Third-Party Services Data Usage Statement

1. Introduction

This Third-Party Services Data Usage Statement explains how Aivine ("we," "our," or "us") interacts with third-party service providers, the data they collect, and how they use and protect your information. By using our services, you acknowledge that certain data may be processed by these third-party providers under their respective policies.

2. Third-Party Service Providers and Their Roles

2.1 OpenAI – AI Model Services

- **Provider**: OpenAI, L.L.C.

- **Website**: https://openai.com

- **Data Collected**: User prompts, chat messages, request metadata.

- **Purpose**: ChatGPT API is used to generate intelligent responses for astrology readings, tarot interpretation, and dream analysis.

- **Data Sharing**: OpenAI processes text data to generate responses but does not retain personally identifiable information.

- **Security Measures**: All communications are encrypted and processed in accordance with OpenAI's security protocols.

2.2 AstrologyAPI – Astrological Chart Service

- **Provider**: RAHU Technologies Pvt. Ltd.

- **Website**: https://astrologyapi.com

- **Data Collected**: Date of birth, time of birth, geographic coordinates (latitude & longitude).

- **Purpose**: Used to calculate personalized planetary charts including planets, houses, and aspects.

- **Data Sharing**: This data is sent securely to AstrologyAPI servers for real-time chart calculation and is not stored long-term.

- **Security Measures**: HTTPS encryption is used; strict data handling policies are followed.

2.3 Google Firebase – Authentication, Analytics & Messaging

- **Provider**: Google LLC

- **Website**: https://firebase.google.com

- **Data Collected**:

  - User email, login credentials (via OAuth)

  - Usage events, session data (for analytics)

  - In-app chat content and metadata (for messaging)

- **Purpose**:

  - User authentication and login

  - Anonymous usage analytics

  - Real-time IM/chat features

- **Data Sharing**: Firebase stores and processes user data under Google's privacy terms. Some non-sensitive events may be auto-tracked.

- **Security Measures**: Google uses encryption, access restriction, and auditing controls.

2.4 Google Cloud – Cloud Storage

- **Provider**: Google LLC

- **Website**: https://cloud.google.com

- **Data Collected**: User media files (images, voice messages), chart data, backups.

- **Purpose**: Used to store user-generated content and chart rendering assets in a secure and scalable manner.

- **Data Sharing**: Google Cloud does not access or share data without legal requirement.

- **Security Measures**: Industry-standard encryption and access control policies are enforced.

2.5 GoDaddy – Email Services

- **Provider**: GoDaddy Operating Company, LLC

- **Website**: https://www.godaddy.com

- **Data Collected**: Recipient email address, delivery logs, IP metadata.

- **Purpose**: Used to send verification codes and service-related messages to users.

- **Data Sharing**: Only operational metadata is logged for delivery and spam protection.

- **Security Measures**: Email transmission is secured and monitored for abuse prevention.

2.6 Google Cloud Text-to-Speech – AI Voice Synthesis

- **Provider**: Google LLC

- **Website**: https://cloud.google.com/text-to-speech

- **Data Collected**: Input text (user messages or system-generated content), language, voice parameters.

- **Purpose**: Used to generate lifelike spoken responses using neural voice models (e.g., Chirp 3 HD) in selected languages.

- **Data Sharing**: Input text is sent to Google's Text-to-Speech engine in real-time and is not stored beyond the session.

- **Security Measures**: All data is transmitted over encrypted channels (HTTPS) and processed under Google Cloud's security standards.

3. Data Security Measures

We take security seriously and rely on industry-standard practices implemented by our third-party partners:

- **Encryption**: All data transmissions between our app and third-party services are encrypted using SSL/TLS.

- **Access Control**: Only authorized systems and personnel can access third-party data.

- **Data Retention**: Data is retained only for the duration necessary for service functionality and legal compliance.

4. User Rights and Control

You have the right to:

- **Review Data**: Request details on what third-party data is processed.

- **Opt-Out**: Disable third-party integrations where applicable.

- **Delete Data**: Request removal of your data from third-party services (subject to their policies).

5. Contact Us

For any inquiries regarding third-party data usage, contact us at **hi@aivine.ai**.