

IODA Inc. — Privacy Policy

Effective Date: May 5, 2026 **Last Updated:** May 5, 2026 **Applies to:** ioda.pro website, iOS application, Android application, and all related services **Contact:** ioda.council@gmail.com **Canonical URL:** https://www.ioda.pro/ioda_LEGAL_Privacy_Policy_FINAL.pdf

1. Overview

This Privacy Policy explains how IODA Inc. ("IODA," "we," "us," or "our") collects, uses, discloses, and otherwise processes information in connection with the IODA website (ioda.pro and any successor websites), our mobile applications for iOS and Android, and related services (collectively, the "Services").

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy. If you do not agree, please do not use the Services.

IMPORTANT. IODA is designed for self-discovery and reflection. It is not therapy, does not provide medical or mental health diagnosis or treatment, and is not an emergency service. If you or someone else is in immediate danger, call 911 (United States) or your local emergency number. In the United States, you may also call or text 988 (Suicide & Crisis Lifeline).

Transparency note. The Services include AI-generated outputs. When you interact with IODA, you may be interacting with an AI system designed to support reflective exercises. See Section 7 (AI and Automated Processing).

1.1 Data Controller and Contact

Data Controller: IODA Inc. (United States). **Registered Address:** 50 Murray Street, New York, NY 10007, United States. **Privacy Contact Email:** ioda.council@gmail.com

1.2 Scope

This Privacy Policy applies to the Services, including any future features, platforms, and integrations that link to this Privacy Policy. If we introduce new features that materially change our data practices, we will update this Privacy Policy before launch and obtain any additional consents required by applicable law.

2. Key Definitions

Capitalized terms not defined elsewhere have the meanings below.

- **"Account Data"** means information used to create and manage your account (for example, name, email address, authentication method, date of birth, and settings).

- **"Interaction Data"** means your responses and activity within the Services, including structured inputs (for example, swipe cards, sliders, multiple choice, rankings) and any free-text inputs or transcripts.
 - **"User Content"** means information you submit through the Services, including Interaction Data, feedback, and other content.
 - **"AI-Derived Data"** means information generated by our AI systems based on your inputs (for example, paraphrased summaries, profile signals and weights, keywords, archetypes, superpowers, personality traits, and related descriptions).
 - **"Mirror"** means your evolving profile composed of keywords, archetypes, superpowers, personality traits, and related descriptions.
 - **"Animal Guide"** means the companion identity assigned during onboarding (for example, "Desert Coyote"), including the associated illustration and descriptive text.
 - **"Personal Information"** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to you.
 - **"Sensitive Personal Information"** means Personal Information that is considered sensitive under applicable laws, including information that may reveal mental or emotional well-being (for example, reflective content).
 - **"Special Category Data"** means personal data that is treated as special category data under the General Data Protection Regulation ("GDPR") and the United Kingdom General Data Protection Regulation ("UK GDPR") (for example, data concerning health, including mental health or emotional well-being).
-

3. Information We Collect

We collect information in three ways: (a) information you provide; (b) information collected automatically; and (c) information we generate or derive (for example, AI-derived profile updates).

3.1 Information You Provide

3.1.1 Account creation and authentication

- Identifiers and contact details (name, email address).
- Date of birth (used for eligibility and age gating).
- Sex selection (Male, Female, or Irrelevant) if you choose to provide it.
- Authentication and verification information (for example, OAuth tokens, login timestamps, password reset requests, and verification codes sent by email).
- Social-login identifiers from third-party identity providers (Apple and Google) as permitted by your settings and the provider's policies.

3.1.2 Photos for Animal Guide assignment

During onboarding, you may upload or take a photo so we can assign your Animal Guide. Supported formats include JPG, JPEG, PNG, and WEBP, up to 20 MB per file. We process the photo solely to assign an Animal Guide.

We do not retain your photo in your account or store it as a user asset on our servers. To perform the analysis, the photo is transmitted to a third-party AI vision provider (see Section 6.1), which may retain the image for a limited period under its standard data-handling practices for safety and abuse-monitoring purposes. We do not control that provider's retention period.

We do not use your photo for advertising, identification, verification, or tracking. We do not sell, lease, trade, or otherwise profit from any biometric data. See Section 8 and **Appendix A** (Biometric Privacy Notice and Consent).

3.1.3 Interaction Data (structured, free-text, and voice)

- Structured responses (for example, swipe cards, slider values, multiple-choice selections, rankings, short answers).
- Free-text responses you type.
- Voice responses you dictate, and the corresponding text transcripts.
- Session metadata (for example, timestamps, completion status, streaks, progress).
- Sharing actions you initiate (for example, generating a shareable card or link).

Voice responses are transmitted to a third-party speech-to-text provider for transcription. We retain the resulting text transcript. We do not retain the underlying audio recording in your account as a stored audio file. The speech-to-text provider may retain the audio for a limited period under its standard data-handling practices for safety and abuse-monitoring purposes. We do not control that provider's retention period.

3.1.4 Support communications and feedback

If you contact us or submit feedback, we collect the content of your message and any information you choose to provide (for example, contact details and a diagnostic snapshot you authorize when using the in-app "Contact Support" function).

3.2 Information We Generate or Derive

3.2.1 AI-derived profile data (Mirror updates)

We generate and store AI-Derived Data to provide personalization and update your Mirror. This may include paraphrased evidence summaries derived from your Interaction Data; profile signals, weights, and updates; narrative profile descriptions; contextual Animal Guide messages; and summaries of Nodes or Chapters.

In general, the processing flow is: you answer a prompt; we store your response as Interaction Data; our AI layer generates a profile update (for example, a paraphrased evidence summary and profile-signal updates); and we store that update as part of your Mirror. We may generate embeddings or other vector representations of certain derived text to support retrieval and personalization.

3.2.2 Optional chat conversations

If we offer an optional conversational chat feature and you choose to use it, we may store chat messages to provide the feature and support continuity.

3.3 Information Collected Automatically

- Device and app data (for example, device model, operating system, app version, language).
- Log data (for example, IP address, timestamps, structured event logs, diagnostic data).
- Usage metrics (for example, screens viewed, features used, and time spent).
- Approximate location derived from IP address (typically city- or region-level).

We do not currently use third-party analytics or crash-reporting SDKs. Diagnostic information is collected through our own backend (including session-lifecycle events and timeout telemetry) and is associated with your account identifier for the purposes described in Section 4. Diagnostic logs are typically retained for up to 24 months.

3.4 Information from Third Parties

If you use third-party authentication providers (Apple or Google), we receive limited account information from them as authorized by you during the authentication flow (typically your name and email address). We do not access your contacts, posts, or other content from these providers.

3.5 Payments and Subscriptions

If we offer subscriptions or in-app purchases in the future, those transactions will be processed through Apple's App Store or Google Play billing. We will not receive or store your full payment-card number or bank details. We may receive transaction metadata (for example, subscription status, product purchased, purchase date, renewal date, and region) to provide the purchased features and for accounting.

4. How We Use Information

We use information for the following purposes:

- Provide and operate the Services (account creation, authentication, delivering Nodes and Chapters, updating your Mirror, and displaying your Animal Guide).
- Provide AI-powered personalization, including "Receive Advice" and "Go Deeper" features and contextual Animal Guide messaging.

- Maintain progress and gamification features (streaks, progression path, rewards, tags, archetypes, badges).
 - Enable sharing features (generating shareable cards and links).
 - Send service-related communications (verification codes, password resets, security notices, changes to terms or policies) and, where permitted, promotional messages (you may opt out of non-essential marketing).
 - Monitor safety, detect potential crisis or self-harm signals, and surface relevant resources. We do not provide emergency services.
 - Understand usage and improve the Services (debugging, quality assurance, analytics, and product development).
 - Protect the security and integrity of the Services, prevent fraud, and enforce our terms.
 - Comply with legal obligations and respond to lawful requests.
-

5. Legal Bases for Processing (GDPR / UK GDPR)

If you are located in the European Economic Area, the United Kingdom, Switzerland, or another jurisdiction requiring a lawful basis, we process Personal Information under the following bases, as applicable.

5.1 Contract

We process Personal Information to perform our contract with you to deliver the core mechanics of the Services, such as creating your account, authenticating you, delivering Nodes and Chapters, maintaining your progress, and storing your Mirror updates.

5.2 Consent and explicit consent (Sensitive, Special Category, and Biometric)

Where required by law, we rely on your consent in addition to the contractual basis above. This includes:

- **Explicit consent** to process Special Category Data (for example, the portion of your reflective responses that may reveal mental or emotional well-being) in order to provide personalized features such as the Mirror.
- **Consent** to process your onboarding photo (and any associated biometric processing) solely to assign your Animal Guide.
- **Consent** for optional features (for example, optional chat features or marketing communications).

You may withdraw consent at any time. If certain processing is necessary to provide core features, withdrawal may mean we cannot continue providing those features and you may need to delete your account.

5.3 Legitimate interests

We may process Personal Information where it is necessary for our legitimate interests, such as improving the Services, preventing fraud, and securing our systems, provided those interests are not overridden by your rights.

5.4 Legal obligations

We may process information to comply with legal obligations, including tax, accounting, and responding to lawful requests.

6. How We Share Information

We do not sell your Personal Information. We share information only in the limited circumstances described below.

6.1 Service providers (processors)

We share Personal Information with vendors who help us operate the Services, including:

- **Identity and authentication providers** (Apple and Google) to enable login and verification.
- **AI processing providers** to generate AI outputs and profile updates, including large-language-model providers, vision providers used for Animal Guide assignment, and speech-to-text providers used for voice transcription.
- **Cloud hosting and infrastructure providers** to store and process data.
- **Customer-support tools** to receive and respond to user inquiries.

We require service providers to process Personal Information on our behalf and under contractual restrictions. Some AI service providers may process limited data for safety and abuse-monitoring purposes under their own published policies; we do not authorize any provider to use your data to train general-purpose models. An up-to-date list of material sub-processors is available on request to ioda.council@gmail.com.

6.2 Sharing initiated by you

If you choose to share an Animal Card, Trait Card, or other content via social platforms or links, we generate the shared asset or link at your direction. Content you share may become public and may be collected by others. Use caution when sharing.

6.3 Legal, safety, and protection disclosures

We may disclose information if we believe in good faith that disclosure is necessary to: (a) comply with law or legal process; (b) protect the rights, property, or safety of IODA, our users, or others; (c) enforce our terms; or (d) detect, prevent, or address security or technical issues.

6.4 Business transfers

If we are involved in a merger, acquisition, financing, reorganization, bankruptcy, or sale of assets, information may be transferred as part of that transaction, subject to applicable law and appropriate safeguards.

6.5 Aggregated or de-identified information

We may share aggregated, anonymized, or de-identified information that cannot reasonably be used to identify you.

7. AI and Automated Processing Disclosures

7.1 How AI is used

IODA uses AI to generate and personalize content, including Mirror updates, trait descriptions, contextual messaging from your Animal Guide, "Receive Advice" guidance, and "Go Deeper" exploration prompts. AI outputs are generated based on your Interaction Data and your Mirror profile.

7.2 AI systems overview

- A journey-orchestration layer that selects and sequences interactions and uses large language models to generate certain content.
- A photo-analysis system used during onboarding to assign an Animal Guide.
- Optional conversational features that may use retrieval-augmented generation grounded in your stored context.

7.3 AI-generated content is informational

AI outputs are for self-reflection and informational purposes only. They may be incomplete, inaccurate, or inappropriate for your situation. Do not rely on the Services for medical, legal, financial, or other professional advice.

7.4 No automated decisions with legal or similarly significant effects

IODA does not make decisions that produce legal effects or similarly significant effects concerning you (for example, decisions about employment, housing, insurance, or credit). Profile assignments (keywords, archetypes, and the like) are for personal reflection.

7.5 AI providers

We use third-party AI service providers to support text generation, photo analysis, voice transcription, and embeddings. Our contracts and configurations with these providers prohibit them from using your data to train general-purpose models. Some providers may retain limited data for safety and abuse-monitoring purposes under their own published policies; we do not control those retention periods. The list of material AI sub-processors is available on request.

7.6 Safety and human oversight

We use safety measures designed to identify certain high-risk content (for example, self-harm indicators) and to surface appropriate resources. We do not monitor users in real time and do not provide emergency response. In limited circumstances, we may review certain flagged events to improve safety systems and address misuse.

7.7 Your controls

You may delete your account at any time through Settings within the application. Account deletion permanently removes your Personal Information from our active systems as described in Section 9.

8. Photo Processing and Biometric Data

During onboarding, you may upload or take a photo so we can assign your Animal Guide. We do not retain the photo in your account or store it as a user asset on our servers. The photo is transmitted to a third-party AI vision provider for the assignment and is deleted from our systems following processing. The vision provider may retain the image for a limited period under its standard data-handling practices.

Depending on the processing method and your jurisdiction, analyzing a face photo may be considered processing biometric data. See **Appendix A** (Biometric Privacy Notice and Consent) for additional disclosures.

9. Data Retention and Account Deletion

We retain Personal Information for as long as necessary to provide the Services and for legitimate business purposes, unless a longer retention period is required or permitted by law. In general, we retain most account-related and interaction-related data until you delete your account, except for device and usage data and diagnostic logs, which we retain for up to 24 months.

9.1 Retention summary by category

Data Category	Stored?	Typical Retention	Notes
Account Data	Yes	Until account deletion	Includes identifiers, date of birth, settings
Structured interaction responses	Yes	Until account deletion	Choices, values, rankings
Free-text responses and transcripts	Yes	Until account deletion	Audio is not stored as a user asset
AI-derived summaries and profile updates	Yes	Until account deletion	Paraphrased evidence, signals, embeddings
Journey progress, streaks, badges	Yes		Progress tracking and rewards

Data Category	Stored?	Typical Retention	Notes
		Until account deletion	
Onboarding photo	No	Not stored as a user asset	Third-party AI provider may retain transiently
Authentication tokens	Yes	Session-based, as needed	Stored securely
Payment card numbers	No	Not applicable	Handled by Apple or Google
Device and usage data	Yes	Up to 24 months	Aggregated or de-identified where possible
Diagnostic and audit logs	Yes	Up to 24 months	Linked to user identifier; used for debugging and analytics

Retention periods may vary by jurisdiction and operational requirements. Where feasible, we de-identify or aggregate data used for analytics and product improvement.

9.2 Account deletion

You may delete your account at any time through Settings within the application. When you request account deletion, we delete your Personal Information from our active systems within 30 days, except where retention is required or permitted by law. Residual copies in encrypted backups are overwritten on a rolling basis, typically within 90 days. This action cannot be undone.

10. International Data Transfers

IODA is based in the United States, and we and our service providers may process and store information in the United States and other countries.

For users in the European Economic Area or the United Kingdom, where we transfer Personal Information internationally, we rely on appropriate safeguards such as the Standard Contractual Clauses approved by the European Commission and the United Kingdom International Data Transfer Addendum, or other lawful transfer mechanisms.

11. Your Rights and Choices

11.1 In-app controls

- Access and update certain account details in Settings.
- Delete your account.

11.2 EEA and UK (GDPR / UK GDPR) rights

- Request access to your Personal Information.
- Request correction or rectification.
- Request deletion (erasure).
- Request restriction of processing.
- Object to processing (including processing based on legitimate interests).
- Request data portability.
- Withdraw consent at any time where processing is based on consent.
- Lodge a complaint with your local supervisory authority. A list of EEA supervisory authorities is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

11.3 United States privacy rights (including California)

Depending on your United States state of residence, you may have rights to access, delete, correct, and obtain a copy of your Personal Information, and to opt out of certain processing.

California (CCPA / CPRA) notice. We do not sell Personal Information and do not share Personal Information for cross-context behavioral advertising as of the Effective Date of this Privacy Policy. If this changes, we will update this Privacy Policy and provide opt-out mechanisms and honor Global Privacy Control ("GPC") signals where required.

You may have the right to limit the use and disclosure of Sensitive Personal Information to what is necessary to provide the Services.

11.4 How to exercise your rights

You may exercise many rights through Settings within the application. You may also contact us at **ioda.council@gmail.com**. We may need to verify your identity before responding. Where permitted, you may use an authorized agent to submit requests on your behalf.

We will respond within the time required by applicable law, including (a) within 30 days for GDPR and UK GDPR requests (extendable where permitted) and (b) within 45 days for many United States state privacy requests (extendable where permitted).

11.5 Appeals (certain United States states)

If we deny your request, you may have the right to appeal. To appeal, contact us at **ioda.council@gmail.com** with "Privacy Appeal" in the subject line.

12. Cookies, Tracking Technologies, and Global Privacy Control

Our website may use cookies and similar technologies for strictly necessary functions (for example, login and security), preferences, and analytics. Where required, we provide a cookie notice and preference controls.

12.1 In-app tracking

We do not use cross-app tracking technologies (such as the iOS Identifier for Advertisers, "IDFA"). We do not display the iOS App Tracking Transparency prompt because we do not engage in tracking as defined by Apple's policies.

12.2 Global Privacy Control (GPC)

Where applicable, we treat a browser-based Global Privacy Control signal as a request to opt out of the sale or sharing of Personal Information, as those terms are defined by applicable law.

12.3 Do Not Track (DNT)

Some browsers offer "Do Not Track" signals. Because there is no universal standard, our website may not respond to DNT signals. We will, however, provide choices through cookie preference tools where required.

13. Children's Privacy

The Services are not directed to children. By default, the Services are intended for users who are at least 18 years old. We do not knowingly collect Personal Information from children under 13. If you believe a child has provided us Personal Information, contact us at ioda.council@gmail.com and we will take appropriate steps to delete it.

If we later permit younger users (for example, ages 13 to 17), we will implement additional protections and, where required, obtain verifiable parental consent and youth-specific safeguards.

14. Security

We use administrative, technical, and organizational measures appropriate to the risk to protect Personal Information. These include encryption in transit using Transport Layer Security ("TLS"), encryption at rest where appropriate, role-based access controls, audit logging, and a documented incident response process. No method of transmission or storage is, however, 100% secure.

Breach notification. If a breach affects your Personal Information, we will notify you and any applicable regulators as required by law, including, where applicable, within 72 hours of becoming aware of the breach as required by Article 33 of the GDPR.

15. Sensitive Self-Reflection Data

Because the Services involve personal reflection, Interaction Data may include Sensitive Personal Information and may be treated as Special Category Data under GDPR and UK GDPR.

- We process reflective data solely to provide and improve the Services.
 - We do not share identifiable reflective data with advertisers or data brokers.
 - We use de-identified or aggregated data where possible for analytics and improvement.
 - Where required, we obtain explicit consent before processing Special Category Data.
-

16. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will provide notice through the Services, by email, or as otherwise required by law. The "Last Updated" date reflects the most recent version.

17. Contact Us

For privacy inquiries, requests, or complaints, contact us at ioda.council@gmail.com.

IODA Inc. Attn: Privacy Inquiries 50 Murray Street, New York, NY 10007, United States

If required, we will provide contact information for a Data Protection Officer or an EU/UK representative here.

Appendix A — Biometric Privacy Notice and Consent (Illinois BIPA, Texas, Washington)

This Appendix applies only to the extent our Animal Guide assignment process is considered to involve biometric data under applicable law.

1. **Purpose.** We process your onboarding photo solely to assign an Animal Guide and to provide the associated Animal Card and identity element within the Services.
2. **No persistent storage by IODA.** We do not store your photo in your account or as a user asset on our servers after processing. We do not maintain a biometric template for identification, verification, or tracking.
3. **Third-party processor retention.** The photo is transmitted to a third-party AI vision provider for the assignment. That provider may retain the image for a limited period under its standard data-handling practices for safety and abuse-monitoring purposes. We do not control that provider's retention period.

4. **Disclosure.** We do not sell, lease, trade, or otherwise profit from biometric data. We disclose the photo only to our processing vendor solely to perform Animal Guide assignment, subject to contractual restrictions and security measures.
 5. **Consent.** By uploading or capturing a photo for Animal Guide assignment, you consent to the processing described in this Appendix.
-

Appendix B — California (CCPA / CPRA) Notice at Collection (Summary)

This summary is provided for California residents and is intended to supplement the disclosures above.

- **Categories of Personal Information collected** may include: identifiers (email), account information, interaction and self-reflection data, device and usage data, and (if introduced) subscription-status metadata.
- **Sensitive Personal Information** may include reflective content that could reveal mental well-being information, and date of birth used for age gating.
- **Purposes:** provide and improve the Services, personalization, safety, fraud prevention, and support.
- **No sale or sharing.** We do not sell Personal Information and do not share Personal Information for cross-context behavioral advertising as of the Effective Date. If this changes, we will update this Privacy Policy and provide opt-out mechanisms.
- **Shine the Light (California Civil Code §1798.83).** We do not disclose Personal Information to third parties for those third parties' own direct marketing purposes.