Security & Privacy Disclosure, Final Report

MyFitnessPal for Android (com.myfitnesspal.android)

A diet app that classifies calorie goals against eating-disorder thresholds, reads blood glucose and declares food histories as shared with advertisers.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. ONE GENERIC SUPPORT REPLY AND AUTOMATED ACKNOWLEDGEMENTS ONLY, THREE WRITTEN QUESTIONS UNANSWERED.

Target	MyFitnessPal, Inc., 100 Congress Avenue, Suite 400, Austin, TX 78701, USA
Versions Audited	26.33.0 / versionCode 51226 (analysed 2026-08-23)
EU Representative	DataRep (Art. 27 GDPR), myfitnesspal@datarep.com
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	6: 2 High, 4 Medium (H2 and H4 reassessed from High)
Status	NO ANSWER TO THE THREE WRITTEN QUESTIONS AS OF 21 NOVEMBER 2026. One generic support reply on 18 September 2026, automated acknowledgement of the notice of 15 November 2026.
SHA-256 (base APK)	`9fbfb44350a38011ba5028b81fca11b2d02453e49df2db3ed6867b3cded5cba4`

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 H1: Locally computed eating-disorder-adjacent inference layer, confirmed by the operator's own policy admission . . . 6

5.2 H2: Blood-glucose reading pipeline correlated with the food diary inside the same app . . . 7

5.3 H3: Barcode and meal-scan food data falls under the operator's own "Commercial Information" category, declared as shared with marketing and advertising partners . . . 8

5.4 H4: Policy claim of technical measures against under-18 sign-up next to an all-ages PEGI 3 rating, no enforcing gate located . . . 9

5.5 M1: Advertising and analytics SDK bootstraps run at process start, before any consent dialog, despite a genuine Google UMP and IAB TCF implementation . 10

5.6 M2: Play Data Safety label states precise location is collected and shared, the privacy policy states the opposite . . . 11

6 Impact Analysis 12

7 The Complete Chain 12

8 Health Data & Vulnerable Users 13

9 Consumer Protection & Platform Disclosures 13

10 Data Protection: Article by Article 14

11 Regulatory & Legal Landscape 15

12 Indicators of Compromise & Reproducible Evidence 15

13 Disclosure Timeline & Outcome 16

14 What MyFitnessPal Got Right 17

15 Residual Risk & Recommendations 17

Executive Summary

MyFitnessPal is a food-diary and fitness app published on Google Play by MyFitnessPal, Inc. of Austin, Texas, with more than 100 million downloads. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF MYFITNESSPAL-2026-R1 after a root level code analysis of version 26.33.0. The notice described four High and two Medium findings and put three questions to the operator in writing.

The central finding is an eating-disorder-adjacent classification layer. The shipped app defines named low-calorie thresholds for men and for women, a weight-trend class and a screen called EatingDisorderAdjustGoalComplete, and the operator's own privacy policy states that diary data can allow someone to infer a health condition. Around that core the report documents a blood-glucose reading feature that sits next to the food diary, a policy that declares food-purchase and consumption histories as shared with marketing and advertising partners, an 18-plus claim next to a PEGI 3 rating, SDK bootstraps that run before any consent dialog, and a Play Data Safety label that contradicts the privacy policy on precise location.

The three written questions asked whether a Data Protection Impact Assessment exists for the inference feature, which of the two location statements is accurate, and which GDPR legal basis covers sharing barcode and meal-scan food data with advertising networks. A first follow-up on 12 September 2026 repeated them. On 18 September 2026 a support agent replied on a separate ticket with a pointer to the policy section on additional information for certain jurisdictions. That reply names none of the findings and answers none of the questions. A third message on 19 September 2026, a reminder on 17 October 2026 and a notice on 15 November 2026 drew no further answer. The only message received after the reply of 18 September 2026 is an automated acknowledgement of 15 November 2026 (ticket 5429890), which states that someone from the privacy team will be in touch soon. No such contact followed by 21 November 2026.

This report applies a stricter standard than the first notice in two places. H2 (blood glucose) and H4 (age gate) are reassessed from High to Medium because the data flow in H2 and the absence of an enforcing gate in H4 were not demonstrated. Everything the operator wrote itself, including the Yes to sharing purchasing and consuming histories with advertising partners, is quoted from the live policy and rated on that basis.

The report is published on 21 November 2026, 90 days after delivery of the notice, whether or not the operator answers.

Scope: Root level code analysis of the Google Play release of com.myfitnesspal.android, version 26.33.0 (versionCode 51226): AndroidManifest.xml, decoded resources, network security configuration and the string pool of all seven classes.dex files. Public web pages read by plain HTTP GET: the Google Play listing and Data Safety page, and the privacy policy at myfitnesspal.com/privacy-policy (HTTP 200, effective date 18 March 2025). No account was created, no backend was called, no traffic was intercepted and no runtime instrumentation was used. CVSS v4.0 measures exploitability. The findings in this report are mostly data-governance findings with no attacker, so the printed scores are low and several findings carry an explicit blast-radius escalation.

ID	Severity	Title
H1	HIGH	Locally computed eating-disorder-adjacent inference layer, confirmed by the operator's own policy admission
H2	MEDIUM	Blood-glucose reading pipeline correlated with the food diary inside the same app
H3	HIGH	Barcode and meal-scan food data falls under the operator's own "Commercial Information" category, declared as shared with marketing and advertising partners
H4	MEDIUM	Policy claim of technical measures against under-18 sign-up next to an all-ages PEGI 3 rating, no enforcing gate located
M1	MEDIUM	Advertising and analytics SDK bootstraps run at process start, before any consent dialog, despite a genuine Google UMP and IAB TCF implementation
M2	MEDIUM	Play Data Safety label states precise location is collected and shared, the privacy policy states the opposite

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
H1	HIGH	HIGH	No answer to the DPIA question. Feature unchanged as far as this report covers (version 26.33.0 only).
H2	HIGH	MEDIUM	No answer. Reassessed because no transfer of glucose values was demonstrated.
H3	HIGH	HIGH	No answer to the legal-basis question.
H4	HIGH	MEDIUM	No answer. Reassessed because the absence of an enforcing gate was not demonstrated.
M1	MEDIUM	MEDIUM	No answer.
M2	MEDIUM	MEDIUM	No answer to the question which statement is accurate.

Subject & Operator Analysis

The controller named in the live privacy policy is MyFitnessPal, Inc., 100 Congress Avenue, Suite 400, Austin, TX 78701, USA. Google Play names the same company as developer, with the website myfitnesspal.com and the privacy policy at myfitnesspal.com/privacy-policy. The store listing shows more than 100 million downloads, a rating of 4.2 from 2.91 million reviews, the category Health and Fitness and the labels Contains ads and In-app purchases.

The operator has no establishment in the Union that this analysis could identify. It appointed DataRep as its representative under Art. 27 GDPR for the EU, the UK and Switzerland, with the contact address myfitnesspal@datarep.com and a web form at datarep.com. The policy names privacy@myfitnesspal.com as the privacy and data protection contact. That address is a shared functional inbox and not a named person.

Because Art. 27 representation does not create a main establishment, the one-stop-shop mechanism is not engaged on the facts available. For a matter initiated in Austria the competent supervisory authority is the Austrian Datenschutzbehörde, which was copied on the first notice together with the European Data Protection Supervisor.

Architecture & Data Flow

MyFitnessPal is a native Android application written in Kotlin. The base APK is 67,308,277 bytes, minSdkVersion is 33 (Android 13) and targetSdkVersion is 36. The code sits in seven classes.dex files of about 56.6 MB combined. The manifest declares com.android.vending.BILLING for subscriptions and reads health data through Android Health Connect and the Samsung Health SDK.

- Diary and goals: user-entered food, weight and calorie goals. Named thresholds LOW_CALORIES_MEN_MIN and LOW_CALORIES_WOMEN_MIN, WeightTrend class, EatingDisorderAdjustGoalComplete screen (H1).
- Health platform: Health Connect permissions including READ_BLOOD_GLUCOSE, historic data access enabled, BloodGlucoseActivity and a feature.bloodglucose package (H2).
- Commerce: Instacart promo and Walmart product-match classes, grocery store enum, barcode and meal-scan event constants (H3).
- Consent: Google User Messaging Platform (com.google.android.ump.ConsentInformation) and the IABTCF and IABGPP key set. Facebook SDK deferred by manifest flags.
- Start-up: MobileAdsInitProvider, FirebaseInitProvider and Unity AdsSdkInitializer run at process bind (M1).
- Third-party SDKs: Firebase, Google Mobile Ads, Facebook App Events, AppsFlyer, Amplitude, Unity Ads, Amazon Publisher Services, Fyber / Inneractive, Braze.
- Network configuration: one network_security_config.xml with a debug-overrides block only. No cleartext base-config override and no user-CA trust in production.

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

Findings

H1: Locally computed eating-disorder-adjacent inference layer, confirmed by the operator's own policy admission

HIGH, 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), rated HIGH by blast-radius escalation

The compiled app defines the threshold constants LOW_CALORIES_MEN_MIN and LOW_CALORIES_WOMEN_MIN, a WeightTrend utility class and a dedicated screen named EatingDisorderAdjustGoalComplete that belongs to the flow triggered when a self-set calorie goal is classified against those thresholds. The privacy policy states in the operator's own words that Food and Activity Diary Data may include sensitive personal information when it indicates or allows someone to infer a health condition.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to HIGH because CVSS scores exploitability and gives a documented on-device classification with no demonstrated exposure 0.0. The finding is rated HIGH because the feature targets a vulnerable group, people at risk of eating disorders, because the operator's own policy confirms that diary data can reveal a health condition, and because the app has more than 100 million downloads on Google Play.

```
Lcom/myfitnesspal/dashboard/util/WeightTrend;
LOW_CALORIES_MEN_MIN
LOW_CALORIES_WOMEN_MIN
Lcom/myfitnesspal/feature/goals/ui/activity/EatingDisorderAdjustGoalComplete;
Lcom/myfitnesspal/feature/goals/ui/activity/EatingDisorderAdjustGoalComplete$a;
FragmentEatingDisorderUpdateGoalsCompleteBinding
```

Privacy policy, effective 18 March 2025, read on 23 August 2026: "Food and Activity Diary Data may include sensitive personal information when the information indicates or allows someone to infer a health condition." The same document lists "Inferences drawn from other personal information" as its own data category and states that this category has been shared with service providers within the last 12 months.

What the root level code analysis does not show: the exact combination of calorie goal, weight trend and profile data that opens the flow, whether the computed state is stored, logged as an analytics event or sent to any of the SDKs listed under H3, and how long it is kept. These points are UNVERIFIED. The finding rests on what is shown: the classification logic and the screen it drives exist in the shipped app, and the operator itself documents that diary data can reveal a health condition.

Art. 22 GDPR was raised in the first notice as a question. This report does not assert it, because a goal-adjustment screen is not shown to produce a legal or similarly significant effect.

GDPR: Art. 9(1), Art. 5(1)(a), Art. 35(1), Art. 35(3)(b), Art. 22 (raised as a question only)

Impact: A person who sets a calorie goal below a threshold the operator itself treats as risk-adjacent is classified by the app, and the app responds with a flow named for eating disorders. Whether that classification is kept or shared is the question the operator was asked on 23 August 2026 and has not answered.

Fix: Document in writing whether a Data Protection Impact Assessment under Art. 35 exists for this feature, state the Art. 9(2) condition relied on if the classification is stored or transmitted in any form linked to the user, and confirm that the classification stays on the device.

H2: Blood-glucose reading pipeline correlated with the food diary inside the same app

---

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), reassessed from HIGH in the first notice

The manifest declares android.permission.health.READ_BLOOD_GLUCOSE and the meta-data healthdata_access_historic_data set to true. The app ships its own BloodGlucoseActivity, a feature.bloodglucose package with named use cases for fetching readings by date range, a deep-link route for glucose data and references to the Samsung Health blood-glucose constants. Blood glucose is health data under Art. 9.

RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to MEDIUM because the data category is health data under Art. 9, the feature is built for two health-data back ends (Health Connect and Samsung Health), and it sits in an app that carries nine third-party SDKs. HIGH, as disclosed on 23 August 2026, is withdrawn because no transfer of glucose values was demonstrated.

```
uses-permission: name='android.permission.health.READ_BLOOD_GLUCOSE'
meta-data: name='healthdata_access_historic_data' value='true'

Lcom/myfitnesspal/glucose/ui/BloodGlucoseActivity;
Lcom/myfitnesspal/glucose/ui/BloodGlucoseActivity$GlucoseContent$1$1$1
com.myfitnesspal.feature.bloodglucose.FetchDailyBloodGlucoseUseCaseImpl
fetchDailyBloodGlucoseUseCase / fetchBloodGlucoseByRange / handleBloodGlucose
com.myfitnesspal.shared.deeplink.Routes$handleBloodGlucose$1
Lcom/samsung/android/sdk/healthdata/HealthConstants$BloodGlucose;
```

This is a dedicated feature, not a passthrough permission. Reading glucose values is lawful when the user asks for it and consents to it. What this report cannot establish is whether the app derives any correlation between glucose and logged meals beyond display, whether glucose values reach any of the analytics or CRM SDKs in H3, and whether a consent step specific to this data category exists. These points are UNVERIFIED. For that reason the finding is rated MEDIUM here, reassessed from the HIGH label used in the first notice, which assumed a data flow that the analysis did not demonstrate.

GDPR: Art. 9(1), Art. 9(2)(a), Art. 35(1)

Impact: Users with diabetes or prediabetes who connect a glucose sensor or a health platform to a food diary place health data in a product that also carries an advertising and attribution stack. The report documents the feature and the data category. It does not document a transfer of glucose values.

Fix: State in writing the Art. 9(2)(a) consent mechanism for glucose data, confirm that glucose values are excluded from every analytics, attribution and advertising SDK, and cover the feature in the Art. 35 assessment.

H3: Barcode and meal-scan food data falls under the operator's own "Commercial Information" category, declared as shared with marketing and advertising partners

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), rated HIGH by blast-radius escalation

The privacy policy lists "records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies" as Commercial Information and answers the question whether it was shared within the last 12 months with Yes, naming "Marketing and advertising partners (including social media platforms and third-party advertising networks)". The binary adds named Instacart and Walmart grocery integrations, telemetry event names that identify individual scanned and logged food items, and nine analytics, attribution, advertising and CRM SDKs.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the sharing is not inferred by RFI-IRFOS but declared by the operator in its own policy, the data describes what people eat and take as medication, and the app has more than 100 million downloads on Google Play. The network payload remains UNVERIFIED and is not part of this rating.

```
com.myfitnesspal.feature.mealplanning.ui.onboarding.navigation.PersonaDestination.
    InstacartPromo
com.myfitnesspal.mealplanning.domain.repository.
    InstacartPromoDefaultRepository$isUserEligible$2
ApiWalmartProductMatchResult(groceryItemId=...)
grocery-integration-walmart-android-2024-12
com.myfitnesspal.mealplanning.domain.model.enums.GroceryStore

barcode_scan / barcode_scan_dialog / barcode_scan_manual_match /
    barcode_scan_match_and_logged
barcode_createfood_logged / branded_with_barcode / barcode_miss
food_scanner_accessed / food_scanner_alt_action_clicked /
    food_scanner_start_scan_clicked
meal_scan_search / meal_scan_review_completed / meal_scan_food_removed
streak_food_log_count / STREAK_CELEBRATION_BRAZE
```

SDK	Namespace	References
Firebase / Google Analytics	com/google/firebase/analytics	9
Google Mobile Ads	com/google/android/gms/ads	186
Facebook App Events	com/facebook/appevents	43
AppsFlyer	com/appsflyer	561
Amplitude	com/amplitude	23
Unity Ads	com/unity3d/ads and services	1,269 and 1,242
Amazon Publisher Services	com/amazon/device/ads and aps	78 and 40
Fyber / Inneractive	com/fyber	1,786

SDK	Namespace	References
Braze	com/braze	566

Under ”Personal Information We Collect Directly from You” the policy also lists food, drink and medications a user consumes ”and purchase (via our grocery integrations)”.

UNVERIFIED at network level: the payload of any single analytics event, for example whether branded_with_barcode carries a brand name, a category or neither, and which of the nine SDKs receives barcode-derived events. The finding rests on three documented facts that do not depend on that question: the operator’s own Yes, the named grocery integrations and the named event constants.

GDPR: Art. 5(1)(a), Art. 5(1)(c), Art. 6(1), Art. 13(1)(e)

Impact: A user who scans a branded product to log it creates a consumption record. By the operator’s own disclosure, consumption histories of this kind have reached marketing and advertising partners, including social media platforms and third-party advertising networks. Diet, medication and pregnancy are visible in food logs.

Fix: Name the Art. 6 legal basis for each recipient class, list the data fields that leave the app per event, and remove food-log and barcode events from advertising and social-media destinations unless a valid consent covers them.

H4: Policy claim of technical measures against under-18 sign-up next to an all-ages PEGI 3 rating, no enforcing gate located

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

The privacy policy opens with ”you have to be at least 18 years old to use MyFitnessPal” and states ”We implement technical measures to prevent individuals under 18 years of age from creating an account or otherwise using our Services.” The Google Play listing of the same package carries PEGI 3 in the Austrian store, the lowest rating level. The analysis located one registration class, AgeInputError, which is a text-input validation model.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the app is a diet tracker with an eating-disorder-adjacent flow (H1), the group most affected by such features is young people, and the operator makes a specific claim of technical prevention that the analysis could not match to a mechanism. HIGH, as disclosed on 23 August 2026, is withdrawn because the absence of an enforcing gate was not demonstrated.

```
Lcom/myfitnesspal/feature/registration/shared/textinput/model/AgeInputError;
```

This is a statement about what was not found, and it is read that way. A resources and string-pool pass cannot decide whether logic elsewhere blocks a self-reported under-18 birth date. The documented part is the tension between a specific written claim of technical prevention and the lowest possible age rating. The finding is rated MEDIUM here, reassessed from the HIGH label used in the first notice, because the central question, whether an enforcing mechanism exists, is UNVERIFIED.

GDPR: Art. 8, Art. 5(1)(a), Art. 25(1)

Impact: The product handles calorie goals and an eating-disorder-adjacent flow (H1). If under-18 users can register, they are exactly the group for whom such a flow matters most, and the operator tells readers that this is prevented. The report documents the claim and the rating. It does not document a minor creating an account.

Fix: Describe the age-verification measure in writing, align the Play age rating with the policy, and confirm whether an under-18 birth date blocks registration.

M1: Advertising and analytics SDK bootstraps run at process start, before any consent dialog, despite a genuine Google UMP and IAB TCF implementation

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)

MobileAdsInitProvider (initOrder 100) and FirebaseInitProvider (directBootAware true, initOrder 100) are ContentProviders, and Unity's AdsSdkInitializer starts through Jetpack App Startup. All three run when Android binds the process, before Application.onCreate completes and before any consent dialog can be shown. A real consent implementation exists: com.google.android.ump.ConsentInformation and the IABTCF key set.

```
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider" android:
    initOrder="100" android:exported="false"/>
<provider android:name="com.google.firebase.provider.FirebaseInitProvider" android:
    directBootAware="true" android:initOrder="100" android:exported="false"/>
<provider android:name="androidx.startup.InitializationProvider" ...>
    <meta-data android:name="com.unity3d.services.core.configuration.AdsSdkInitializer
    " android:value="androidx.startup"/>
    ...
</provider>
```

The Facebook SDK is configured the correct way: AutoInitEnabled false, AutoLogAppEventsEnabled false, AdvertiserIDCollectionEnabled false. No deferral flag of the delay_app_measurement_init type was found for the Firebase and Google Ads stack.

Premium: the app declares com.android.vending.BILLING and its store description promises ad-free food logging. No evidence was found that Firebase Analytics, AppsFlyer, Amplitude or Braze are reduced for Premium subscribers. Those are attribution, analytics and CRM SDKs, so ad-free as marketed plausibly describes displayed advertising only.

UNVERIFIED: whether ad personalization is gated by the answer in the UMP dialog, which is a class-level call-order question.

GDPR: Art. 7(1), Art. 25(1), ePrivacy Directive Art. 5(3)

Impact: The consent dialog the operator built cannot gate a component that Android starts first. A subscriber who pays for Premium is not shown to be tracked less than a free user.

Fix: Defer Firebase and Google Ads initialization until the consent state is known, set the Firebase and AdMob manifest flags that delay measurement, and state in writing what Premium changes for analytics and attribution.

M2: Play Data Safety label states precise location is collected and shared, the privacy policy states the opposite

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), rated MEDIUM by blast-radius escalation

The Data Safety label for com.myfitnesspal.android lists Location, Precise location, under both data shared and data collected. The privacy policy states under Geolocation data: ”MyFitnessPal does not collect specific geolocation information.” Neither ACCESS_FINE_LOCATION nor ACCESS_COARSE_LOCATION is declared in the manifest, which matches the policy and contradicts the label.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the contradiction is documented in two operator-authored statements that users and the store rely on, and the app has more than 100 million downloads on Google Play. No exploit is involved and CVSS correctly gives 0.0.

```
Play Data Safety (2026-08-23):   Location > Precise location, collected and shared
Privacy policy, CCPA table:       "MyFitnessPal does not collect specific geolocation
    information."
AndroidManifest.xml:              no ACCESS_FINE_LOCATION, no ACCESS_COARSE_LOCATION
```

The policy separately acknowledges ”general location information (including inferred location based off of your IP address)”. It is possible that the label classifies IP-derived location under Google’s Location category. Which explanation is correct is UNVERIFIED and is the second written question put to the operator.

GDPR: Art. 5(1)(a), Art. 12(1), Art. 13(1)

Impact: Two operator-authored statements about the same processing cannot both be right. A reader who relies on the store label overestimates location tracking, a reader who relies on the policy cannot reconcile it with the label.

Fix: Confirm which statement is accurate, correct the other, and describe the IP-derived location processing in both places.

Impact Analysis

The people affected are users of a food diary on a very large scale. They enter what they eat, what they weigh and what they aim for, and some connect a glucose source. In a product of this kind the entries describe health, even though no form asks for a diagnosis.

- People who restrict food intake. The app has a screen for the case where a calorie goal crosses a threshold the operator itself associates with eating-disorder risk (H1). They have not been told whether that classification is stored or shared.
- People with diabetes or prediabetes who connect glucose readings (H2). They place Art. 9 data in the same product as an advertising and attribution stack.
- People managing a medical condition, a medication schedule or a pregnancy, whose food logs show it (H3). Per the operator's own disclosure, consumption histories have reached marketing and advertising partners.
- Young users. The policy says 18-plus with technical prevention, the store rating says PEGI 3 (H4).
- Every reader of the store label, who is told that precise location is collected and shared while the policy says it is not (M2).

Premium subscribers pay for an ad-free experience. The analysis does not show that the tracking and attribution stack behaves differently for them (M1).

The Complete Chain

The anchor of this report is the food diary and the single path an entry takes from the user's hand to a third party.

- 1. A user finds the app on Google Play, rated PEGI 3, and installs it. At process start, before any screen exists, the Google Ads, Firebase and Unity components initialize (M1).
- 2. The user registers. The policy says under-18 sign-up is technically prevented. The analysis located an input validator named AgeInputError and no enforcing mechanism (H4).
- 3. The user logs meals by barcode or meal scan and sets a calorie goal. Named event constants identify scanned and logged items, and grocery integrations with Instacart and Walmart exist (H3).
- 4. If the goal crosses a threshold held in the app, the user is routed to a flow named for eating disorders (H1).
- 5. A user who connects Health Connect or Samsung Health can have blood glucose read next to the same day's meals (H2).
- 6. By the operator's own policy, purchasing and consuming histories have been shared with marketing and advertising partners in the last 12 months (H3), and the Data Safety label tells the store reader something different about location than the policy does (M2).
- 7. The user asks what legal basis covers this. The operator's reply is a link to the policy.

Every later section of this report refers to one of these seven links. The harm is that a person cannot find out, from the operator, what happens to the most personal thing a diet app holds,

the pattern of what they eat.

Health Data & Vulnerable Users

Art. 9(1) GDPR protects data concerning health. A food log is not automatically health data, but the operator's policy states that it becomes sensitive personal information when it indicates or allows someone to infer a health condition. That sentence defines the legal question for H1, H2 and H3 together.

The app does more than store entries. It classifies a calorie goal against thresholds (H1) and reads glucose values (H2). A controller that builds such features has to be able to say which Art. 9(2) condition it relies on, and Art. 35(3)(b) points to a Data Protection Impact Assessment where special-category data is processed on a large scale. With more than 100 million downloads, scale is not in doubt. Whether the processing of H1 and H2 reaches the threshold of special-category data depends on the open questions of storage and transmission, which is why the DPIA question was asked first.

Consumer Protection & Platform Disclosures

Two operator statements describe the same product to two audiences and disagree. The Data Safety label on Google Play says Precise location is collected and shared. The privacy policy says specific geolocation is not collected. The manifest declares no location permission, which supports the policy (M2).

The store rating is also an operator declaration. PEGI 3 is the lowest rating level. The privacy policy tells readers that the service is not for anyone under 18 (H4). The marketing promise of ad-free food logging for Premium subscribers (M1) describes advertising, and the analysis does not show a reduction of tracking.

Platform accountability is limited to what the platform displays. Google Play shows the label and the rating as submitted by the developer. This report makes no finding against the platform.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a)	Transparency of processing. The label and policy disagree on location (M2). The 18-plus technical-prevention statement is not matched by a located mechanism (H4). Purchasing and consuming histories are shared per the operator's own policy (H3).
Art. 5(1)(c)	Data minimisation. Nine independent third-party SDK families in a food diary (H3).
Art. 6(1)	Legal basis. The operator was asked which basis covers sharing food-purchase data with advertising networks (H3). Unanswered.
Art. 7(1)	Consent must be demonstrable. Three SDK bootstraps run before any dialog (M1).
Art. 8	Conditions for a child's consent. Relevant if under-18 users register, the age of digital consent in Austria is 14 under Section 4 (4) DSG (H4).
Art. 9(1), 9(2)	Health data. Inference layer (H1) and glucose pipeline (H2). The condition relied on has not been stated.
Art. 12(1) and 13(1)	Clear information. Contradictory statements on location (M2) and recipients (H3).
Art. 22	Raised as a question in the first notice. Not asserted in this report (H1).
Art. 25(1)	Data protection by design. Pre-consent initialization (M1) and the age gate (H4).
Art. 27	Representation. Satisfied, DataRep is named. See What MyFitnessPal Got Right.
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.
Art. 35(1), 35(3)(b)	DPIA for the inference feature and the glucose pipeline. The question was asked three times.
ePrivacy Directive Art. 5(3)	Storage of or access to information on the terminal device requires consent unless strictly necessary (M1).

Regulatory & Legal Landscape

The competent authority for a matter initiated in Austria is the Datenschutzbehörde (DSB). The European Data Protection Supervisor was copied for transparency. The activity of RFI-IRFOS is research under Art. 17 StGG (Forschungsfreiheitsgesetz) and follows the coordinated vulnerability disclosure model of ISO/IEC 29147.

The CCPA-style disclosure table in the policy is the source of the strongest operator statements in this report. It is an American-law instrument. This report uses it as evidence of what the operator says it does, and applies GDPR to the processing of EU users.

Industry comparison: the operator ships a real consent platform and defers the Facebook SDK correctly, and it appointed an Art. 27 representative. Those are better practices than many operators outside the Union show. The open questions are about the features that sit on top of that base.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public Google Play build and the public policy page. The APK was obtained from a mirror (APKPure) because no device was available on the analysis day. Package name, developer, app name and version were cross-checked against the live Google Play listing before use. APKPure showed an update date of 20 August 2026 and Google Play showed 14 August 2026, both for the identical version 26.33.0 / 51226.

```
Package       com.myfitnesspal.android
Version       26.33.0 / versionCode 51226
XAPK          SHA-256 6599d515814d1792bc9cb9a84e15d65b7a048e0972db07de17d96ecae50936f4
      (83,514,840 bytes)
base APK      SHA-256 9fbfb44350a38011ba5028b81fca11b2d02453e49df2db3ed6867b3cded5cba4
      (67,308,277 bytes)
config.arm64_v8a.apk SHA-256
    edeb6affb8cdcd6c2e82002e8b1d1eef5d3e9d5d69354cecd9ed3452d0e219eb  (5,046,851 bytes
    )
```

```
aapt2 dump badging com.myfitnesspal.android.apk      permission list, no
    ACCESS_FINE_LOCATION / ACCESS_COARSE_LOCATION
apktool d -f --no-src com.myfitnesspal.android.apk       manifest, res, res/xml/
    network_security_config.xml
strings -n 6 classes*.dex                                303,783 lines, class and
    constant names listed in H1 to H4
```

```
Policy URL        https://www.myfitnesspal.com/privacy-policy   (HTTP 200, effective
    2025-03-18, read 2026-08-23)
Terms URL         https://www.myfitnesspal.com/terms-of-service
Privacy contact   privacy@myfitnesspal.com
Support           support@myfitnesspal.com
Art. 27 rep.      myfitnesspal@datarep.com, http://www.datarep.com/data-request
Support tickets   W67PE1-N51JR (2026-08-23), 5364327 (reply 2026-09-18)
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 26.33.0. Notice REF MYFITNESSPAL-2026-R1 delivered to privacy@myfitnesspal.com and support@myfitnesspal.com, copied to the Datenschutzbehörde and the EDPS. Three written questions. Same day: automated acknowledgment, ticket W67PE1-N51JR.
2026-09-12	Follow-up on the same thread. Three questions repeated, answer requested by 19 September 2026.
2026-09-18	Reply from a support agent named Jean on ticket 5364327. It states that the operator takes data protection seriously and refers to the policy section "Additional Information for Certain Jurisdictions". It names no finding, answers no question and does not quote the REF.
2026-09-19	Third message, copied to the Datenschutzbehörde and the EDPS. Three questions asked a third time.
2026-10-17	Reminder, 35 days before publication. Three questions unchanged.
2026-11-15	Notice from the security team five days before publication, announcing publication on 21 November 2026. The privacy inbox answers with an automated acknowledgement within one minute (ticket 5429890): "Someone from our Privacy Team will be in touch soon."
2026-11-21	No answer to any of the three questions received. Publication, 90 days after delivery of the notice, as announced in every message.

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

What MyFitnessPal Got Right

- A clean network security configuration: one file with a debug-overrides block only, no production cleartext override and no user-CA trust.
- allowBackup is false and no debuggable flag was found.
- A genuine Google UMP and IAB TCF v2 consent implementation is present.
- The Facebook SDK is deferred by manifest flags (AutoInitEnabled, AutoLogAppEventsEnabled and AdvertiserIDCollectionEnabled all false).
- An Art. 27 representative is appointed and named in the policy.
- No hardcoded Firebase or Google API key, no AKIA or sk_ pattern secret and no plaintext Braze or AppsFlyer key was found in the resources or string pool.
- The app contains an intervention flow for risky calorie goals. That is a deliberate safety decision. The open question in H1 is what happens to the data around it.

Residual Risk & Recommendations

All six findings are open. The operator has given no written answer to the DPIA question, the location question or the legal-basis question, neither by 21 November 2026 nor in the generic reply of 18 September 2026. Later builds than 26.33.0 are not covered by this report.

- State in writing whether a Data Protection Impact Assessment exists for the inference feature and the glucose pipeline.
- Say whether the low-calorie classification and glucose values are stored, logged or sent to any SDK.
- Reconcile the Data Safety label and the privacy policy on precise location, and list IP-derived location in both.
- Name a legal basis per recipient class for barcode and meal-scan data, and remove food-log events from advertising and social destinations unless consent covers them.
- Defer Firebase, Google Ads and Unity initialization until consent is known, and say what Premium changes for analytics.
- Describe the under-18 prevention measure and align the Play age rating with the policy.
- Replace the shared privacy inbox with a named, monitored data-protection contact that answers questions in writing.

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 policy page and store listing. No MyFitnessPal servers or accounts were probed. 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 MYFITNESSPAL-2026-R1.