Security & Privacy Disclosure, Final Report

Cycle AI: Chat, Talk & Stories for Android (com.cycleai.android)

An AI character chat app with more than one million installs names no operator in its legal documents, gives four different age rules and declares sexual orientation on Google Play without mentioning it in the privacy policy.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	Beefun Pte. Ltd., Singapore (Google Play developer)
Versions Audited	2.6.0 / 2060014 (pulled 2026-08-20). Builds published since are not analysed.
Notice / Publication	2026-08-20 / 2026-11-18 (90 days, unchanged)
Findings	9: 1 High, 6 Medium, 2 Low (M6 reassessed from Critical)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026

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 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Findings 7

5.1 H1: Sexual orientation declared as collected on Google Play, absent from the privacy policy . . . 7

5.2 M1: Operator, EU representative, data protection officer and transfer basis are not stated in the legal documents . . . 8

5.3 M2: Google Play label and ad stack disagree on sharing and purpose, SDK page omits two components . . . 9

5.4 M3: Policy contradicts itself on whether photos with faces reach third-party AI providers . . . 10

5.5 M4: Age rules contradict each other across the store listing, the terms, the policy and the child safety policy . . . 11

5.6 M5: Consent for the ad stack cannot be shown from the binary . . . 12

5.7 M6: Google API key and Firebase project identifiers are readable in the app resources, key restrictions unknown . . . 13

5.8 L1: Dangerous permissions in the manifest exceed what the Play label declares 14

5.9 L2: Firebase project and class names carry another product name, relationship unverified . . . 14

6 Impact Analysis 15

7 The Complete Chain 15

8 Child Protection & Age Assurance 16

9 Data Protection: Article by Article 16

10 Consumer Protection & Platform Disclosures 17

11 Regulatory & Legal Landscape 17

12 Indicators of Compromise & Reproducible Evidence 17

13 Disclosure Timeline & Outcome 18

14 What the Operator Documents State Clearly 18

15 Residual Risk & Recommendations 19

Executive Summary

Cycle AI is an AI character chat and interactive storytelling app published on Google Play by Beefun Pte. Ltd. of Singapore. The listing shows more than one million downloads, in-app purchases and advertising. On 20 August 2026 RFI-IRFOS sent the operator nine findings from a root level code analysis of version 2.6.0 under REF CYCLEAI-2026-R1, with the Austrian data protection authority and the European Data Protection Supervisor in copy.

The operator has sent no reply. beefunptd.ltd@gmail.com, the only address that accepted delivery, answered neither the notice nor three follow-ups of 28 August, 5 September and 11 September 2026 nor the message of 17 October 2026. privacy@cycleai.ai rejected delivery on 23 August 2026. This report therefore rests on the binary, the operator's published documents and the Google Play pages as read on 14 November 2026.

Reading the documents against each other produces the findings that hold. None of the privacy policy, terms of use, child safety policy and SDK page names a legal entity, an address, a data protection officer or an EU representative (M1). The documents give four different age rules, and the store label now reads PEGI 18 (M4). The operator's own Data safety declaration lists sexual orientation as collected for personalisation, and the privacy policy does not mention it (H1). The same declaration omits advertising as a purpose for device identifiers although the operator's SDK page lists six advertising SDKs (M2). The policy states in one sentence that Face Data is not shared with third parties and in the preceding sentence that uploaded materials go to third-party AI providers (M3).

Several statements in the notice of 20 August 2026 are not carried forward. The key in the resources is a Firebase client key and is rated MEDIUM instead of CRITICAL (M6). The claim that no data is shared is replaced by the label as it reads today. The claim that the SDKs initialise before consent, the absence of an age gate and the use of camera, microphone and location need a runtime trace and stay UNVERIFIED.

Scope: Root level code analysis of the Google Play release 2.6.0 (versionCode 2060014, SHA-256 2d83186eb63e80dca97e8a643f1631662a7a7569b2318044585532dd7bcd4873): manifest, resources, string tables and class inventory. Public pages read by plain HTTP GET: the privacy policy, terms of use, child safety policy and SDK page on cycleai.ai, and the Google Play listing and Data safety page on 14 November 2026. No runtime tracing, no backend call, no account, no key test. Findings that need runtime behaviour are marked UNVERIFIED.

ID	Severity	Title
H1	HIGH	Sexual orientation declared as collected on Google Play, absent from the privacy policy
M1	MEDIUM	Operator, EU representative, data protection officer and transfer basis are not stated in the legal documents
M2	MEDIUM	Google Play label and ad stack disagree on sharing and purpose, SDK page omits two components
M3	MEDIUM	Policy contradicts itself on whether photos with faces reach third-party AI providers
M4	MEDIUM	Age rules contradict each other across the store listing, the terms, the policy and the child safety policy
M5	MEDIUM	Consent for the ad stack cannot be shown from the binary
M6	MEDIUM	Google API key and Firebase project identifiers are readable in the app resources, key restrictions unknown
L1	LOW	Dangerous permissions in the manifest exceed what the Play label declares
L2	LOW	Firebase project and class names carry another product name, relationship unverified

ID	Notice item	This report	Status on 14 November 2026

Finding Status at a Glance

ID	Notice item	This report	Status on 14 November 2026
H1	Item 3 and 7 (Data Safety)	HIGH (new)	Open. Operator has not replied. Label and policy differ on sexual orientation.
M1	Question 2 (authority, representative)	MEDIUM	Open. No entity, representative or DPO named in any document read.
M2	Item 3 and 8 (label, SDK page)	MEDIUM	Restated. The label now lists Purchase history as shared. Advertising purpose and two SDKs still missing.
M3	Item 7 (face data)	MEDIUM	Restated as a contradiction inside the policy. The label discrepancy is not demonstrated.
M4	Item 5 (child code)	MEDIUM	Restated on the four age statements. Absence of an age gate is UNVERIFIED.
M5	Question 1 (consent)	MEDIUM	Open. Runtime trace not performed.
M6	Item 1 and 2 (key, Firebase)	MEDIUM	Reassessed from CRITICAL. Key restrictions unknown.
L1	Item 4 (permissions)	LOW	Restated against the label. The listing statement is not carried.
L2	Item 9 (Dokify)	LOW	Restated as UNVERIFIED.
-	Item 6 (Remote Config)	not carried	Absence of a defaults file in res/xml does not show the absence of defaults in code.

Subject & Operator Analysis

Google Play lists the app as Cycle AI: Chat, Talk & Stories by Beefun Pte. Ltd., with a Singapore address. The listing carries the Contains ads and In-app purchases labels, more than one million downloads and, on 14 November 2026, PEGI 18. The developer contact on the listing is beefunptd.ltd@gmail.com. The listing was last updated on 5 November 2026, after the analysed build 2.6.0 of 18 August 2026.

The legal documents on cycleai.ai call the operator ”Cycle AI” and ”the Company”. They state no legal form, no registered address, no data protection officer and no representative in the Union. The link between the brand and Beefun Pte. Ltd. is visible on Google Play only. The privacy policy dates itself to 8 May 2026, the terms to 20 November 2025 and the child safety policy to 18 July 2025.

The app is offered in Austria, so a controller outside the Union falls under Art. 3(2) GDPR. No establishment in the Union is shown, so no one-stop-shop lead authority exists and every authority where users are affected is competent.

Architecture & Data Flow

The app is built with Flutter. The host activity is com.dokify.app.DokifyActivity. Targets are SDK 35, minimum SDK 23. Backend services visible in the resources are Firebase Analytics, Authentication, Remote Config, Crashlytics, Cloud Messaging, Installations and Storage under project dokify-3c0e2. The binary carries no hardcoded chat backend address. The domains in the resources are www.cycleai.ai (website and legal documents), s.cycleai.ai (short links) and n-res.cycleai.ai (asset CDN).

Advertising and measurement run through AppLovin MAX as mediation layer with Pangle, Unity Ads, Vungle, Mintegral, IronSource, Facebook Audience Network and Google Mobile Ads, plus Adjust for attribution and OMID for viewability. Google Play Billing handles purchases. FFmpegKit handles media.

The privacy policy describes AI processing. Prompts, text and uploaded materials are processed by the operator and, where necessary, transmitted to external AI model providers, named by example as OpenAI, Google and Anthropic. Where the chat traffic goes at runtime was not observed and is UNVERIFIED. The file res/raw/o.json holds the state machine of the AppLovin consent alert.

Findings

H1: Sexual orientation declared as collected on Google Play, absent from the privacy policy

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because sexual orientation is special category data under Art. 9(1) GDPR, the operator itself declares it on a listing with more than one million installs, and the privacy policy it links names no such data and no explicit consent under Art. 9(2)(a). The CVSS vector scores a disclosure gap, it does not capture the sensitivity of the category.

```
Personal info
  Email address     Optional   App functionality, Account management
  User IDs          Optional   App functionality, Account management
  Phone number      Optional   App functionality, Account management
  Sexual orientation           Personalization
```

A search of the saved privacy policy (privacy_policy_clean.txt) and the terms (terms_clean.txt) for the terms orientation, sensitive, special category and explicit consent returns no match. The policy lists face data, contact data, device data, log data, third-party login data (name, profile picture, gender, birthday) and AI chat content. It does not list sexual orientation.

The binary does not show how the attribute is collected, from whom, or which feature uses it for personalisation. Both are UNVERIFIED. The finding rests on the operator's own declaration and on the policy text.

Impact: A person who tells an AI companion about their sexual orientation, or who is asked for it, cannot find out from the privacy policy that the operator records it, why it uses it, or on what legal basis. Exposure of this attribute can lead to discrimination, and consent for it must be explicit and specific.

Fix: State in the privacy policy whether sexual orientation is collected, how, for which purpose and on which Art. 9(2) basis. If the declaration on Google Play is an error, correct the label. If the attribute is collected, obtain explicit consent before collection and document a data protection impact assessment under Art. 35.

M1: Operator, EU representative, data protection officer and transfer basis are not stated in the legal documents

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)

The privacy policy, terms of use, child safety policy and SDK page, all saved from cycleai.ai, name no legal entity, no postal address, no data protection officer and no representative in the Union. The only place the operator is named is the Google Play developer field. The policy contact address is rendered as an obfuscated e-mail token. The transfer section is one generic sentence.

```
Google Play developer      Beefun Pte. Ltd., Singapore
Privacy policy (cycleai.ai/privacy)    entity name: none    address: none    DPO: none
        EU representative: none
Terms of use                           entity name: none (defines "Cycle AI" as the
    Company)
Child safety policy                    entity name: none
SDK page                               entity name: none
Transfers (policy section 9)           "may be transferred to and processed on servers
     located outside your country"
                                       destination: none    mechanism: none
```

The app is offered in Austria on Google Play, so Art. 3(2) GDPR applies to a controller established in Singapore. Art. 27(1) then requires a designated representative in the Union. None is named. The SDK page names providers such as Meta Platforms, Inc., Google LLC, AppLovin Corporation and ByteDance Ltd., and policy section 3.1 names OpenAI, Google and Anthropic as AI providers. The transfer sentence in section 9 leaves open where chat content, device identifiers and photos are processed.

The notice of 20 August 2026 went to beefunptd.ltd@gmail.com and privacy@cycleai.ai. The second address rejected delivery with status 4.1.1 on 23 August 2026.

Impact: A user who wants to access, correct or delete their data, or who wants to complain, finds no named company, address or officer in the documents they accepted. A user in Austria has no representative in the Union to turn to.

Fix: Name the controller with its registered address in the privacy policy, designate and publish an Art. 27 representative, name a contact for data protection matters, and state the destination countries and the Art. 46 safeguards used for each transfer.

M2: Google Play label and ad stack disagree on sharing and purpose, SDK page omits two components

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

The Data safety page of 14 November 2026 lists only Purchase history as shared data. Device or other IDs are listed as collected for App functionality and Analytics, with no Advertising or marketing purpose. The operator's own SDK page lists six advertising SDKs, the manifest declares the advertising ID permission, and the policy states that the services rely on advertising support.

Component	In the binary (2.6.0)	On the SDK page	Purpose on the SDK page
AppLovin MAX	yes	yes	Advertising
Pangle (ByteDance)	yes	yes	Advertising
Unity Ads	yes	yes	Advertising
Vungle (Liftoff)	yes	yes	Advertising
Mintegral	yes	yes	Advertising
Google Mobile Ads	yes	yes	Advertising
Adjust	yes	yes	Attribution
Facebook SDK / Audience Network	yes	yes (Facebook SDK)	Analytics
IronSource	yes	no	not listed
OMID (Open Measurement)	yes	no	not listed

The Terms state that these SDKs may collect identifiers, usage data and diagnostics. Policy section 3.5 reads "Our services rely on advertising support." The consequence for the Play label is a gap between the declared purposes for device identifiers and the purposes the operator's own documents give for the SDKs that receive them.

The notice of 20 August 2026 stated that the label reads "No data shared with third parties". The label read on 14 November 2026 lists Purchase history as shared. The state on 20 August 2026 was not archived, so this report rates the label as it stands on 14 November 2026.

Impact: A person who chooses this app because the store label tells them what happens to their device identifiers gets a different picture than the operator's own terms provide. At least six advertising networks, among them ByteDance's Pangle, are named there.

Fix: Align the Data safety declaration with the SDK inventory, declare advertising as a purpose and device identifiers as shared data where the ad SDKs receive them, and add IronSource and OMID to the SDK page.

M3: Policy contradicts itself on whether photos with faces reach third-party AI providers

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

Policy section 3.1 states that uploaded materials may be processed by third-party AI infrastructure providers such as OpenAI, Google or Anthropic, and in the next sentence that Face Data is not shared with any third party. Face Data is defined in section 1.1 as photos or images that contain facial features. Section 1.1 also states that processing may run on the device or on cloud infrastructure operated by Cycle AI or authorised technology partners.

```
1.1 Face Data: "photos or images that may contain human facial features"
    "processing may occur either directly on the device or through secured cloud
    infrastructure operated by Cycle AI or authorized technology partners"
3.1 "submitted prompts, text, or uploaded materials may be processed by third-party AI
     infrastructure providers"
    "However, we will not share your Face Data with any third party."
8.1 Face Data "deleted after the requested processing task has been completed, except
    where temporary retention is necessary for technical, security, or legal reasons"
```

The policy states that it performs no facial recognition, builds no templates and compares no photos across users. On that description the data is not biometric data under Art. 4(14) GDPR and Art. 9 is not asserted here. The Play label lists Photos as collected for App functionality. A discrepancy between the label and the policy on face data, as stated in the notice of 20 August 2026, is not demonstrated, because the Play label has no face category.

Where uploaded selfies go at runtime is UNVERIFIED. The binary shows no hardcoded AI provider endpoint, and the chat backend address is not visible in the resources.

Impact: Users who upload a photo of themselves, or of another person, for an avatar or image feature cannot tell from the policy whether a third-party AI provider receives it. The photo shows a face and can identify the person.

Fix: State in section 3.1 which AI providers receive uploaded images, for which feature, and under which retention terms. Remove the sentence that excludes Face Data from sharing if image uploads do reach those providers.

M4: Age rules contradict each other across the store listing, the terms, the policy and the child safety policy

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B)

Four documents give four age rules. The terms state Google Play use from age 16 and iOS use from age 17, and add that Cycle AI cannot verify age and that younger users may use the service with a parent's consent. The child safety policy states that only adults may register and that automated systems identify and block accounts that do not meet the age requirement. The privacy policy states that the user is an adult or a guardian consenting for a minor. The Play listing on 14 November 2026 shows PEGI 18.

Document	Statement
Terms 2.2	Google Play: users aged 16 and above (IARC rating)
Terms 2.3	"Cycle AI cannot verify the user's age"
Terms 2.4	Under the limit only "with the consent of your parent or guardian"
Child safety 1.1 and 1.2	"Only adults are allowed" / "automated systems to identify and block accounts"
Privacy policy 6	"you represent that you are an adult or that you are the parent or guardian of such a minor"
Google Play, 14 Nov 2026	PEGI 18

Whether the app asks for age at onboarding was not observed. The notice of 20 August 2026 stated that no age gate exists. That statement is UNVERIFIED because it needs a runtime walk-through. The binary contains the child-directed treatment and under-age flags of the bundled AdMob, AppLovin and Pangle libraries, plus birthday fields. These strings belong to the SDK code and show that the ad SDKs refuse child users. They do not show how the app itself handles age.

Austria sets the age of digital consent at 14 under section 4(4) DSG. A service that accepts minors with parental consent needs a way to verify that consent. The documents describe none.

Impact: A thirteen or fourteen year old who installs an AI character chat app meets a store label of 18, a terms page that says 16 and a child safety page that says adults only. Nothing in the documents tells the family which rule the operator enforces or how.

Fix: Choose one age rule, state it identically in all four documents and the store listing, describe the verification used, and remove the clause that admits minors with parental consent if the product is adults only.

M5: Consent for the ad stack cannot be shown from the binary

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)

The only consent flow found in the resources is the AppLovin terms and privacy alert (state machine in res/raw/o.json, keys is_al_gdpr, cmp_show, gdpr_ok). A search for Usercentrics, Didomi, OneTrust and Quantcast identifiers returned nothing. A search for Google User Messaging Platform classes is not recorded in the working notes, so their absence is UNVERIFIED. The initialisation order of the ad SDKs, Adjust and Firebase relative to any consent screen was not traced.

The notice of 20 August 2026 stated that these SDKs initialise on first launch before any consent screen. That statement needs a runtime trace and is UNVERIFIED. What the binary supports is the presence of ten advertising, measurement and attribution components next to a consent artefact supplied by one of them.

Policy section 2.6 states that advertisements are shown with consent where necessary and otherwise on legitimate interests. Reading and writing of advertising identifiers on the device falls under Art. 5(3) of Directive 2002/58/EC, which Austria implements in section 165(3) TKG 2021, and which requires consent for such access.

Impact: A user in Austria has no way to confirm, from the app or its documents, that device identifiers are withheld from the ad networks until they agree. The operator has not answered the question put to it on 20 August 2026 about the legal basis and the technical measure.

Fix: Use an independent consent platform that records choices per purpose, hold ad SDK and Adjust initialisation until consent is stored, and publish what happens when a user declines.

M6: Google API key and Firebase project identifiers are readable in the app resources, key restrictions unknown

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

The resources hold a Firebase client API key under google_api_key, reused as google_crash_reporting_api_key, together with project dokify-3c0e2, sender 276902961936 and storage bucket dokify-3c0e2.firebasestorage.app. Firebase client keys ship in every app by design. Whether this key is restricted by API and by package and certificate was not tested and cannot be read from the binary. The notice of 20 August 2026 rated the key CRITICAL. This report rates it MEDIUM because no abuse path is demonstrated.

```
google_api_key                AIzaSyDnVnPqNUB2MreCFnwrKEsDBhJ8fNR4N0
google_crash_reporting_api_key same value
project_id                    dokify-3c0e2
gcm_defaultSenderId           276902961936
google_app_id                 1:276902961936:android:b1f4dc3df4f17361fbbb95
google_storage_bucket         dokify-3c0e2.firebasestorage.app
```

The value as recorded has 38 characters, one fewer than the 39 of a complete Google API key. It is printed here exactly as recorded in the notice of 20 August 2026. No request was sent with the key.

Impact: If the key carries no restriction, a third party can use the operator’s Google quota and the operator carries the bill. No user data exposure is demonstrated.

Fix: Check the key in the Google Cloud console and restrict it to the required Firebase APIs and to the app’s package name and signing certificate. Review Firebase Security Rules for the storage bucket.

L1: Dangerous permissions in the manifest exceed what the Play label declares

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B)

The 2.6.0 manifest declares CAMERA, RECORD_AUDIO, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, READ_CONTACTS, READ_CALENDAR, READ_PHONE_STATE, ACTIVITY_RECOGNITION, BODY_SENSORS, SYSTEM_ALERT_WINDOW and legacy storage permissions. The Data safety label lists Photos and Approximate location and none of audio, contacts, calendar, phone state or health sensor data. Whether any feature uses these permissions, and whether they come from the app's own code or from merged SDK manifests, was not established.

The notice of 20 August 2026 stated that the Play listing shows only Photos/Media/Files, Storage and Wi-Fi. The listing read on 14 November 2026 shows no permission list, so that statement is not carried into this report. The finding rests on the manifest compared with the Data safety label.

The notice of 17 October 2026 described the app's declared purpose as health and cycle tracking. The Play listing describes an AI chat and interactive storytelling app. The three questions of 17 October 2026 about location, microphone, camera and key restrictions stay open as questions about permissions the manifest declares.

Impact: A user cannot tell before install whether a chat app can reach the microphone, camera, contacts or a precise location. Runtime permission prompts give a second chance, so the practical risk depends on which features request them. That was not observed.

Fix: Remove permissions no feature uses, and declare on the Data safety label every data type a retained permission can reach.

L2: Firebase project and class names carry another product name, relationship unverified

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B)

The launchable activity is com.dokify.app.DokifyActivity, the application class is com.dokify.app.App, a resource is named dokify_background_color and the Firebase project is dokify-3c0e2. The notice of 20 August 2026 inferred a shared backend with a product called Dokify. The binary shows the names. It does not show whether another product uses the same Firebase project, or whether Dokify is an earlier name of the same operator.

UNVERIFIED. If the project serves several products, user data of this app shares storage and access rules with them, and the policy names none of them. If Dokify is an earlier name of the operator, the finding closes with an explanation.

Impact: Users who read the policy of Cycle AI cannot learn whether their data sits next to the data of another product.

Fix: State whether the Firebase project serves other products and separate the data if it does.

Impact Analysis

The people affected are users of an AI character chat app. The store label of 18 suggests adults, the terms state 16 and the iOS rule 17, and the child safety policy says adults only. The documents admit that age cannot be verified. Teenagers are therefore a realistic part of the user base, and the documents give their families no usable rule (M4).

Users who share personal details with an AI character reveal more than they would in a form. The operator's declaration that it records sexual orientation (H1) makes that concrete. Sexual orientation is special category data, and its exposure can lead to discrimination. Users who upload selfies for avatars cannot tell whether a third-party AI provider receives them (M3). Users who ask who runs the service find a brand name and no company (M1).

The weight of the case lies in the number of installs, the intimate character of the conversation and the lack of any reply. The technical weaknesses are modest. The key in the resources (M6) and the Firebase naming (L2) carry no demonstrated user harm.

The Complete Chain

Step 1, the store page: a user finds the app on Google Play. The label says that device identifiers are collected for app functionality and analytics, that purchase history is shared, that data is encrypted in transit and that deletion can be requested. The page shows PEGI 18, ads and in-app purchases (M2, M4).

Step 2, install: the manifest asks for camera, microphone, precise location, contacts, calendar, phone state and sensor permissions that the label does not list. Whether the app requests them at runtime was not observed (L1).

Step 3, first launch: ten advertising, measurement and attribution components sit in the build next to an AppLovin consent alert. When they start was not traced (M5).

Step 4, sign-up and profile: the label declares email, phone number, user IDs and sexual orientation. The policy mentions login data with gender and birthday and says nothing about orientation (H1).

Step 5, chat and photos: prompts and uploaded materials go to external AI providers. The policy says in the same section that face data is not shared (M3).

Step 6, the question who is responsible: the documents name no company, no address, no officer and no representative. The one address that bounced was the privacy contact used by RFI-IRFOS (M1).

Step 7, age: the user, or the parent, finds four rules (M4). The operator has not answered any of these points.

Child Protection & Age Assurance

The operator publishes a dedicated child safety policy, with a reporting channel, a ban on sexualised content involving anyone under 16 and a promise of automated age checks. The terms contradict it by admitting inability to verify age and by allowing minors with parental consent. The Play listing shows PEGI 18 while the terms still cite a 16 rating. A product that carries AI companion conversations, and that lists a sexual orientation attribute, needs one age rule and a verification method that matches the rule. The binary shows the age-related flags of the bundled advertising SDKs. Those SDKs refuse child users, which makes a child account a technical error path in the ad stack. The behaviour of the app itself in that case is UNVERIFIED.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1, M1, M2, M3 and M4. The documents conflict with each other and with the store label.

Article 5(1)(c) and Article 25, minimisation and data protection by design: engaged by L1. Permissions declared in the manifest exceed the label. Use at runtime is UNVERIFIED.

Article 6(1)(a), Article 7 and Article 4(11), consent: engaged by M5. Consent for advertising identifiers cannot be shown from the binary.

Article 8, child's consent: engaged by M4. Austria sets the age at 14 under section 4(4) DSG. The documents describe no way to verify parental consent.

Article 9(1) and (2)(a), special categories: engaged by H1 through the operator's own declaration. Not asserted for face data (M3), because the policy describes no biometric identification.

Article 12(1), concise, transparent and intelligible information: engaged by M2 and M4.

Article 13(1)(a), (b), (e) and (f), controller, officer, recipients and transfers: engaged by M1, M2 and M3.

Article 27(1), representative: engaged by M1. No representative is named.

Article 28: contingent on L2, if the Firebase project serves other products.

Article 32(1)(b): engaged by M6 as a hygiene point only.

Article 35(3)(b), data protection impact assessment: engaged by H1 if sexual orientation is processed at scale. The question put to the operator on 20 August 2026 stays unanswered.

Articles 44 and 46, transfers: engaged by M1. The policy names no destination and no safeguard.

Directive 2002/58/EC Article 5(3), implemented in section 165(3) TKG 2021: engaged by M5.

Consumer Protection & Platform Disclosures

Google Play publishes the Data safety label with the words "The developer says". The declaration is the operator's statement, and the operator's own documents contradict it on purpose and on sharing (M2, H1). The Play listing, the terms and the child safety policy give different age ratings (M4). A consumer who decides on the strength of these pages decides on inconsistent information.

The operator's policy tells users that the account can be deleted, that subscriptions bill through the platform after deletion, and that logs may be kept in pseudonymised form. Those statements are specific and useful. Their accuracy was not tested.

Regulatory & Legal Landscape

Beefun Pte. Ltd. has no establishment in the Union in the documents read. Every supervisory authority where users are affected is competent. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the notice of 20 August 2026 in copy. The home regulator of the operator is the Personal Data Protection Commission of Singapore. Google Play is the distribution channel and presents the label.

The case belongs to a group of AI companion apps that RFI-IRFOS examines under the same method. The method reads the binary, the published documents and the store pages against each other, regardless of the size of the operator.

Indicators of Compromise & Reproducible Evidence

Every point below is reproducible from the public Google Play build and the public pages named. The working files sit in the case folder.

```
Package       com.cycleai.android
Version       2.6.0 / versionCode 2060014   pulled 2026-08-20
SHA-256       2d83186eb63e80dca97e8a643f1631662a7a7569b2318044585532dd7bcd4873
Firebase      project dokify-3c0e2   sender 276902961936
              app 1:276902961936:android:b1f4dc3df4f17361fbbb95
              bucket dokify-3c0e2.firebasestorage.app
API key       AIzaSyDnVnPqNUB2MreCFnwrKEsDBhJ8fNR4N0
```

```
cycleai.ai/privacy            privacy_policy_clean.txt
cycleai.ai/terms              terms_clean.txt
cycleai.ai/childsafety        childsafety_clean.txt
cycleai.ai/third-party-sdk    third_party_sdk.txt
Google Play listing and Data safety   playstore_snapshot_2026-11-14.txt
```

Reproduction for H1 and M2: open the Data safety page of com.cycleai.android on Google Play and compare it with the privacy policy. Reproduction for M4: read terms sections 2.2 to 2.4, child safety sections 1.1 and 1.2, policy section 6 and the PEGI rating on the listing.

Disclosure Timeline & Outcome

2026-08-20 Notice REF CYCLEAI-2026-R1 to beefunptd.ltd@gmail.com and privacy@cycleai.ai, copy to dsb@dsb.gv.at and edps@edps.europa.eu. Nine findings, three questions.

2026-08-21 to 2026-08-23 privacy@cycleai.ai returns two delay notices and then a final failure, status 4.1.1.

2026-08-28 First follow-up to beefunptd.ltd@gmail.com.

2026-09-05 Second follow-up.

2026-09-11 Third follow-up with the three questions repeated.

2026-10-17 Message from security@rfi-irfos.com to beefunptd.ltd@gmail.com, copy to the same authorities, with three questions on lawful basis for location, use of microphone and camera, and restrictions on the API key.

2026-11-14 No reply of any kind from the operator is recorded. Data safety page and listing read on this date.

The description of the app as a health and cycle tracking app in the message of 17 October 2026 is withdrawn. The Play listing describes an AI chat and storytelling app.

What the Operator Documents State Clearly

The privacy policy lists data subject rights in full, including withdrawal of consent, portability and complaint. It states a retention period of 180 days after the end of the contract. It states that face data is processed temporarily and not used for recognition. The Play label states encryption in transit and a way to request deletion. The child safety policy offers a reporting channel. The build declares no network security configuration, and on target SDK 35 Android blocks cleartext traffic by default. Whether the manifest sets usesCleartextTraffic was not recorded.

Residual Risk & Recommendations

Open on 14 November 2026: all nine findings, because the operator has not replied. The runtime questions stay open. They are the initialisation order of the ad stack and Firebase, the use of camera, microphone and location, the presence of an age gate, the destination of photos and chat content, and the restrictions on the API key. Builds since 2.6.0 were not analysed.

Recommendations: name the controller, address, representative and contact in the privacy policy. Explain the sexual orientation attribute or correct the label. Adopt one age rule and a verification method. Align the Data safety declaration with the SDK inventory. Add IronSource and OMID to the SDK page. Hold ad SDK initialisation until consent. Remove unused permissions. Restrict the Google API key.

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 public pages read by plain GET. No Cycle AI servers or accounts were probed and no key was tested. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF CYCLEAI-2026-R1.