JUMPUP Inc.
Privacy Policy

Enacted: 1/3/ 2026

JUMPUP Inc. (hereinafter referred to as "the Company") is engaged in AI-powered system development and promotional consulting services (including video production, sales tool creation, training and educational material development, and distribution services). The Company recognizes that the appropriate protection of personal information of its customers, business partners, and related parties is an important social responsibility, and commits to complying with the Act on the Protection of Personal Information of Japan (hereinafter referred to as "APPI"), related laws and regulations, guidelines issued by the Personal Information Protection Commission, and standards such as JIS Q 15001.

The Company is committed to the appropriate handling and protection of personal information in accordance with the following policy.

Article 1 (Company Information)

- Company Name: JUMPUP Inc.
- Address: Miyamasuzaka Building 609, 2-19-15 Shibuya, Shibuya-ku, Tokyo, Japan
- Representative Director: Tei Kawasaki
- Personal Information Protection Officer: Tei Kawasaki, Representative Director

Article 2 (Definitions)

In this Policy, the following terms shall have the meanings set forth below.

1. "Personal Information" means information relating to a living individual that can identify the specific individual by name, date of birth, or other descriptions contained in such information (including information that can be easily cross-referenced with other information to identify the specific individual), or that contains an individual identification code.
2. "Special Care-Required Personal Information" means personal information that includes descriptions prescribed by the APPI as requiring special care in handling so as not to cause unjust discrimination, prejudice, or other disadvantage to the individual, such as race, creed, social status, medical history, criminal record, or the fact of having suffered damage by a crime.

3. "Personal Data" means personal information constituting a personal information database, etc.
4. "Retained Personal Data" means personal data over which the Company has the authority to disclose, correct, add to, delete, cease utilization of, erase, and cease provision to third parties.
5. "Anonymously Processed Information" means information relating to an individual obtained by processing personal information so that the specific individual cannot be identified, and such that the original personal information cannot be restored, through measures prescribed by the APPI.
6. "Pseudonymously Processed Information" means information relating to an individual obtained by processing personal information so that the specific individual cannot be identified without cross-referencing with other information, through measures prescribed by the APPI.

Article 3 (Collection of Personal Information)

The Company collects personal information through lawful and fair means to the extent necessary for its business activities. Special Care-Required Personal Information shall be collected only with the prior consent of the individual, except where permitted by law.

The primary methods of collection include the following:

- Web forms (inquiries, document requests, applications, etc.)
- Email, telephone, and in-person communications
- Exchange of business cards
- Execution of outsourcing agreements and service contracts
- Applications for surveys, events, and seminars
- Data generated through the use of AI services provided by the Company (such as ONE Conne)
- Various platforms (social media, business matching services, etc.)

Article 4 (Purpose of Use of Personal Information)

The Company uses personal information collected within the scope of the following purposes and shall not use such information beyond these purposes without the consent of the individual. When changing the purpose of use, the Company shall do so only to the extent reasonably related to the original purpose and shall notify or publicly announce the revised purpose.

(1) Purposes Related to AI System Development

- Communications and meetings related to the development, operation, and maintenance of AI systems (such as ONE Conne)
- Implementation proposals, technical support, and consulting
- Provision of training and role-playing functions through AI avatars
- Statistical analysis of usage data for service quality improvement (conducted after processing data into a non-personally identifiable format)
- Contract, billing, and payment management

(2) Purposes Related to Promotional Consulting

- Execution of video production, sales tool creation, training material development, and distribution services
- Project planning, progress management, delivery, and after-sales support
- Planning and execution of marketing initiatives

(3) General Purposes

- Responding to inquiries and requests
- Notifications and communications regarding important service matters
- Announcements of new services, campaigns, etc. (only with the consent of the individual)
- Recruitment and human resources management
- Compliance with laws and regulations, and protection of the Company's rights and interests

Article 5 (Data Handling in AI Services)

With respect to AI-related services provided by the Company, including the AI avatar service "ONE Conne," data shall be handled in accordance with the following principles.

1. The Company's AI systems do not access the client's internal information and operate as independent, isolated systems. A logically isolated dedicated environment is provisioned for each client to ensure strict data segregation.
2. Conversational text data generated during training sessions with AI avatars is stored in an encrypted state and managed under strict controls within a logically isolated database.

3. Audio and video data is used temporarily for analytical processing and promptly deleted thereafter. Retention in a secure environment is available only upon explicit request from the client.
4. The Company does not use client dialogue data for the purpose of AI training or model improvement.
5. External data transfers are not performed as a general rule. Where unavoidable for the performance of services, appropriate security measures shall be implemented.
6. Profiling within AI services (such as behavioral pattern analysis of users) is conducted only upon request from the client. The purpose and methodology shall be communicated in advance prior to implementation.
7. Upon termination of the contract, all data held by the Company relating to the client (including conversational text and analytical results) shall be physically deleted immediately.

Article 6 (Provision of Personal Information to Third Parties)

The Company shall not provide personal information to third parties without the consent of the individual, except in the following cases:

1. Where required by law.
2. Where necessary for the protection of the life, body, or property of an individual and it is difficult to obtain the consent of the individual.
3. Where particularly necessary for improving public health or promoting the sound development of children and it is difficult to obtain the consent of the individual.
4. Where it is necessary to cooperate with a national government organ, a local government body, or a person entrusted thereby in performing duties prescribed by law, and obtaining the consent of the individual is likely to impede the performance of such duties.

The following cases shall not constitute "provision to a third party":

- Where the handling of personal data is entrusted, in whole or in part, within the scope necessary for the achievement of the purpose of use.
- Where personal data is provided as a result of the succession of business due to merger or other reasons.
- Where personal data is jointly used (limited to cases where the scope, purpose, and responsible manager of the joint use have been publicly announced in advance).

[Regarding Joint Use] The Company may jointly use personal data with KAKUSHIN Corporation, a group company, for the purpose of providing and improving the ONE Conne service. In such cases, the categories of personal data jointly used, the scope of joint users, the purpose of use, and the responsible manager shall be separately announced.

Article 7 (Provision to Third Parties in Foreign Countries)

When providing personal data to a third party located in a foreign country, the Company shall take one of the following measures in accordance with the APPI:

1. Obtaining the prior consent of the individual for the provision to a third party in a foreign country (consent shall be obtained after providing information including the name of the destination country, the state of the personal information protection system in that country, and the protective measures taken by the recipient).
2. Providing personal data to a third party located in a country recognized by the Personal Information Protection Commission as having a personal information protection system equivalent to that of Japan.
3. Confirming that the recipient has continuously implemented a system equivalent to the measures that a personal information handling business operator is required to take under the APPI.

Article 8 (Security Measures for Personal Information)

The Company shall implement the following measures for the security management of personal data, including the prevention of leakage, loss, damage, and unauthorized access.

(1) Organizational Security Measures

- Appointment of a Personal Information Protection Officer and clarification of the responsibility structure
- Development, operation, and regular review of internal rules for the handling of personal data
- Record-keeping and regular inspections and internal audits of the handling of personal data
- Establishment of a system for responding to incidents such as data breaches

(2) Human Security Measures

- Regular education and training of employees on personal information protection
- Thorough communication of confidentiality obligations regarding the handling of personal data
- Development of employment regulations relating to the handling of personal data

(3) Physical Security Measures

- Access control for areas where personal data is handled
- Secure storage and appropriate disposal of media (paper and electronic) containing personal data
- Anti-theft measures for equipment and electronic media

(4) Technical Security Measures

- Access controls and access privilege management for personal data (principle of least privilege)
- Measures to prevent unauthorized access to information systems (firewalls, WAF, IDS/IPS, etc.)
- Encryption of personal data (at rest: AES-256 or equivalent; in transit: TLS 1.2 or higher)
- Deployment of security software, maintenance of up-to-date status, and vulnerability management
- Collection, retention, and regular analysis of access logs

Article 9 (Supervision of Subcontractors)

The Company may entrust the handling of personal data, in whole or in part, to external parties within the scope necessary for the achievement of the purpose of use. In such cases, the Company shall implement the following measures to ensure that the security management of personal data by the subcontractor is appropriately maintained.

1. Conducting a thorough evaluation of the subcontractor's personal information management system and security measures prior to engagement.
2. Executing outsourcing agreements that include confidentiality provisions, restrictions on sub-outsourcing, and audit rights.
3. Regularly verifying the subcontractor's handling of personal data and requesting corrective action as necessary.

Article 10 (Retention Period and Disposal of Personal Information)

The Company shall retain personal data only for the period necessary to achieve the purpose of use. When the purpose of use has been achieved or the retention period has expired, the Company shall promptly erase or dispose of the personal data. However, where retention is required by law, the data shall continue to be retained for the period prescribed by such law.

Disposal shall be carried out by irrecoverable means, including shredding of paper documents and complete erasure of electronic data (logical erasure or physical destruction).

Article 11 (Cookies and Access Logs)

The Company's website may use cookies and similar technologies for the purpose of improving user experience, analyzing access patterns, and measuring advertising effectiveness.

1. Information collected through cookies includes data that cannot identify specific individuals on its own (such as access dates and times, pages viewed, browser type, and IP addresses). However, where such information is linked with other personal information, it shall be treated as personal information.
2. Users may refuse the acceptance of cookies through browser settings; however, certain services may not function properly as a result.
3. Where third-party analytics services such as Google Analytics are used, the privacy policies of those service providers shall apply separately. Please refer to the respective service providers' websites for details.

Article 12 (Response to Personal Data Breaches)

In the event of a leakage, loss, damage, or other security incident involving personal data (hereinafter referred to as a "Breach"), or where there is a risk thereof, the Company shall promptly take the following actions:

(1) Investigation of the facts and identification of the cause.

(2) Implementation of emergency measures to prevent the spread of damage.

(3) Prompt notification to individuals who may be affected.

(4) Reporting to the Personal Information Protection Commission (where required by law).

(5) Development and implementation of measures to prevent recurrence, and review of internal systems.

Article 13 (Rights of Individuals Regarding Retained Personal Data)

Individuals have the following rights with respect to the Company's retained personal data under the APPI. Upon receiving a request from an individual or their authorized representative, the Company shall respond within a reasonable period following identity verification and prescribed procedures.

(1) The right to request notification of the purpose of use.

(2) The right to request disclosure (including provision by electronic record).

(3) The right to request correction, addition, or deletion of content.

(4) The right to request cessation of use or erasure.

(5) The right to request cessation of provision to third parties.

(6) The right to request disclosure of third-party provision records.

The Company may be unable to comply with all or part of a request in the following cases. In such cases, the Company shall notify the individual of the decision and the reasons therefor without delay.

- Where the identity of the individual (or the legitimacy of the authorized representative) cannot be verified.
- Where compliance would violate applicable laws or regulations.
- Where there is a risk of harm to the life, body, property, or other rights and interests of the individual or a third party.
- Where compliance would significantly impede the proper conduct of the Company's business.

Article 14 (Handling of Anonymously Processed and Pseudonymously Processed Information)

When creating anonymously processed information, the Company shall carry out appropriate processing in accordance with the standards prescribed by the APPI to ensure that the specific individual cannot be identified and the original personal information cannot be restored. The categories of information contained in the anonymously processed information shall be publicly announced, and security measures shall be implemented.

When creating pseudonymously processed information, the Company shall appropriately process such information in accordance with applicable laws and handle it only within the scope of the purpose of use. The Company shall not contact the individual or provide pseudonymously processed information to third parties.

Article 15 (Handling of Personal Information of Minors)

When collecting personal information from minors under the age of 16, the Company shall, as a general rule, obtain the consent of a legal representative (parent or guardian) prior to collection. If it is discovered that personal information of a minor has been collected without the consent of a legal representative, the Company shall promptly delete such information.

Article 16 (Continuous Improvement)

The Company shall respond to changes in laws and regulations, guidelines issued by the Personal Information Protection Commission, and other applicable standards concerning the handling of personal information, and shall continuously review and improve its internal systems, regulations, and operational methods for the protection of personal information.

Article 17 (Amendments to This Policy)

The Company may amend this Policy from time to time due to revisions in laws and regulations, changes in business operations, changes in social circumstances, or other reasons. The amended Policy shall take effect upon publication on the Company's website.

In the event of material changes, the Company shall provide notice through announcements on its website, email notification, or other appropriate means. A revision history of this Policy shall be maintained and published on the Company's website.

Article 18 (Contact Information)

For inquiries, complaints, consultations regarding the handling of personal information, and requests concerning retained personal data, please contact the following:

JUMPUP Inc. — Personal Information Inquiry Desk

Address: Miyamasuzaka Building 609, 2-19-15 Shibuya, Shibuya-ku, Tokyo, Japan

Inquiry Form: https://www.jumpup.city/one-contact

Business Hours: 10:00 AM – 6:00 PM (JST), excluding Saturdays, Sundays, and public holidays

* Inquiries received outside business hours will be responded to on the following business day.

End of Policy

JUMPUP Inc.
Tei Kawasaki, Representative Director