Security & Privacy Disclosure, Final Report

FLOWBIO companion app for the sweat sensor patch, Android (com.flowbio.companionapp)

A sweat sensor app whose only privacy policy belongs to the webshop, with a Play label that claims sexual orientation data.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	FLOWBIO LTD, London, United Kingdom (company number not verified)
Versions Audited	1.0 / versionCode 22, analysed 2026-08-22
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	8: 1 Critical, 2 High, 3 Medium, 1 Low, 1 observation
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`5488de222fbe3d9447c081552593b42ccd7959b4cbd19dee0ad3dbfae5a93b14`

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 Engagement Summary 5

6 Findings 6

6.1 C1: The only privacy policy linked from the Play listing is a webshop policy that never mentions the app, the sensor or any health data . . . 6

6.2 H1: The only consent step in the app is a general Terms and Conditions acceptance, with no dedicated consent for health-related data . . . 7

6.3 H2: The Play Data Safety label says the app collects sexual orientation, and the package contains no field for it . . . 8

6.4 H3: The controller is established in the UK and no Article 27 representative is named for the EU market . . . 9

6.5 M1: The label says no data is shared with third parties, and the package has an OAuth exchange for Garmin, Wahoo, Zwift and Coros . . . 10

6.6 M2: Android Auto Backup is enabled with empty include and exclude rules . . 11

6.7 M3: Login runs through a US-region Auth0 tenant and the policy names no transfer mechanism for it . . . 12

6.8 M4: Server-side physiological profiling is not disclosed as automated processing 13

7 Impact Analysis 13

8 The Complete Chain 14

9 Physiological Data and the Sexual Orientation Declaration 14

10 Data Protection: Article by Article 15

11 Platform Disclosures: Google Play Data Safety 15

12 Regulatory & Legal Landscape 16

13 Indicators of Compromise & Reproducible Evidence 16

14 Disclosure Timeline & Outcome 17

15 What FLOWBIO Got Right 17

16 Residual Risk & Recommendations 18

Executive Summary

FLOWBIO is the companion app for a wearable sweat and sodium sensor patch, marketed as Advanced Hydration Intelligence. The app pairs with the sensor over Bluetooth LE, uploads raw readings to a cloud backend and receives server-computed hydration and recovery recommendations. It is published on Google Play by FLOWBIO LTD of London under the package com.flowbio.companionapp, rated PEGI 3. On 22 August 2026 RFI-IRFOS disclosed eight findings from a root level code analysis of version 1.0 under REF FLOWBIO-2026-R1.

The data is physiological data under Article 4(15) GDPR and not biometric data in the sense of Article 4(14). The package is among the cleanest seen in this programme on third-party code: no advertising, attribution, analytics or session replay SDK, no Firebase and no hardcoded API key. The findings do not describe a hidden tracking operation. They describe a company that cannot point to one published document that describes what its own app processes.

The only privacy policy linked from the Play listing is the policy of the flowbio.com webshop. It never mentions the app, the sensor, Bluetooth or any health data (C1). The Data Safety label states that the app collects sexual orientation, and the package has no field for it (H2). The app has a single general Terms and Conditions acceptance and no dedicated consent step for health-related data (H1). The controller sits in the UK and names no Article 27 representative (H3). Four further items cover the sharing label (M1), backup (M2), the US-region Auth0 tenant (M3) and undisclosed server-side profiling (M4).

The notice of 22 August 2026 went to support@flowbio.com and technical-operations@flowbio.com with the Austrian DSB and the EDPS in copy. A follow-up on 12 September 2026 and a second one on 17 October 2026 restated the findings and the three questions. The only replies are automated Zendesk ticket confirmations. No person has answered a finding or a question. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of the Google Play release 1.0 (versionCode 22): manifest, resources, backup rules and the dex string pool of six classes*.dex files with about 46,800 catalogued classes. The Play listing, the Data Safety page and the privacy policy at flowbio.com/pages/privacy-policy were read from the public sites on 22 August 2026. No FLOWBIO server was called, no account was created, no sensor was paired, no traffic was captured and no runtime instrumentation was used. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	CRITICAL	The only privacy policy linked from the Play listing is a webshop policy that never mentions the app, the sensor or any health data
H1	MEDIUM	The only consent step in the app is a general Terms and Conditions acceptance, with no dedicated consent for health-related data
H2	HIGH	The Play Data Safety label says the app collects sexual orientation, and the package contains no field for it
H3	HIGH	The controller is established in the UK and no Article 27 representative is named for the EU market
M1	INFO	The label says no data is shared with third parties, and the package has an OAuth exchange for Garmin, Wahoo, Zwift and Coros
M2	LOW	Android Auto Backup is enabled with empty include and exclude rules
M3	MEDIUM	Login runs through a US-region Auth0 tenant and the policy names no transfer mechanism for it
M4	MEDIUM	Server-side physiological profiling is not disclosed as automated processing

Finding Status at a Glance

ID	Disclosed	This report	Status on 14 November 2026
C1	CRITICAL	CRITICAL	Open. Question 1 and 3 unanswered.
H1	HIGH	MEDIUM	Open. Question 1 unanswered. Terms text not read.
H2	HIGH	HIGH	Open. Question 2 unanswered.
H3	HIGH	HIGH	Open. No answer received.
M1	MEDIUM	INFO	Observation. Fields exchanged not shown.
M2	MEDIUM	LOW	Open. No answer received.
M3	MEDIUM	MEDIUM	Open. No answer received.
M4	MEDIUM	MEDIUM	Open. No answer received.

Subject & Operator Analysis

The Play developer record names FLOWBIO LTD, K402 The Biscuit Factory, 100 Clements Road, London SE16 4DG, United Kingdom. The privacy policy gives the controller address as 100 Drummond Road, London, ENG, SE16 4DG, GB. Both are recorded as read. The company registration number was not verified. The product is marketed as FLOWBIO and as Advanced Hydration Intelligence (AHi). The support contact is support@flowbio.com and the contact for privacy requests in the policy is technical-operations@flowbio.com. No data protection officer and no press contact were found.

The operator is established in the United Kingdom, which makes it a third-country controller under the GDPR. The UK Information Commissioner is the regulator of its home state, and the Austrian Datenschutzbehörde is the authority for a matter that starts in Austria. The Play listing was observed under the Austrian storefront.

Architecture & Data Flow

The app is a Kotlin and Jetpack Compose application with six dex files and a base APK as part of a 73.6 MB bundle. It pairs over Bluetooth LE with the sweat sensor through BluetoothService and uploads raw readings in batches through ApiServiceWrapper.createBatchReadings. It never computes a profile on the phone. getSweatProfile, getRecommendations and getLatestWorkout are server calls that return the derived results. An onboarding questionnaire collects physiological inputs including Sex. LocationService provides foreground location for ambient temperature lookups. Login runs through Auth0 in a US-region tenant. Integration tokens for Garmin, Wahoo, Zwift and Coros are created through the backend. No native libraries of the operator, no Firebase, no analytics and no advertising SDK are present. minSdk is 29 and targetSdk is 35, so cleartext traffic is denied by platform default and the app adds no network security config.

Engagement Summary

The notice REF FLOWBIO-2026-R1 was delivered on 22 August 2026 at 22:41 UTC to support@flowbio.com and technical-operations@flowbio.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. The letterhead carries the date 23 August 2026, which is the local date in Vienna at that minute. It listed one critical, three high and four medium findings with evidence, credited the clean SDK footprint and asked three questions. The support system confirmed receipt within 20 seconds as ticket 3233.

A follow-up with the findings restated and three questions with a deadline of 26 September 2026 went to the same two addresses on 12 September 2026. A second follow-up from security@rfi-irfos.com on 17 October 2026 repeated the open items and the questions and named 20 November 2026 as the end of the embargo. The ticket system answered with automatic confirmations 3380 and 3719, the latter on 18 October 2026 at 19:37 UTC.

No message from a person at FLOWBIO is on record.

Findings

C1: The only privacy policy linked from the Play listing is a webshop policy that never mentions the app, the sensor or any health data

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, open, rated CRITICAL by blast-radius escalation

The Play listing links to https://flowbio.com/pages/privacy-policy/ (last updated June 5, 2025). Its scope is defined as how FLOWBIO collects, uses and discloses personal information when users visit the site, use its services or make a purchase from flowbio.com. It covers contact, order and payment data for buying the sensor, account credentials and website usage data. Its recipients are "vendors", "business and marketing partners" and "affiliates", none named. It never mentions the Android app, Bluetooth, the sweat sensor, sodium or hydration readings, health or fitness data, biometric login, the Auth0 identity provider, location for weather lookups, or the Garmin, Wahoo, Zwift and Coros integrations that the app description advertises. The binary shows that all of this processing exists: createBatchReadings, getSweatProfile, getRecommendations, BluetoothService, LocationService and createIntegrationToken. Consent to a document that does not describe the processing cannot be specific and informed consent under Article 4(11) and Article 7(2). This is a transparency and legal-basis finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to CRITICAL because the policy is the only public document and does not describe the core health-related processing of the product, so no valid basis for that processing can rest on it. The score is zero because no technical vector exists.

```
Play listing -> Privacy Policy -> https://flowbio.com/pages/privacy-policy/
"Last updated: June 5, 2025"

Scope (verbatim): "how FLOWBIO [...] collects, uses, and discloses your personal
information when you visit, use our services, or make a purchase from flowbio.com."

Binary: ApiServiceWrapper.createBatchReadings, getSweatProfile, getRecommendations,
        BluetoothService.gattCallback, LocationService, createIntegrationToken
```

The privacy policy names the controller as FLOWBIO at 100 Drummond Road, London, ENG, SE16 4DG, GB. The Play developer record gives K402 The Biscuit Factory, 100 Clements Road, London SE16 4DG, United Kingdom. Both addresses are recorded as read.

Impact: A runner or cyclist who pairs the sensor and uploads sweat and sodium readings is told nothing about it. The one document on offer explains how an online shop handles orders. The user has no way to learn who receives the readings, how long they are kept or what the recommendations are built from.

Fix: Publish an app-specific privacy notice that names the sensor readings, the server-side profiles, location, biometric unlock, Auth0 and the four integration partners. Link it from the Play listing and show it before the first upload.

H1: The only consent step in the app is a general Terms and Conditions acceptance, with no dedicated consent for health-related data

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated MEDIUM by blast-radius escalation

A case-insensitive search of all class names for consent, gdpr, cookie, terms and privacy returns three items: ApiServiceWrapper$acceptTermsAndConditions$2, ApiServiceWrapper$getTermsAndConditions$2 and ui.views.TermsAndConditionsView. No Consent, CMP or ConsentManager class exists. The onboarding questionnaire collects the physiological inputs, including Sex, that feed the sweat-rate model, and the only affirmative gate is the single Terms and Conditions acceptance. The Terms text is delivered by the server through getTermsAndConditions and is not bundled in the package. Whether that text separately addresses consent for health-related processing is UNVERIFIED and is the subject of question 1. This is a legal finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the product handles physiological readings and the app has one general acceptance step. The score is zero because no technical vector exists.

```
com.flowbio.companionapp.data.network.api.ApiServiceWrapper$acceptTermsAndConditions$2
com.flowbio.companionapp.data.network.api.ApiServiceWrapper$getTermsAndConditions$2
com.flowbio.companionapp.ui.views.TermsAndConditionsView

OnboardingViewModel, OnboardingModel, QuestionBlock, YesNoQuestionBlock,
    TextFieldQuestionBlock
```

The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the server-delivered text that the user accepts was not read and may contain the consent the package does not show.

Impact: A person who answers a body questionnaire and uploads sweat readings taps one general acceptance. Nothing in the app separates agreement to a contract from agreement to the handling of health-related readings.

Fix: Add a distinct, specific consent step for health-related processing with its own text, record the choice, and allow withdrawal in the app.

H2: The Play Data Safety label says the app collects sexual orientation, and the package contains no field for it

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The Data Safety page fetched on 22 August 2026 reads: "This app may collect these data types: Location, Personal info, and Health and fitness", and expands Personal info as Name, Email address and Sexual orientation. A case-insensitive search for sexual, orientation and gender across all six dex files found only Android layout orientation properties and Transgender.kt, an unused icon from the stock Material icons pack. No form field, onboarding question, data model or API class refers to sexual orientation. The only related field is Sex, used by getSweatProfile for the sweat-rate calculation, which is a proportionate use. Either the declaration is accurate and the data is collected through a channel outside this package, or it is a form error. A server-only or web-only path cannot be excluded from the package. In both cases the public declaration does not match the product. Sexual orientation is a special category under Article 9(1). This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the claim names a special category of personal data in a public declaration about a sports product, and users cannot tell which reading is true. The score is zero because no technical vector exists.

```
https://play.google.com/store/apps/datasafety?id=com.flowbio.companionapp (read
    2026-08-22)

"This app may collect these data types: Location, Personal info, and Health and
    fitness"
Personal info: Name, Email address, and Sexual orientation.

classnames matching sexual|orientation|gender:
  androidx layout Orientation properties (UI boilerplate)
  androidx.compose.material.icons.extended Transgender.kt (unused stock icon)
data.model.Sex  <- the only related field, used by getSweatProfile
```

Impact: A person choosing a sweat sensor reads on the store page that the app collects information about their sexual orientation. If that is true, a sports tool holds a special category of data without telling its users. If it is not true, the company has put a sensitive claim about its own users on a public label.

Fix: Correct the Data Safety form. If sexual orientation is collected anywhere, name the channel, the purpose and the Article 9(2) basis.

H3: The controller is established in the UK and no Article 27 representative is named for the EU market

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

FLOWBIO LTD is a UK-established controller with no identified EU establishment. The Play listing was observed under the Austrian storefront, and the shop on flowbio.com lists every EU member state in its country selector. The app processes physiological data as its continuous core purpose, which fits poorly with the occasional-processing exemption of Article 27(2)(a). No representative is named in the Play listing, the privacy policy or the contact strings of the package. The policy refers to Standard Contractual Clauses for transfers out of Europe and names no representative to whom users in the EU can address requests. This is a legal and transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data is physiological data processed continuously, and users in the Union have no local contact to exercise their rights. The score is zero because no technical vector exists.

Controller as recorded: FLOWBIO LTD, K402 The Biscuit Factory, 100 Clements Road, London SE16 4DG, United Kingdom (Play developer record). Company registration number: not verified. Data protection officer: none found. Article 27 representative: none found.

Impact: A user in Austria or Germany who wants a copy or deletion of their sweat and workout data has a London address and a technical-operations mailbox. Supervisory authorities in the Union have no Member State address to write to.

Fix: Designate a representative established in a Member State where the product is sold, publish the name and address in the policy, and name a data protection contact.

M1: The label says no data is shared with third parties, and the package has an OAuth exchange for Garmin, Wahoo, Zwift and Coros

INFO, no CVSS v4.0 score assigned, disclosed as MEDIUM on 22 August 2026, recorded as an observation

The Data Safety page states that the developer says the app does not share user data with other companies or organisations. The package contains createIntegrationToken, disconnectIntegration, IntegrationType and IntegrationsViewModel$getIntegrationURL, and the store description advertises integrations with Garmin, Wahoo, Zwift and Coros. No partner domain is hardcoded, and the flow runs through the backend, so which fields reach each partner is UNVERIFIED. Google's own definition of sharing excludes transfers made at the user's request, so the label may be correct under the platform's rules. Article 4(2) GDPR is wider, because disclosure by transmission is processing. The finding is a question to the operator and carries no score.

```
com.flowbio.companionapp.data.network.api.ApiServiceWrapper$createIntegrationToken
com.flowbio.companionapp.data.network.api.ApiServiceWrapper$disconnectIntegration
com.flowbio.companionapp.data.model.IntegrationType
com.flowbio.companionapp.ui.integrations.IntegrationsViewModel$getIntegrationURL
```

The notice of 22 August 2026 rated this finding MEDIUM. This report records it as an observation, because the package does not show what is exchanged.

Impact: A user who connects a watch platform wants their workouts to travel there. The open point is which sweat and sodium data travel with them, and whether the user is told.

Fix: List the fields exchanged with each partner, the legal basis, and describe the exchange in the privacy notice.

M2: Android Auto Backup is enabled with empty include and exclude rules

LOW, CVSS v4.0 AV:P/AC:L/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 22 August 2026, open

AndroidManifest.xml sets android:allowBackup to true, and both data_extraction_rules.xml and backup_rules.xml exist with no include or exclude scoping. The whole app-private data directory is therefore eligible for Auto Backup to the user's Google account. What local data the app keeps pending sync is not known from the package. Tokens held in Keystore-backed storage are normally excluded by the platform, so this is not shown to expose a token. The operator has made no explicit decision on what may leave the device through backup.

```
<!-- AndroidManifest.xml -->
android:allowBackup="true"
android:dataExtractionRules="@xml/data_extraction_rules"
android:fullBackupContent="@xml/backup_rules"

<!-- res/xml/data_extraction_rules.xml -->
<data-extraction-rules>
    <cloud-backup />
</data-extraction-rules>

<!-- res/xml/backup_rules.xml -->
<full-backup-content />
```

The notice of 22 August 2026 rated this finding MEDIUM. This report rates it LOW, which is the CVSS band of the exposure that the package shows.

Impact: Physiological readings that wait on the phone for upload may be copied into a cloud backup the user never thought about.

Fix: Exclude health and session data from backup in both rule files, or set allowBackup to false.

M3: Login runs through a US-region Auth0 tenant and the policy names no transfer mechanism for it

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, open, rated MEDIUM by blast-radius escalation

res/values/strings.xml sets the Auth0 domain flowbio-production.us.auth0.com with the scopes openid profile offline_access. Name, email, credentials and long-lived refresh tokens are brokered through a US-region tenant of Auth0 (Okta). The privacy policy refers in general terms to Standard Contractual Clauses and UK equivalents for transfers out of Europe. It does not name Auth0 or Okta and it does not name a transfer mechanism. The current Data Privacy Framework status of the provider was not checked in this analysis and is a question for the operator. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the identity data is tied to a health-related product and the policy names no safeguard for the recipient. The score is zero because no technical vector exists.

```
<string name="Auth0__Audience">https://flowbio.com/api</string>
<string name="Auth0__ClientId">qa6IgjugJ7wEEdxUmOe9P0UGip2dlxkJ</string>
<string name="Auth0__Domain">flowbio-production.us.auth0.com</string>
<string name="Auth0__Scopes">openid profile offline_access</string>
```

Impact: The identity of every user, in connection with a health product, sits with a provider in the United States without the policy telling the user which safeguard applies.

Fix: Name Auth0 and the transfer mechanism in the privacy notice, or move the tenant to an EU region.

M4: Server-side physiological profiling is not disclosed as automated processing

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, open, rated MEDIUM by blast-radius escalation

The app never computes a hydration, sweat or sodium profile on the phone. getSweatProfile and getRecommendations are server round-trips that return derived scores and personalised hydration strategies and recovery plans, built from the uploaded raw readings, questionnaire answers such as Sex, and workout context. The outputs shape training and recovery behaviour. The existing policy and the strings of the package do not disclose that this logic exists, which inputs it uses or any route to a person. Advisory output probably stays below the Article 22 threshold of a legal or similarly significant effect. The duty under Article 13(2)(f) to describe the existence of profiling and the logic involved applies regardless. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the derived scores are more specific than the raw readings and steer the user's training and recovery, and nothing tells the user that they exist. The score is zero because no technical vector exists.

```
ApiServiceWrapper$getSweatProfile
ApiServiceWrapper$getRecommendations
ApiServiceWrapper$getLatestWorkout
ApiServiceWrapper$createBatchReadings  (upload of raw BLE readings)
```

Impact: The user receives instructions on what to drink and when to recover, computed from their body readings on a server. The user is not told that a profile is built or what goes into it.

Fix: Describe the profiling, its inputs and its logic in the privacy notice and give a route to a person for questions.

Impact Analysis

The people affected are athletes who wear the sensor during training and races and use the app to plan hydration and recovery. They hand over body readings, a physiological questionnaire, location and the identity behind an account. The product page and the privacy policy say nothing about this data.

The gap that matters most is the distance between the public documents and the product. The policy describes a webshop. The label describes a collection of sexual orientation that the package does not show. A user cannot work out from either what the company holds about them (C1, H2). Users in the Union who want to use their rights have no local contact (H3). The technical findings are small by comparison and are listed for completeness (M2, M3).

The Complete Chain

Step 1, store: a person reads the Play listing and the Data Safety label, which names a collection of sexual orientation and no sharing with third parties (H2, M1). The privacy link leads to a webshop policy (C1).

Step 2, onboarding: the user answers a physiological questionnaire and taps one general acceptance of terms (H1).

Step 3, pairing and upload: the sensor sends readings by Bluetooth and the app uploads them in batches to the backend. Login runs through a US-region identity tenant (M3).

Step 4, profile: the server returns a sweat profile and recommendations built from the readings and the questionnaire, with no disclosure of the logic (M4).

Step 5, integrations: the user may connect Garmin, Wahoo, Zwift or Coros through a token exchange that the backend brokers (M1).

Step 6, rights: the user wants access or deletion and finds a London address and no representative in the Union (H3). A deletion call exists in the app.

Step 7, device: Auto Backup may copy local data to the user’s Google account without scoping (M2).

Physiological Data and the Sexual Orientation Declaration

Sweat volume, sodium concentration and the inferred hydration and recovery state are physiological data under Article 4(15) GDPR. This report uses that term and does not call the data biometric. Health-related data enjoys the protection of Article 9 where it reveals the state of a person’s health, and the notice treats the data with that care.

The Data Safety label adds a different category. Sexual orientation is a special category under Article 9(1). The package contains no field for it, so the entry is either an error in the form or a collection that happens outside this package. A user who reads the label has no way to tell which it is. The operator can settle it in one sentence.

Data Protection: Article by Article

Article 3(2), territorial scope: engaged by H3. The product is offered to users in the Union.

Article 4(15) and Article 9, health-related and special-category data: engaged by C1, H1 and H2.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H2, M1, M3 and M4.

Article 5(1)(f) and Article 25, integrity and data protection by design: engaged by M2.

Article 5(2), accountability: engaged by C1 and H2. The controller carries the burden of showing which document describes the processing.

Article 7(2) and Article 9(2)(a), consent: engaged by C1 and H1.

Article 13 and Article 14, information to be provided: engaged by C1, H3, M1, M3 and M4. Article 13(2)(f) is engaged by M4.

Article 22, automated individual decisions: asked in M4. Advisory output probably stays below the threshold, and the disclosure duty remains.

Article 27(1), representative: engaged by H3.

Article 44 and Article 46, transfers: engaged by M3.

Platform Disclosures: Google Play Data Safety

The Data Safety label is a declaration made by the developer in Google Play Console. This report attributes its content to FLOWBIO LTD and makes no claim about the conduct of the platform operator.

The label read on 22 August 2026 lists Location, Personal info (Name, Email address and Sexual orientation) and Health and fitness as collected data, states that no data is shared with third parties, and states that deletion can be requested. The deletion claim matches the deleteAccount call in the package and is credited below. The entry for sexual orientation is the subject of H2 and the sharing statement is the subject of M1. The page was not archived at the time of reading and should be fetched again before publication.

The Play rating of PEGI 3 suits the general sporting audience of the product, and no mismatch was observed.

Regulatory & Legal Landscape

The framework applied is the GDPR, with Article 27 for a controller outside the Union, Article 9 for health-related and special-category data and Chapter V for transfers. The operator is established in the United Kingdom and offers its product to users in the Union, which brings Article 3(2) GDPR into play. The UK GDPR applies in its home state.

No obligation under other digital regulation is asserted for this operator, because its classification has not been established. The competent authority for an Austrian initiated matter is the Österreichische Datenschutzbehörde (dsb@dsb.gv.at). The European Data Protection Supervisor (edps@edps.europa.eu) is in copy under the standing practice of the programme. The disclosure follows ISO/IEC 29147 and Art. 17 StGG.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding from the published package. All values are given in full.

Package	com.flowbio.companionapp
Version	1.0 (versionCode 22), analysed 2026-08-22
minSdk / target	29 / 35
base APK SHA-256	5488de222fbe3d9447c081552593b42ccd7959b4cbd19dee0ad3dbfae5a93b14
XAPK SHA-256	2f09207f955b895df8a6626c3ca58e88602c28866f395d68bece65b25f8f1ea7
Auth0 domain	flowbio-production.us.auth0.com
Auth0 client ID	qa6IgjugJ7wEEdxUmOe9P0UGip2dlxkJ
Auth0 audience	https://flowbio.com/api
Privacy policy	https://flowbio.com/pages/privacy-policy/ (updated June 5, 2025)
Operator	FLOWBIO LTD, London

C1	https://flowbio.com/pages/privacy-policy/ (read 2026-08-22)
H1	class names: acceptTermsAndConditions, getTermsAndConditions, TermsAndConditionsView
H2	https://play.google.com/store/apps/datasafety?id=com.flowbio.companionapp (read 2026-08-22)
H2	grep sexual|orientation|gender over 6 dex files: UI properties and Transgender.kt only
H3	Play developer record, privacy policy controller statement, Austrian storefront
M1	createIntegrationToken, disconnectIntegration, IntegrationType, getIntegrationURL
M2	AndroidManifest.xml, res/xml/data_extraction_rules.xml, res/xml/backup_rules.xml
M3	res/values/strings.xml: Auth0__*
M4	getSweatProfile, getRecommendations, createBatchReadings

Reproduction: obtain com.flowbio.companionapp 1.0 from Google Play, check the SHA-256 above, decode the manifest and resources with apktool and read the named files and class names. No device, account or network access is needed for the package findings.

Disclosure Timeline & Outcome

2026-08-22 Notice REF FLOWBIO-2026-R1 delivered at 22:41 UTC (00:41 on 23 August in Vienna) to support@flowbio.com and technical-operations@flowbio.com, CC DSB and EDPS. One critical, three high and four medium findings, three questions asked. Ticket confirmation 3233 within 20 seconds.

2026-09-12 Follow-up to the same addresses with the findings restated and three questions, deadline 26 September 2026, embargo named as 20 November 2026. Ticket confirmation 3380.

2026-10-17 Second follow-up from security@rfi-irfos.com, 34 days before the embargo date, with the open findings and the same three questions.

2026-10-18 Automatic ticket confirmation 3719. No message from a person.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026.

What FLOWBIO Got Right

The third-party footprint is among the cleanest in the programme. Checks across all six dex files for advertising, attribution, analytics, session replay and consent platform SDKs, for Firebase and for SDKs from sanctioned or high-risk jurisdictions returned no match. No code initialises tracking before consent, because no tracking SDK exists. Location use is foreground only, tied to a weather lookup for the sweat-rate model, with no ACCESS_BACKGROUND_LOCATION. No hardcoded Firebase or Google key and no secret pattern was found. The app adds no permissive network security config, and cleartext traffic is denied by platform default. Biometric permissions come from the standard androidx.biometric library and no class ties them to health data. A deleteAccount call exists and matches the Data Safety statement on deletion. The package ships no custom native libraries.

Residual Risk & Recommendations

Open at the date of publication: all eight items, with no written position from the operator. Items that only the operator can close are the notice in C1, the consent step and the Terms text in H1, the label in H2, the representative in H3, the partner exchange in M1, the backup rules in M2, the transfer basis in M3 and the profiling disclosure in M4.

Recommendations: publish an app-specific privacy notice and link it from the Play listing, add a separate consent step for health-related processing, correct the Data Safety form for sexual orientation and for sharing, appoint a representative in a Member State, exclude local data from backup, name Auth0 and the transfer mechanism, and describe the profiling and its inputs.

Statements are limited to the package and the public documents named above.

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.

No FLOWBIO servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF FLOWBIO-2026-R1.