Privacy Policy and Data Collection Statement

Deep Soul Privacy Policy

Last Updated: October 12, 2026 | Version: v1.6

Deep Soul Heritage Management Limited (the "Company", "we", "us", or "our") values your privacy. This Policy applies to the Deep Soul App (the "App"), related websites, and related services provided by us. It explains how we collect, use, disclose, transfer across borders, retain, and protect your personal data, and how you may exercise your related rights.

This Policy should be read together with our Terms of Service and any Personal Information Collection Statement provided at a specific data collection interface. Where a particular feature is subject to a more specific data processing notice, that notice supplements this Policy in relation to that feature.

1. Data We Collect

We only collect personal data that is reasonably necessary in connection with the functions, activities, and services of the Company. Depending on the features you use, we may collect the following data:

1.1 Registration and Account Data

• Required data: name, phone number, date of birth, title, and nickname. Your name, title, and nickname are primarily used to identify and address you within the App; your phone number is used to create and log in to your account (a one-time password (OTP) may be used when creating an account); your date of birth is used to support relevant App functions.

• If you do not provide data necessary to create or log in to an account, we may be unable to create your account, verify your login, or provide features that require an account.

• Optional data: profile picture/photo and other data you choose to provide through individual features.

1.2 Device, Login, and Technical Data

• IP address, IP country/region code, device model, device name, browser or User Agent, operating system, language, login and last access times, session identifiers, user identifiers, and records relating to security, debugging, and system operation.

1.3 Content and Sensitive Data You Voluntarily Provide

Depending on the features you choose to use, you may voluntarily provide text, photos, videos, voice recordings, audio transcripts, emotional or mood records, life stories, messages, social interactions, location, participants, food/restaurant information, study or work interests, academic information, advance planning information, family office information, trust information, property information, bank account numbers, safe deposit box information, beneficiary information, confidential events, and other content you choose to record.

Bank account numbers and safe deposit box information are encrypted in accordance with the Company's security arrangements. The App does not ask you to provide bank passwords. We currently do not require users to provide copies of identity cards or passports as part of general account registration.

1.4 Third-Party Data

When you provide the name, phone number, or other data of a successor, beneficiary, participant, contact person, or other third party, you should ensure that you have reasonable authority or another appropriate basis to provide that data to us, and avoid providing data beyond what is necessary for the relevant feature.

2. How We Use Data

We may use personal data for the following purposes:

• To create, manage, verify, and secure your account;

• To provide, maintain, personalize, and improve the App, Website, and related features;

• To store, display, organize, and process content you actively create;

• To provide AI-assisted journaling, content creation, emotional companionship, analysis, general reminders, and related features;

• To provide user interactions, comments, replies, sharing, and push notifications;

• To provide customer service, troubleshooting, information security, and detection of fraud or unauthorized access;

• To conduct service usage statistics, performance analysis, error diagnosis, and product improvement;

• To support invitation, successor, referral, OneLink/deep link, and similar linking features;

• To process account inheritance, read-only access, and related permission verification according to settings made during the user's lifetime and platform procedures;

• To comply with applicable laws, court orders, law enforcement or regulatory requirements, and to create necessary audit records.

3. Authentication Services (Authgear)

We use Authgear as our authentication and account security service provider to support account creation, phone login, one-time passwords, multi-factor authentication, session management, security detection, and related audit functions.

Authgear's service region is currently located in the United States. Accordingly, data relating to authentication may be transferred outside Hong Kong for processing. Such data may include your name, phone number, date of birth, title/gender, nickname, profile picture link, IP address, device/User Agent, user and session identifiers, and login times.

Authgear's processing of data is also governed by its applicable privacy policy and the relevant arrangements between the Company and the service provider.

4. Artificial Intelligence (AI) Data Processing

4.1 Positioning of AI Features

Souli and related AI features are designed as tools for journaling, self-reflection, and emotional companionship. They are not medical, psychotherapy, clinical diagnosis, or crisis intervention services. Please also refer to the Terms of Service for provisions relating to the nature of the services and limitations of AI outputs.

4.2 Data Transmitted to Alibaba Cloud

To provide AI content generation, Souli emotional companionship, content analysis and insights, and related features, we may transmit data necessary for the relevant feature to Alibaba Cloud for processing. The AI processing region is currently Singapore. Depending on the feature you use, such data may include:

• Content you provide: such as post titles, text content, voice recordings, images, and videos;

• Media-related data: such as voice transcripts, image or video descriptions, and file links required to process the relevant media;

• Content and contextual data: such as post type, dates, weather, participants, location, restaurant or food information, school or learning-related information, mood scores, activity level, and other information related to the relevant content;

• Personalization and feature-setting data: such as age, nickname, App language, and writing style.

In some AI processing flows, before transmitting text content, we use automated masking to the extent practicable for specified categories of data, such as phone numbers, email addresses, identity document numbers, passwords, bank account numbers, and credit card numbers. However, these masking measures do not cover all data that may identify an individual, such as names or addresses. Users should therefore avoid entering unnecessary personal or sensitive data when using AI features unless it is necessary.

We only transmit data applicable to the needs of the relevant AI feature; not all of the data listed above is transmitted each time an AI feature is used.

4.3 Alibaba Cloud Data Protection

According to the Alibaba Cloud Model Studio privacy notice publicly available as of the date this Policy was updated, Alibaba Cloud states that it does not use customer-transmitted data for model training and that transmitted data is protected using AES-256 encryption. We also use reasonable contractual, technical, and administrative arrangements to require third-party service providers to process data in accordance with applicable requirements. For Alibaba Cloud's data processing terms, please refer to its Data Processing Addendum (DPA): https://www.alibabacloud.com/help/zh/legal/latest/fe2cxg.

4.4 AI Safety Processing

AI responses are generally not individually reviewed by humans, but are subject to content safety checks. If content does not pass a safety check, the system may stop displaying the original AI response and display a safety message instead. Where the system identifies content that may require crisis support, it may display a lifebuoy or similar prompt directing users to information about professional support hotlines in Hong Kong.

5. Third-Party Service Providers and Data Recipients

To provide and support the services, we may disclose or transmit personal data reasonably necessary for the relevant services to the following categories of service providers:

• Authentication and account security services: processing account creation, login, verification, security, and related records;

• Artificial intelligence services: processing text, voice, images, videos, and related contextual data required to provide AI features;

• Payment services: processing identity, payment, and transaction data required for payments and transactions;

• Push notification services: processing device push identifiers and content required to send notifications, including replies from other users;

• Analytics, attribution, and technical services: these services may process device data, IP addresses, advertising identifiers, App usage events, and other technical identifiers for service analytics, troubleshooting, install/campaign attribution, invitations, referral, deep link, and similar features.

We only provide service providers with data reasonably necessary for the relevant service purpose and use appropriate contractual, technical, and administrative measures to protect personal data. We do not sell your private records or other user content to third parties for advertising placement. The App currently does not display Google advertisements.

6. Promotional Messages and Direct Marketing

We may use App push notifications to provide users with information about new products, offers, paid plans, or other promotions. Where such activities constitute direct marketing under Hong Kong's Personal Data (Privacy) Ordinance, we will provide the required notice in accordance with applicable law and obtain the required consent or indication of no objection before using the relevant personal data for direct marketing.

You may at any time request that we stop using your personal data for direct marketing through the App's notification/promotional settings (where available), your device notification settings, or by contacting us. We will not charge you for such a request. Non-promotional notifications necessary for service, security, or account operation may not constitute direct marketing.

7. Cross-Border Transfers and Data Storage Locations

Our primary servers and backups are currently located in Hong Kong, China. Certain third-party services process data outside Hong Kong, including Authgear's United States region and Alibaba Cloud AI's Singapore region.

When using service providers outside Hong Kong, we take reasonable and practicable contractual, technical, and administrative measures, having regard to the nature of the data, purpose of processing, and risks, to protect personal data transferred.

8. Data Retention

We retain personal data only for as long as reasonably necessary to fulfil the purposes of collection or use, provide services, protect system security, handle disputes, and comply with legal or regulatory requirements. When data is no longer needed, we will delete or anonymize it in accordance with applicable procedures.

• Account termination/deletion: we will delete data associated with the membership account, but authentication records retained for security and audit purposes may be kept for up to 90 days.

• Authentication records: these may include IP address, country/region code, User Agent, user/session identifiers, login times, and name, phone number, date of birth, title/gender, nickname, and profile picture link associated with the authentication account.

• Backend debug server logs: generally retained for 30 days for troubleshooting, security, and system operation.

• Backups: backups are currently located in Hong Kong, China. A fixed public rotation/deletion period for backup data following account deletion has not currently been established. We limit retention according to backup cycles, security, and operational needs, and avoid restoring deleted-account backup data for ordinary business use.

Where a longer retention period is required for legal, regulatory, dispute-handling, or information-security purposes, we may retain necessary data for a reasonable period required for the relevant purpose.

9. Data Security and Internal Access

We take reasonable security measures proportionate to the nature and risk of the data, including encryption in transit or at rest, access controls, authentication, backups, logging, and other technical or administrative measures. Bank account and safe deposit box information is encrypted in accordance with the Company's security arrangements.

General staff are not permitted to view users' private content. Only authorized technical or security personnel may access relevant data on a least-privilege basis where necessary for troubleshooting, information-security incidents, legal requirements, or user support. Such access is logged in accordance with applicable arrangements.

No internet, cloud, or electronic storage service can guarantee absolute security. We continually review our security measures and, in the event of a data incident, take appropriate action having regard to the nature of the incident, risk, and applicable requirements.

10. Account Inheritance and Posthumous Data

If you use the account inheritance feature, you may designate authorized successors and related permissions during your lifetime. After the inheritance process is triggered and the required verification is completed, a successor may, according to your authorization, view designated content on a read-only basis, such as "Final Chapter", "Legacy in the World", obituary-related content, life experiences/life line, Secret Base, Life Plan, Discovery, and Acquired Beliefs.

Account inheritance is a read-only access arrangement and does not amount to taking over the account. The data actually viewable is subject to settings made during your lifetime, platform functionality, verification procedures, third-party privacy interests, and applicable law.

If relevant content contains personal data of other individuals, we may, where necessary, restrict, mask, or refuse disclosure of part of the content to protect third-party interests or comply with legal obligations. The legal status of account inheritance and other rules of use are set out separately in the Terms of Service and relevant inheritance rules.

11. Minors

The services are currently intended for persons aged 13 or above. Persons under 18 should use the services under the guidance of a parent or legal guardian and should avoid providing unnecessary sensitive personal data without appropriate assistance.

The App currently does not have a separate parent/legal guardian consent verification process. If we become aware of an account or data processing situation that does not meet the minimum age requirement, we may take

reasonable measures to restrict the account, stop the relevant processing, or delete data that was inappropriately collected.

12. Your Data Rights

Subject to Hong Kong's Personal Data (Privacy) Ordinance and other applicable laws, you may request access to personal data we hold about you and request correction of inaccurate personal data. We may require reasonable information from you to verify your identity and process the request.

You may also delete your account through features provided in the App or request deletion of specific data. Deletion is not an absolute right in all circumstances; we may retain certain data for a limited period for legal, information-security, dispute-handling, backup-cycle, or other lawful and necessary purposes.

If you wish to stop receiving direct marketing, you may make a request using the methods described in Section 6.

13. External Websites and Third-Party Content

Certain features of the App may provide links to third-party websites or platforms. Third-party websites are not operated or controlled by the Company. Personal data you provide directly on such websites is governed by the relevant third party's privacy policy and terms. We recommend that you review the relevant privacy policy and security arrangements before providing data.

14. Changes to This Policy

We may update this Policy due to changes in our services, technology, third-party service providers, laws, or data processing practices. Updated versions will be published through the App, Website, or other appropriate channels. Where changes materially affect data use or user rights, we will provide additional notice where appropriate. If applicable law requires separate consent, we will take the required steps before the relevant processing.

15. Contact Us

If you have questions about this Policy or how we process personal data, or wish to request access, correction, deletion, or cessation of direct marketing, you may contact us by email:

Email: itsupport@deepsoulai.com

This Policy is intended to explain Deep Soul's personal data processing arrangements. If there is any inconsistency between this Policy and mandatory requirements of applicable law, the applicable legal requirements will prevail.

This document is available in Traditional Chinese, Simplified Chinese and English. In the event of any ambiguity, inconsistency or conflict among these versions, the Traditional Chinese version shall prevail.