai.app.reactnativefirebaseappinitprovider
    "
          android:exported="false" android:initOrder="99"
          android:name="io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider
    "/>
<meta-data android:name="firebase_analytics_collection_enabled" android:value="true"/>
<meta-data android:name="app_data_collection_default_enabled" android:value="true"/>
<meta-data android:name="google_analytics_default_allow_analytics_storage" android:
    value="true"/>
<meta-data android:name="google_analytics_default_allow_ad_storage" android:value="
    true"/>
<meta-data android:name="google_analytics_default_allow_ad_user_data" android:value="
    true"/>
<meta-data android:name="google_analytics_default_allow_ad_personalization_signals"
    android:value="true"/>
<meta-data android:name="google_analytics_adid_collection_enabled" android:value="true
    "/>
<meta-data android:name="google_analytics_ssaid_collection_enabled" android:value="
    true"/>
```

Mitigating facts, recorded in the notice of 21 August 2026: assets/app.config lists com.google.android.gms.permission.AD_ID, ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION under blockedPermissions, so the Google advertising ID is not collected, and no ad mediation or attribution SDK exists anywhere in the binary. These facts

narrow what the granted flags can do today. They do not change that the defaults are granted and that collection starts before a user can decide.

Disclosed as CRITICAL on 21 August 2026. This report rates the finding on the evidence the root level code analysis supports: initialisation order and manifest defaults are demonstrated, transmission of any health field is not.

Impact: Every person who installs the app, whose stated audience is people managing Type 2 diabetes, has analytics session, device and IP-derived location data collected from the first process start, before they see a consent choice. The pattern also covers a person who installs the app and never opens it.

Fix: Set all four Consent Mode defaults to denied in the manifest, disable automatic collection until the user decides, and start Firebase from application code after a recorded consent. Document the Art. 6(1) basis for any collection that remains before consent.

H1: Google Play Data Safety says no data is shared with third parties, the privacy policy says data may be shared

---

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 (CVSS-B)

The Data Safety page states ”No data shared with third parties” and lists seven collected categories: device or other IDs, precise location, name and email address, crash logs, app interactions and in-app search history, photos, and health info. Section 4 of the privacy policy states ”We may share data with: Third-party service providers (hosting, support, email delivery), Legal authorities when required, Security & fraud prevention partners”. Google excludes pure processors acting on the developer’s instructions from its definition of sharing, so hosting and email delivery alone could be consistent with the label. The category ”Security & fraud prevention partners” is not obviously a processor, and the policy does not name any recipient. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the Data Safety label is the disclosure most people read before installing, the app collects seven data categories including health information, precise location and photos, and the two statements come from the same controller at the same time.

```
No data shared with third parties
This app may collect these data types: Location, Personal info and 5 others
(Device or other IDs, Precise location, Name and Email address, Crash logs,
 App interactions and In-app search history, Photos, Health info)
```

```
We may share data with:
- Third-party service providers (hosting, support, email delivery)
- Legal authorities when required
- Security & fraud prevention partners
```

Impact: A person with diabetes who relies on the store label to decide whether to enter glucose logs, A1C values and meal photos is told that nothing is shared, while the policy they would have to open separately says otherwise and names no recipient.

Fix: Reconcile the two documents so that both state the same recipients, name each recipient

category with its processor role, and align the Data Safety form with the policy.

H2: No EU representative and no named Data Protection Officer for a US company processing health data of EU users

---

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 (CVSS-B)

Section 13 of the privacy policy is a single generic paragraph addressed to individuals in the EEA, UK and Switzerland. It names no EU representative, no EU postal address and no Data Protection Officer. The Play Store listing does not name one either. The controller's only listed address is in Aliso Viejo, California. The app was available in the Austrian Google Play storefront (English, United Kingdom) when analysed. Art. 27(2)(a) exempts only processing that is occasional, does not include large scale processing of special categories, and is unlikely to risk individuals' rights. A diabetes coaching service processes health data as its core and continuing function, so the occasional limb does not fit, and the policy itself addresses EEA individuals. Whether the processing is large scale at a store count of 10+ installs is a question for the controller and the supervisory authority. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the controller is a US limited liability company, the processing is health data that is the core function of the product, and the only EU-facing content is one generic paragraph, so a person in Austria has no address or contact in the EU to exercise rights against.

```
GDPR Privacy: Applicable to individuals in the EEA, UK, or Switzerland. Outlines
    rights
including access, correction, objection, erasure, data transfer, and withdrawal of
    consent.
(no representative, no EU address, no DPO named)
```

Impact: An Austrian user who wants to access or delete their A1C and glucose records has a support mailbox and a US address and nothing else, and no EU contact exists to receive a complaint or a request on the controller's behalf.

Fix: Designate an Art. 27 representative or document in writing why Art. 27(2)(a) applies, name the representative and a data protection contact in the policy and the store listing.

H3: Microphone, contacts and precise location permissions with no traceable feature or disclosure

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B)

The shipped manifest declares ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, CAMERA, READ_CONTACTS, WRITE_CONTACTS, RECORD_AUDIO, SYSTEM_ALERT_WINDOW, READ_EXTERNAL_STORAGE and WRITE_EXTERNAL_STORAGE. Only the location, camera and RECORD_AUDIO permissions appear in the developer's own android.permissions array in assets/app.config. The contacts, overlay and legacy storage permissions were merged in from bundled libraries. No NSMicrophoneUsageDescription exists in app.config, the store listing gives no voice feature, and every microphone hit in the Hermes bundle is an icon glyph name such as microphone-off. The iOS contacts text says contacts help "share your health insights with your healthcare providers and support network", but the bundle contains no contacts-picker or contacts-read strings, only icon glyph names. The iOS location text refers to "nearby healthy options and services". RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the app requests a microphone and write access to the address book on an Art. 9 health app, no feature in the build matches either, and the only stated purpose for location (nearby restaurants) is one that coarse location normally satisfies.

```
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.CAMERA
android.permission.READ_CONTACTS
android.permission.WRITE_CONTACTS
android.permission.RECORD_AUDIO
android.permission.SYSTEM_ALERT_WINDOW
android.permission.READ_EXTERNAL_STORAGE
android.permission.WRITE_EXTERNAL_STORAGE
```

A permission requires a runtime grant by the user for the dangerous classes, so the declaration alone does not read data. The finding is that the build requests capabilities it has no visible use for and the controller has published no purpose for the microphone.

Impact: A person with diabetes who grants the microphone or address book prompt gives an app with a health profile access to capabilities that nothing in the app or the store listing explains.

Fix: Remove RECORD_AUDIO, READ_CONTACTS, WRITE_CONTACTS and SYSTEM_ALERT_WINDOW from the shipped manifest unless a feature uses them, use coarse location for the nearby-options feature, and publish the purpose of each permission that remains.

M1: Date of birth is collected with no age check, the store rating is PEGI 3 and the policy says the app is not for under 18

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 (CVSS-B)

The Hermes bundle contains an onboarding date of birth field with the validation message ”Date of Birth date cannot be in the future” and a birthdate form component. Section 8 of the privacy policy states the app is not intended for individuals under 18. The Play Store content rating is PEGI 3. The bundle contains no blocking, escalation or age verification logic for an entered date of birth.

The restriction exists in the policy text only. Neither the store rating nor the code enforces it. Whether any minors use the app is not established by the analysis.

Impact: A teenager with diabetes can complete onboarding and enter diagnosis, medication and glucose data, and the controller has no technical way to notice.

Fix: Block onboarding for dates of birth under 18 or implement the parental authorisation that Art. 8 requires where consent is the basis, and align the store rating with the policy.

M2: allowBackup is true on an app that stores glucose logs, meal photos and chat history locally

LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B), disclosed as MEDIUM on 21 August 2026, reassessed in this report

The application element in the manifest does not set allowBackup to false. App data therefore stays eligible for Android Auto Backup to the user’s own Google account and for device-to-device transfer. The adb backup route named in the notice of 21 August 2026 is restricted by the platform for apps that target Android 12 or later and this build targets API 36, so the exposure reachable by an attacker with a cable is narrower than that notice described. The remaining point is a hardening gap on an app whose local data includes glucose logs, cached meal photos and chat history.

```
<application android:allowBackup="true" ... android:name="com.glucocoachai.app.
    MainApplication" ...>
```

Disclosed as MEDIUM on 21 August 2026. The vector uses AV:P, AC:H and AT:P because the residual routes need physical access or access to the person’s own backup account.

Impact: Health records held by the app can be copied into backups the controller does not manage, which widens where a person’s diabetes data lives beyond the app itself.

Fix: Set android:allowBackup=”false” or define explicit data extraction rules that exclude health and chat data.

M3: No network security configuration and no certificate pinning for the production API

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B)

res/xml contains no network_security_config.xml and the application element declares no networkSecurityConfig attribute. Because targetSdkVersion is 36, the platform default denies cleartext traffic, which removes the most serious consequence. The absence of any pinning for api.glucocoachai.com leaves the TLS channel for glucose, A1C and chat content exposed to interception by a device or network that carries a trusted rogue certificate authority.

The vector uses AC:H and AT:P because interception needs a trusted rogue certificate authority on the device or network path.

Impact: On a managed or hostile network that has installed its own root certificate, the contents of a person's glucose and A1C uploads could be read in transit.

Fix: Add a network security configuration that disallows cleartext explicitly and pins the production API certificate or public key.

M4: Privacy policy contradicts itself and a staging backend reference to an external agency domain shipped in the production bundle

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B)

Section 2.1 of the privacy policy lists "Shipping & Billing Address" as information collected directly from users. Section 3 of the same document states that subscriptions are processed exclusively through Apple or Google and that no payment details are collected. The product is digital and ships nothing. Separately, the Hermes bundle contains the fragment https://api.staging.glucocoachai.mightybyte. (the top-level domain suffix could not be isolated cleanly from the string table), which points at a staging backend under the namespace of an external development studio and shipped in the production binary.

```
https://api.staging.glucocoachai.mightybyte.
```

This finding is supporting evidence for the build provenance of the product more than a standalone breach. It shows a privacy policy that was not tailored to the actual service and a build that retained a staging reference.

Impact: A user cannot tell from the policy which personal data the service actually collects, because a data category that cannot apply sits next to a statement that excludes payment data.

Fix: Rewrite the policy against the actual data flows and remove staging endpoints from the production bundle.

Impact Analysis

People affected: users of the app, who by its purpose are people managing Type 2 diabetes. The product asks them for the most sensitive category of data the GDPR defines, and for a continuing stream of it.

- Analytics start before the person can decide (C1). The harm is concrete even without a health field in the payload, because a device that runs a diabetes coaching app tells the analytics service something about its owner.
- The store label gives a reassurance the policy does not support (H1). A person who reads only the label enters data believing nothing is shared.
- Rights are hard to exercise (H2, M4). With no EU representative and a policy that lists a shipping address for a digital product, a user in Austria cannot tell what is held or whom to write to inside the EU.
- Capabilities without a stated purpose (H3). A microphone and address book access on a health app widen what a later update or a compromised library could reach.
- Local and transit protection are thin (M2, M3). Backup is open and no pinning protects uploads on a hostile network.
- No age enforcement (M1). The policy bars minors, the store rating invites them and the code does not check.

Scale is small. The store shows 10+ installs. The severity ratings reflect the nature of the data and the defects, not the size of the user base.

The Complete Chain

Step 1, discovery and install: a person in Austria finds the app on Google Play, rated PEGI 3, with a Data Safety label saying no data is shared with third parties (H1, M1).

Step 2, first launch: before any screen renders, FirebaseInitProvider starts with all four Consent Mode signals set to granted and no consent framework present (C1). The advertising ID stays blocked, which limits the effect.

Step 3, onboarding: the app asks for date of birth with no age check, then diabetes type, diagnosis date, A1C and medications (M1). It requests location, camera, microphone and contacts permissions, several without a matching feature (H3).

Step 4, use: glucose logs, meal photos and chat with Kai go to api.glucocoachai.com. The bundle also holds a staging reference to an external studio (M4). Nothing in the client shows a certificate pin or a network security configuration (M3).

Step 5, on the device: the data directory is eligible for backup (M2).

Step 6, the person tries to act: the policy has one generic GDPR paragraph, names no EU representative and no DPO, lists a data category that cannot apply, and says data may be shared with unnamed partners while the store label says it is not (H1, H2, M4). Support is a single mailbox.

Special-Category Health Data: Why the Setting Matters

Art. 9(1) GDPR prohibits processing of data concerning health unless a condition in Art. 9(2) applies. For an app whose entire function is diabetes management, explicit consent under Art. 9(2)(a) is the realistic condition, and consent must be informed, specific and given before processing. A configuration that begins analytics before the consent screen and a policy that does not say who receives data work against that condition at its foundation.

Art. 25 GDPR requires data protection by design and by default. For this app the default is the reverse: collection defaults to on, Consent Mode defaults to granted, and the broadest permission set is requested.

Data Protection: Article by Article

Article	Engaged by	Finding
Art. 3(2)	The policy addresses EEA individuals and the app is available in the Austrian storefront	H2
Art. 4(7)	GlucoCoachAI LLC is named as controller	Subject
Art. 5(1)(a)	Store label, policy and binary describe different realities	C1, H1, M4
Art. 5(1)(c)	Permissions and data categories beyond a stated purpose	H3, M1
Art. 5(2)	Controller must be able to demonstrate compliance, none documented	C1, M4
Art. 6(1)	No basis stated for collection before consent	C1
Art. 7(1)	Controller must demonstrate consent, collection precedes it	C1
Art. 8	Date of birth collected, no age enforcement	M1
Art. 9	Health data is the core processing	C1, H2, Setting
Art. 12(1)	Information must be transparent and easily accessible	H1
Art. 13(1)(a)(b)	Controller identity and contact in the EU absent	H2
Art. 13(1)(c)	Purposes of processing not stated for several permissions	H3, M4
Art. 13(1)(e)	Recipients not named	H1
Art. 25	Defaults favour collection	C1, H3, M1
Art. 27	No EU representative	H2
Art. 32(1)(a)(b)	Backup open, no pinning	M2, M3

Consumer Protection & Platform Disclosures

The Data Safety section on Google Play is completed by the developer and shown to users as a summary of data practices. In this case the summary states that no data is shared with third parties while the developer's own policy lists recipient categories. RFI-IRFOS makes no determination about Google's own developer policy and records only that the two documents conflict on their face.

The PEGI 3 content rating sits beside a policy that excludes under-18 users. A consumer reading the store listing gets a rating that invites all ages and a policy, reached separately, that excludes most of them.

Regulatory & Legal Landscape

Competent authority: the controller has no main establishment in the EU, so the one-stop-shop mechanism does not apply and each concerned supervisory authority is competent. For a matter initiated from Austria the Österreichische Datenschutzbehörde is the authority, with the European Data Protection Supervisor copied on the notice.

Pre-consent analytics also engage Art. 5(3) of Directive 2002/58/EC as implemented in Austria by § 165(3) TKG 2021, which requires prior consent for storing or accessing information on a user's terminal equipment unless strictly necessary for a service the user requested.

Comparison within the programme: the finding pattern of Firebase starting before consent is common across the apps reviewed. What sets this case apart is the combination with Art. 9 data, a store label that contradicts the policy, and the absence of any contact path other than one mailbox.

What GlucoCoachAI Got Right

- No advertising SDK of any kind. A class search of all seven dex files for AppLovin, AdMob, Meta Audience Network, Unity Ads, ironSource, InMobi, Vungle, Mintegral, Pangle, Moloco, Fyber, CloudX, AppsFlyer, Adjust, Braze, Amplitude and OneSignal returned no hit.
- The advertising ID and AdServices permissions are blocked in assets/app.config, a deliberate choice rather than an omission.
- Background location is not requested, and the policy says location is not collected in the background.
- targetSdkVersion 36 means the platform default denies cleartext traffic.
- Purchases run through Apple and Google, with no payment data handled by the controller.
- AI output is labelled as informational and not for medical decisions, repeatedly.
- Account deletion works in the app and by email with a stated permanent deletion commitment.

Indicators of Compromise & Reproducible Evidence

Every point below is reproducible by another researcher from the public Google Play release and the public web pages named.

```
Package        com.glucocoachai.app
Version        1.0.12 (versionCode 1010012)
Size           67.6 MB base.apk (70,927,500 bytes), 92.2 MB XAPK split bundle
SDK levels     minSdkVersion 24, targetSdkVersion 36
Stack          Expo SDK 54.0.0, Hermes bundle (4.7 MB), 7 classes dex files

base.apk SHA-256
573a412f213c2090457176a1db0c15f7f487fdf8a654077497f7403c82fec589

XAPK SHA-256
4b0a10bab63959a4ad9a23803eab3e9233b0a9d7e127ed43e7186a1399eabf5a
```

```
https://api.glucocoachai.com                production API, assets/app.config
https://dashboard.glucocoachai.com          assets/app.config
https://api.staging.glucocoachai.mightybyte.  fragment in assets/index.android.bundle
https://www.glucocoachai.com/privacy-policy  Sections 2.1, 3, 4, 8, 13
play.google.com/store/apps/datasafety?id=com.glucocoachai.app
```

Chain of custody: the package was not installed on an RFI-IRFOS test device. The XAPK was obtained from the APKCombo mirror after the version and developer name were matched against the live Google Play listing. The manifest and resources were decoded with apktool without sources, and the dex files and Hermes bundle were searched as raw strings. The production and dashboard hosts were not contacted.

Disclosure Timeline & Outcome

2026-08-21 First notice (REF GLUCOCOACHAI-2026-R1) to support@glucocoachai.com, CC Austrian Datenschutzbehörde and European Data Protection Supervisor. Findings C1, H1, H2, H3 stated in full, M1 to M4 summarised, three questions asked, reply requested within 14 days.

2026-09-12 Follow-up to the same address restating the findings and the three questions with a deadline of 19 September 2026. No reply of any kind had arrived.

2026-10-17 Reminder from security@rfi-irfos.com to the same address, 33 days before publication. No reply of any kind had arrived.

2026-11-14 No reply, no automated acknowledgement and no delivery failure notice on record.

2026-11-19 Publication date, unchanged since 21 August 2026 and independent of any reply.

Residual Risk & Recommendations

Open on the evidence of this report: all eight findings. The controller has not answered, so no remediation is on record. The findings describe version 1.0.12 as analysed on 21 August 2026. The state of later builds is not part of this report.

For the controller, in order of effect: set Consent Mode defaults to denied and start Firebase after consent (C1), make the Data Safety label and the policy agree and name recipients (H1), designate and publish an Art. 27 representative and a data protection contact (H2), remove permissions with no feature (H3), enforce the age restriction the policy states (M1), disable backup of app data (M2), add a network security configuration with pinning (M3), correct the policy and remove staging references (M4).

For users: treat the app as one that may send analytics before consent, avoid granting microphone and contacts access, and use the in-app or email deletion route the controller documents if you stop using it.

Questions that remain open and are not answered by the client: what the backend does with submitted health data, who the language model provider is, and what the dashboard host serves.

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 All findings derive from root level code analysis of the published application using publicly available tooling, plus public web pages read by plain HTTP GET. No servers, accounts or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF GLUCOCOACHAI-2026-R1.