Privacy Policy

RevComm Inc. (the "Company") and the Company's subsidiaries and affiliates (the "Group Companies" and collectively with the Company, the "Group") handle and carefully monitor the services and systems provided by the Group, including, without limitation, the Site, MiiTel products and Sales Hacker (the "Services") and manage the Personal Information (as defined below) of the users who use the Services ("Users") or that is registered by Users with the Services and other Personal Information as follows.

This Privacy Policy applies to the Company and the Group Companies; provided, however, that, if any Group Company stipulates separate provisions on the handling of Personal Information other than this Privacy Policy, such separate provisions shall prevail.

1. Definition of Personal Information

Personal Information is information that can identify a specific individual by name, address, phone number, email address, employment information, or other such information, including that stipulated in Article 2, Paragraph 1 of the Act on the Protection of Personal Information in Japan (the "Personal Information Protection Act") and individual identification codes as defined by Article 2, Paragraph 2 of the Personal Information Protection Act. Personal Information also includes information that cannot by itself identify a specific individual but can be easily collated with other information and thereby identify a specific individual.

2. Acquisition/Utilization of Personal Information

When acquiring Personal Information, the Group will publish or notify Users of the purpose of use (including publication in this Privacy Policy). When acquiring Personal Information directly in the contract or other documents (including electromagnetic records) from Users, clients/suppliers, and the like (including officers and employees of corporations) (collectively, "Users Et Al."), the Group will clearly specify the purpose of use in advance and shall acquire such Personal Information by lawful and fair means. The Group properly uses Personal Information within the scope necessary to achieve its purposes of use.

3. Purposes of Use of Personal Information

The purposes of use of Personal information are as outlined below. The Group will not use Personal Information for any purpose other than these purposes of use without obtaining the consent of the relevant individual, except where permitted by the Personal Information Protection Act or other laws and regulations.

(1) Information Acquired from Users of the Services

1. Member authentication, management, communication of clerical work, and providing functions of the Services;
2. Verification of User identities;
3. Operating and managing seminars and various events, etc. provided by the Group;
4. Distributing information in relation to the Services;
5. Requests, communication regarding questionnaires and campaigns, etc., or granting of prizes, etc.;
6. Replying to inquiries and comments;
7. Advertising, solicitation, and sale of merchandise, etc. of the Group and third parties;
8. Announcements regarding the Services and seminars operated by the Group;
9. Conducting maintenance work on the Services;
10. Improvement of the Services;
11. Safely providing the Services to Users (including discovery of and notifications to Users breaching the Terms of Use, etc. and investigation, detection, and prevention of misconduct, including fraud, unauthorized access, misuse of services, etc., and responding thereto); and
12. Entrustment of the handling of Personal Information to a subcontractor, partner company, or contractor with whom the Group has concluded a confidentiality agreement concerning Personal Information within the scope necessary to achieve the purposes of use.

(2) Information Registered by Users of the Services

1. Replying to inquiries and comments of Users regarding the Services;
2. Conducting maintenance on the Services;
3. Improvement of the Services;
4. Safely providing the Services to Users (including discovery of and notifications to Users breaching the Terms of Use, etc. and investigation, detection, and prevention of misconduct, including fraud, unauthorized access, misuse of services, etc., and responding thereto); and
5. Entrustment of the handling of Personal Information to a subcontractor, partner company, or contractor with whom the Group has concluded a confidentiality agreement concerning Personal Information within the scope necessary to achieve the purposes of use.

(3) Personal Information of the Group's Clients/Suppliers (Including Officers and Employees of Client/Supplier Corporations)

1. Business-related responses, including negotiation, communication, consultation, ordering and settlement of transactions, or performance of an agreement;
2. Management of client/supplier information; and
3. Any other cases in which the Group must handle the Personal Information of clients/suppliers for appropriate and smooth provision of the Services.

(4) Information of the Group's Shareholders (Including Officers and Employees of Corporate Shareholders)

1. Exercising rights and performing obligations under the Companies Act of Japan and other applicable laws and regulations;
2. Shareholder management, including preparation of records pursuant to prescribed standards under various laws and regulations; and
3. Any other cases in which the Group must handle the Personal Information of shareholders for appropriate and smooth provision of the Services.

(5) Information of Applicants for Employment/Recruiting by the Group

1. Provision of employment/recruitment information, employment selection, and confirmation of application history by the Group;
2. Communication with applicants and responding to inquiries, etc. of applicants;
3. Announcements of events/seminars relating to employment operated by the Group; and
4. Any other cases in which the Group must handle the Personal Information of applicants for appropriate and smooth provision of the Services.

(6) Information of the Group's Officers, Employees, Retirees, and their Families (collectively, "Employees")

1. Business communication/information exchange with the Group's employees;
2. Employment management (payment of compensation, human resources/labor management matters, and provision of benefits, etc.) of the Group's employees;
3. Ensuring the health of and appropriate work environment for the Group's employees;
4. Providing benefits services and handling various insurance procedures, etc.;
5. Notifying and reporting to authorities, etc.; and
6. Any other cases in which the Group must handle the Personal Information of Employees for labor management purposes and for appropriate and smooth provision of the Services.

4. Handling of Private Communication Information

The Group may occasionally browse, confirm, analyze, use, or disclose information pertaining to private communications using the Services ("Confidential Communication Information") to third parties in accordance with the following rules.

(1) Nature of Information Acquired

Data generated while using the Services, including spoken statements, automatic transcriptions of such statements, video images, etc., of the Services.

(2) Primary Acquirer and User

The Group shall acquire and use Confidential Communication Information primarily; provided, however, that the Group may provide its contractors with Confidential Communication Information to the extent necessary for achieving the purposes of use outlined below.

(3) Purposes and Manner of Use

The purposes and manner of use of Confidential Communication Information are as follows:

1. Cases in which the use of Confidential Communication Information is necessary to protect the life, health, or property, etc. of a User or another person;
2. Cases in which disclosure is requested under laws and regulations or any other cases in which disclosure is permitted under laws and regulations;
3. Cases in which a User breaches the Terms of Service or in which it is necessary to confirm whether a User has breached the Terms of Service;
4. Cases in which it confirms whether the communication technology environment that is used by Users conform to the applicable utilization conditions;
5. Cases in which there is a need to operate the Services or to conduct an investigation or analysis, etc. for improvement of the Services (including, but not limited to, automatic transcription of call content, conversation analysis by AI and operational efficiency evaluation); and
6. Cases in which use is within the scope of the Master T&Cs, Individual T&Cs, Explanatory Materials, or a confidentiality agreement, an agreement on the protection of Personal Information, or any other agreements separately executed between the Group and a User in relation to the Services.

(4) Term of Use

The term of use shall be the period necessary to achieve the foregoing purposes of use.

(5) Point of Contact

The point of contact is set forth at the end of this Privacy Policy.

(6) Method for Revoking Consent etc.

In order to revoke your consent to the use of Confidential Communication Information, please contact the point of contact set forth at the end of this Privacy Policy. Please note that the Group sometimes cannot allow consent to be revoked if the use of Confidential Communication Information is indispensable for providing the Services. Please note that the Group may no longer be able to provide the Services to a User that has revoked consent.

5. Provision of Personal Information to Third Parties

In principle, the Group will not provide Personal Information to third parties unless the consent of Users Et Al. is obtained; provided, however, that the Group may provide Personal Information without the consent of Users Et Al. in the following cases:

(1) Cases in accordance with laws and regulations;
(2) Cases in which the provision of Personal Information is necessary to protect human life, health, or property and obtaining the relevant individual's consent is not possible;
(3) Cases in which there is a special need to enhance public health or promote the fostering of healthy children and obtaining the relevant individual's consent is not possible;
(4) Cases in which it is necessary to cooperate with a governmental organization, a local government, or a person entrusted thereby to handle matters prescribed by laws and regulations and obtaining the relevant individual's consent would interfere with the handling of such matters; and
(5) Cases in which the third party is an academic institution, etc. and the third party will handle the relevant Personal Information for academic study purposes (including cases in which a purpose of handling such Personal Information is an academic study but excluding cases in which such handling may unjustifiably infringe upon the rights and interests of an individual).

The following cases do not constitute third-party provision as described above:

(i) Cases in which all or part of the handling of Personal Information is entrusted within the scope necessary to achieve a purpose of use;
(ii) Cases in which Personal Information is provided pursuant to business succession following a merger or other reasons; and
(iii) Cases in which Personal Information is jointly used under the provisions of the Personal Information Protection Act.

6. Information Sharing within the Group

Due to the Group Companies' entrustment of part of their businesses to the Company, there may be cases in which a Group Company shares information acquired from Users with the Company within the scope necessary to operate and provide the Services and within the scope of the purpose of use.

7. Handling of Personal Information in Foreign Countries

In some cases, the Company will entrust the handling of Personal Information to a contractor located in a foreign country for its business operations. In addition to the provision of this paragraph, the Company may provide Personal Information to any third parties located in foreign countries in accordance with the provisions of the Personal Information Protection Act.

The outline of such handling procedures of Personal Information of the Company in foreign countries is as follows.

[Personal Information Handled by the Company (RevComm Inc.)]

Notwithstanding the following, the data stored automatically during the use of MiiTel by Users who entered into contracts with the Company regarding such use in Japan is maintained in a server in Japan.

(1) Countries in which Foreign Contractors are located
Please refer to "Handling of Personal Information in Countries Outside Japan"

(2) Details of the Personal Information Protection Legislation of the Countries Covered by (1)
Please refer to "Handling of Personal Information in Countries Outside Japan"

(3) Personal Information Protection Systems of Contractors
The Company has executed agreements with Contractors obliging them to take action for the protection of Personal Information. These actions include those corresponding to the OECD's Eight Principles.

8. Entrustment of Personal Information

The Group may occasionally entrust the handling of Personal Information to its contractors for business operations. In such event, the Group will stringently select contractors that have established a control system that properly protects Personal Information and ensure that they control Personal Information properly by executing an agreement that establishes a system to prevent the leakage of Personal Information of Users Et Al. through proper management and confidentiality of Personal Information.

9. Disclaimer of Provision to Third Parties

The Group will not take any responsibility for the acquisition of Personal Information by third parties in the following cases:

(1) Cases in which a User reveals Personal Information to a third party using the Services or otherwise;
(2) Cases in which a User is identified by a third party due to information posted by Users Et Al. in relation to the use of the Services;
(3) Cases in which Personal Information is provided by Users Et Al. via an external site linked from the Services, which then is utilized;
(4) Cases in which a third party has obtained information that can identify an individual User (ID and password, etc.) without provision by the Group; and
(5) Cases in which there are no reasons attributable to the Group.

10. Use of Statistically Processed Data

The Group will sometimes create statistical data that is processed so as to be unable to identify an individual based on the Personal Information provided. The Group may unrestrictedly use statistical data that cannot identify an individual.

11. Acquisition and Use of Browsing History and Characteristics Information

Browsing histories and characteristics information are history actions taken or attribute information that will not identify an individual of Users Et Al., such as services used, browsed pages, IP address, or cookie information, not including information that identifies an individual (Personal Information).

The Group uses browsing history and characteristics information for the purposes of protecting the privacy of Users Et Al., improving convenience, distributing advertising, and acquiring statistical data.

The Group uses cookies for such purposes. In addition, the Group sometimes acquires attribute information (limited to one that cannot identify an individual even by combining) that cannot identify an individual, such as age, sex, occupation, or residential area, provided upon member registration, etc., or user action history on the site (URLs accessed, content, and reference order, etc.) by using technology such as cookies or JavaScript; provided, however, that no Personal Information is gathered by cookies or attribute information and action history. You may choose not to allow cookies via your browser settings. If you choose not to allow cookies, some functions of the Services may be restricted.

[Acquisition of Information by Using Third-Party Services]

For details of the information which the Group acquires by using third-party services, please refer to the "Acquisition of Information by Using Third-Party Services" section.

12. Requests for Disclosure, Correction, or Suspension of Use, etc. of Personal Information

The Group properly responds to requests of Users Et Al. for disclosure (including disclosure of third-party provision records; the same shall apply hereinafter), notice of purposes of use, correction, addition to, deletion, suspension of use, erasure, and suspension of provision to a third party of Personal Information in the possession of the Group ("User Request") in accordance with the Personal Information Protection Act (or if laws regarding the handling of personal information outside of Japan is applicable, such laws and regulations).

There may be cases where the Group will not accept the following User Requests:

(1) Disclosure of Personal Information
   1 Cases in which disclosure is likely to harm the life, health, property, or other rights and interests of Data Subjects or a third party;
   2 Cases in which disclosure is likely to significantly interfere with the proper operation of the Services;
   3 Cases in which disclosure would violate other laws and regulations; or
   4 Any other cases which fall under a reason for exception of laws and regulations.

(2) Suspension of Use, Erasure, or Provision of Personal Information to Third Parties
   1 Cases in which great expense would be incurred thereby or in which taking such actions is difficult and substitute actions to protect the rights and interests of Users Et Al. have been taken; or
   2 Any other cases which fall under a reason for exception of laws and regulations.

(3) Correction of, Addition to, or Deletion of Personal Information
   1 Cases in which laws and regulations other than the Personal Information Protection Act specify special procedures; or
   2 Any other cases which fall under a reason for exception of laws and regulations.

Please refer to the point of contact below to submit a User Request.

[If the Personal Information Protection Act is applicable:]

Upon receiving a User Request under the Personal Information Protection Act, the Group will verify the identity of the User with specified materials (driver's license, Individual Number card, etc.).

In addition, upon receiving a User Request by a representative, the Group will verify the authority with the following materials.

• For legal representative:
Documents confirming that he/she has the legal authority to represent the individual in question (family register, a copy of a health insurance card in which dependents are indicated), documents verifying the identity of the legal representative (a copy of a document indicating the name and current address of the representative, such as a driver's license, passport, or health insurance card)

• For a privately appointed agent:
Power of attorney (Personal Information disclosure request form attachment), certificate of the principal's seal (issued within three (3) months of the User Request), documents verifying the identity of the privately appointed agent a copy of a document indicating the name and current address of the agent, such as a driver's license, passport, or health insurance card)

13. Restriction on the Acquisition of Special-Care-Required Personal Information

Except where permitted by laws and regulations or as provided directly by Users Et Al., the Group will not acquire the following Personal Information, which is specified as special-care-required personal information (Article 2, Paragraph 3 of the Personal Information Protection Act), without the prior consent of the relevant Users; provided, however, that this provision shall not apply where such information is provided by Users Et Al:

(1) Race;
(2) Creed;
(3) Social status;
(4) Medical history;
(5) Criminal record;
(6) The fact that the User has suffered damage from a crime; and/or
(7) Personal Information prescribed by the Order for the Enforcement of the Personal Information Protection Act as requiring special care in handling so as not to cause unfair discrimination, prejudice, or other disadvantages to the relevant individual.

14. Management of Personal Information (Security Control Actions)

The Group strives to implement security measures to prevent the leakage, loss, misuse, and alteration, etc. of Personal Information placed under its control and takes the necessary and appropriate security actions. The Group retains Personal Information in a safe environment inaccessible by general Users Et Al.

In order to ensure that security actions are properly taken, the Group has acquired an information security management system authentication and a privacy mark certificate in Japan and regularly reviews the management system.

An outline of the security actions taken by the Group is as follows:

(1) Formulation of the Basic Policy and Policies for the Handling of Personal Information

To ensure the proper handling of Personal Information, the Group has created a Personal Information Protection Policy and this Privacy Policy in order to comply with laws and regulations pertaining to the protection of Personal Information, contact point for inquires and complaint handling and the like.

In addition, the Group has created internal rules for the handling of Personal Information, including handling methods and responsible persons/persons in charge and their duties, etc., at each stage of acquisition, utilization, retention, provision, and deletion/disposal, etc.

(2) Organizational Security Controls

The Group has appointed a manager to handle Personal Information and identified the Group's employees engaged in the handling of Personal Information and the scope of Personal Information handled by such employees. The Group has also developed a reporting system in the event that a violation of the Personal Information Protection Act or a breach of the Group's internal rules is discovered.

The Group regularly conducts audits of its handling of Personal Information and periodically requests audits by other departments and outside auditors.

(3) Human Security Controls

The Group provides employees with regular training with respect to the handling of Personal Information. It also sets forth the confidentiality of Personal Information in the Rules of Employment, etc.

(4) Physical Security Controls

The Group monitors the entry and exit of employees, restricts equipment, etc. brought into areas where Personal Information is handled, and prevents unauthorized persons from browsing Personal Information. The Group takes actions to prevent the theft or loss, etc. of equipment holding Personal Information, electronic media, and documents, etc. and implements measures to avoid Personal Information from being easily found when carrying such equipment or electronic media, etc., including move within an office.

(5) Technical Security Controls

The Group limits access to Personal Information to specific employees and has introduced a mechanism to protect its information system from external unauthorized access or illicit software.

(6) Understanding of External Systems

The Group entrusts cloud service providers and the like with the management of information, including some Personal Information, which is stored and managed by such service providers in the countries indicated in "6. Handling of Personal Information in Foreign Countries." The Group puts security controls in place based on the information provided by the Personal Information Protection Commission in Japan after researching the Personal Information protection systems of each country.

Please see the point of contact indicated below for the details of the security controls put in place by the Group.

15. Optional Provision of Personal Information

The provision of Personal Information to the Group is at the relevant individual's discretion. However, please note that you may not be able to register as a member or User or use the Services or systems if you do not provide the necessary information,

16. Amendment to the Personal Information Protection Policy and the Privacy Policy

The Company may amend the Personal Information Protection Policy and Privacy Policy at its discretion to the extent that such amendment does not violate any laws or regulations.

17. Handling of Links Posted on the Group's Websites

This Privacy Policy does not apply to any third-party websites (websites which are not managed by the Group) linked from the Group's websites.

For details of the handling of Personal Information within such third-party websites, please refer to the privacy policies, etc. on such websites.

18. Point of Contact

The Group's point of contact for complaints, requests, and disclosures, etc. relating to Personal Information is as follows.

[RevComm, Inc./Personal Information Complaints and Consultation Counter]

To: RevComm, Inc.
Personal Information Protection Supervisor
Compliance Manager

Address: HULIC Shibuya 1-chome Building 7F, 1-3-9 Shibuya, Shibuya-ku Tokyo, 150-0002 Japan
Email address:privacy@revcomm.co.jp

[Name of authorized personal information protection organization and point of contact for complaint resolution]

Name of authorized personal information protection organization: Japan Information Processing and Development Center
Point of contact for complaint resolution: Personal Information Protection Complaints and Consultation Office

Address: Roppongi First Building, 1-9-9 Roppongi, Minato-ku, Tokyo, 106-0032 Japan
TEL:+81-(0)3-5860-7565 / 0120-700-779 (Only available from Japan)

Enacted: October 1, 2018
Revised: October 3, 2019
Revised: January 5, 2022
Revised: April 1, 2022
Revised: February 1, 2023
Revised: February 1, 2024
Revised: April 1, 2024

[Exhibit 1]

Handling of Personal Information in Countries Outside Japan

In some cases, the Company will entrust the handling of Personal Information to a contractor located in another country (collectively, "Foreign Contractors") for business operational reasons. The outline of such entrustment is set forth below.

If the handling of Personal Information is entrusted to any country outside Japan other than those listed below, the Company will list such entrustment on this page as necessary.

Among the data stored automatically during the use of MiiTel, the data of Users who have entered into contracts in Japan regarding the use of such service is maintained in a server in Japan.

(1) Countries in which Foreign Contractors (Information Recipients) are Located

United States of America
Australia
Singapore
Germany
Ireland
United Kingdom
Sweden
India
Republic of Korea
Canada
Brazil
Indonesia
Switzerland
Israel
Mexico
Philippines
United Arab Emirates
South Africa
Costa Rica

(2) Details of the Personal Information Protection Legislation of the Countries Listed in (1)

1 United Kingdom and EEA member countries

These countries are prescribed by the rules of the Personal Information Protection Commission as establishing a personal information protection system recognized as having equivalent standards to those in Japan in regard to the protection of individual rights and interests.

For more details, please refer to the "Foreign Countries, Etc. Establishing a Personal Information Protection System Recognized to Have Equivalent Standards to That in Japan in Regard to the Protection of an Individual's Rights and Interests (Public Notice of the Personal Information Protection Commission No. 1 of 2019)" page (in Japanese).

2 Countries or Regions for which the European Commission's Adequacy Decision Has Been Rendered

・Canada

For more details, please refer to the "Investigation on Personal Information Protection Systems in Canada (Personal Information Protection Commission)" page (in Japanese).

・Republic of Korea

For more details, please refer to the "Investigation on Personal Information Protection Systems in the Republic of Korea (Personal Information Protection Commission)" page (in Japanese).

・Switzerland

For more details, please refer to the "Investigation on Personal Information Protection Systems in Switzerland (Personal Information Protection Commission)" page (in Japanese).

・Israel
For more details, please refer to the "Investigation on Personal Information Protection Systems in Israel (Personal Information Protection Commission)" page (in Japanese).

3 APEC Cross-Border Privacy Rules Participating Countries

・United States of America
For more details, please refer to the "Investigation on Personal Information Protection Systems in the United States of America (Personal Information Protection Commission)" page (in Japanese).

・Australia
For more details, please refer to the "Investigation on Personal Information Protection Systems in Australia (Personal Information Protection Commission)" page (in Japanese).

・Canada
For more details, please refer to the "Investigation on Personal Information Protection Systems in Canada (Personal Information Protection Commission)" page (in Japanese).

・Singapore
For more details, please refer to the "Investigation on Personal Information Protection Systems in Singapore (Personal Information Protection Commission)" page (in Japanese).

・Republic of Korea
For more details, please refer to the "Investigation on Personal Information Protection Systems in the Republic of Korea (Personal Information Protection Commission)" page (in Japanese).

・Mexico
For more details, please refer to the "Investigation on Personal Information Protection Systems in Mexico (Personal Information Protection Commission)" page (in Japanese).

・Philippines
For more details, please refer to the "Investigation on Personal Information Protection Systems in Philippines (Personal Information Protection Commission)" page (in Japanese).

4 Other Countries

・India
For more details, please refer to the "Investigation on Personal Information Protection Systems in India (Personal Information Protection Commission)" page (in Japanese).

・Brazil
For more details, please refer to the "Investigation on Personal Information Protection Systems in Brazil (Personal Information Protection Commission)" page (in Japanese).

・Indonesia
For more details, please refer to the "Investigation on Personal Information Protection Systems in Indonesia (Personal Information Protection Commission)" page (in Japanese).

・United Arab Emirates
For more details, please refer to the "Investigation on Personal Information Protection Systems in the United Arab Emirates (Personal Information Protection Commission)" page (in Japanese).

・South Africa
For more details, please refer to the "Investigation on Personal Information Protection Systems in South Africa (Personal Information Protection Commission)" page (in Japanese).

・Costa Rica
For more details, please refer to the "Investigation on Personal Information Protection Systems in Costa Rica (Personal Information Protection Commission)" page (in Japanese).

(3) Personal Information Protection Systems to be Provided by Information Recipients

The Company has executed agreements with information recipients obliging them to take action for the protection of Personal Information. These actions include those corresponding to the OECD's Eight Principles.

In addition to the above, the Company may provide personal information to third parties in other countries in accordance with the provisions of the Act on the Protection of Personal Information.

Last updated: April 1, 2024

[Exhibit 2]

Acquisition of Information by Using Third-Party Services

Please refer to the table below for details on the acquisition of information through third-party services that are used by the Group.

If any acquisition of information is to occur through third-party services other than those listed below, the Company will list such acquisition on this page as necessary.

The Group uses the Services stated in “Names of Information Collection Modules” section provided by the entities stated in the “Names of Parties to Which Information is to Be Transmitted” section.
Through such services, the Group may acquire “Contents of Information to Be Transmitted” for the purposes stated in the “Purpose of Use at the Company” section.

In addition, such information will be managed by the entities stated in the “Names of Parties to Which Information is to Be Transmitted” section during the “Information Retention Period” and will be used for the purposes stated in the “Purpose of Use by Parties to Which Information is to Be Transmitted” section. Please refer to the “Availability to Opt-Out” section for the availability/unavailability of disabling the settings of the Services stated in the “Names of Information Collection Modules” section.

Upon providing the Services, the Group uses cookies, codes or programs, etc. that transmit information stored on each User's terminal device to external servers (collectively, "Information Collection Modules"). The details of the Information Collection Modules used by the Group are as follows:

Name of Information Collection Modules	Content of Information to Be Transmitted	Names of Parties to Which Information is to Be Transmitted	Purpose of Use of Information to Be Transmitted		Availability to Opt-Out	Information Retention Period (if known)
			Purpose of Use at the Company	Purpose of Use by Parties to Which Information is to Be Transmitted		
◎ Information Collection Modules Used on the Company's Website						
Google Analytics	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Google LLC	• To collect data on User behavior • To improve User experience	For more details, please see here: https://policies.google.com/privacy	Available	Up to 26 months
Google Search Console	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Google LLC	• To collect data on User behavior • To improve User experience	For more details, please see here: https://policies.google.com/privacy	Available	Up to 16 months
Google Tag Manager	• Ad identifier • Information on terminal device and app • Information on network • Access history	Google LLC	• To collect data on User behavior • To improve User experience	For more details, please see here: https://policies.google.com/privacy	Available	-
Yahoo Tag Manager	• Ad identifiers • Information on terminal device and app • Information on network • Access history	LY Corporation	• To collect data on User behavior • To improve User experience	For more details, please see here: https://line.me/ja/terms/policy/	Available	Up to 25 months
Microsoft Advertising	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Microsoft Ireland Operations Limited (Microsoft Ad)	• To collect data on User behavior • To improve User experience	For more details, please see here: https://privacy.microsoft.com/ja-jp/privacystatement	Available	-

Microsoft Advertising Universal Event Tracking	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Microsoft Ireland Operations Limited (Microsoft Ad)	• To collect data on User behavior • To improve User experience	For more details, please see here: https://www.facebook.com/privacy/center	Available	-
Facebook Pixel	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Meta Platforms, Inc. (Facebook)	• To collect data on User behavior • To improve User experience	For more details, please see here: https://www.taboola.com/policies/privacy-policy	Available	-
Taboola	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Taboola, Inc.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://www.ptengine.jp/privacy-policy/	Available	Up to 13 months
Ptengine	• Information on terminal device and app • Information on network	Ptmind	• To collect data on User behavior • To improve User experience	For more details, please see here: https://policies.google.com/privacy	Available	The retention period for measured data varies depending on the contract plan, as follows: Free Plan: 1 month Growth Plan: 6 months Premium Plan: Customizable
Microsoft Clarity	• Ad identifiers • Information on terminal device and app • Information on network • Access history	Microsoft	• To collect data on User behavior • To improve User experience	For more details, please see here: https://policies.google.com/privacy	Available	-

OPTEMO						
optemo_visitor_id	Visitor's unique ID	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
optemo_visitor_token	Key required to pass through API (to prevent operation by anyone other than the visitor)	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
optemo_call_on_～	Call flags (i.e., flag to determine whether a call is in progress); controlling multiple tabs	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
isChatting_～	Chat flags (i.e., flag to determine whether the chat icon is open or closed); controlling multiple tabs	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
optemo_session_id_～	Session ID for website visitor	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
optemo_form_notification_id_～	Relevant automatic transmission form ID	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
optemo_manual_form_id_～	Relevant manual transmission form ID	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://privacy.microsoft.com/ja-jp/privacystatement	Unavailable	90 days
Notification ConditionsId_～	Relevant notification conditions ID	J-Tama’s Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days

is_valid_thanks_page_〜	Flag for thank you calls	J-Tama's Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
isDomainShared_〜	Flag to manage whether subdomain is shared	J-Tama's Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
primaryDomain_〜	Primary domain being set when subdomain is shared	J-Tama's Co. Ltd.	• To collect data on User behavior • To improve User experience	For more details, please see here: https://j-tamas.com/privacy-policy/	Unavailable	90 days
d-cast.tokyo	• IP address • User agent • Tracking ID	GEOCODE, Co., Ltd.	• Results measurement	For more details, please see here: https://www.geo-code.co.jp/privacy/	Unavailable	Up to 12 months

Names of Information Collection Modules	Content of Information to Be Transmitted	Names of Parties to Which Information is to Be Transmitted	Purpose of Use of Information to Be Transmitted		Availability to Opt-Out	Information Retention Period (if known)
			Purpose of Use at the Company	Purpose of Use by Parties to Which Information is to Be Transmitted		
◎ Information Collection Modules Commonly Used Among “MiiTel,” “MiiTel Meetings” and “MiiTel RecPod”						
Fullstar	Information contained in the script (personal information may be included) URL of the site browsed • Date and time of browsing the title (to be used for calculating the time spent on the site, etc.) Information on response to reviews and questionnaires response information; identifiers recorded on the device, such as cookies (those created through Fullstar / those created through BowNow) Progress data regarding guide information browsed (unique UID data / CS selector of registration information) Progress data regarding tooltip information browsed (unique UID data)	Cloud CIRCUS, Inc.	• To collect and analyze data on User behavior	For more details, please see here: https://cloudcircus.jp/privacy/	Unavailable	Unlimited period of time

Azure OpenAI Service	MiiTel, MiiTel Meetings and MiiTel Speech recognition results generated by RecPod (transcription), speakers' names, and analysis scores	Microsoft Corporation	• To generate minutes and advice	For more details, please see here: https://privacy.microsoft.com/ja-jp/privacystatement/	Available	30 days
Announcekit	Login ID, company ID, cookie information	AnnounceKit LLC	• For reference for product development •For the provision of information corresponding to client quality and type	For more details, please see here: https://announcekit.app/privacy-policy	Available	-

Names of Information Collection Modules	Content of Information to Be Transmitted	Names of Parties to Which Information is to Be Transmitted	Purpose of Use of Information to Be Transmitted		Availability to Opt-Out	Information Retention Period (if known)
			Purpose of Use at the Company	Purpose of Use by Parties to Which Information is to Be Transmitted		
◎ Information Collection Modules Used in “MiiTel Meetings”						
Recall.ai	1) When using calendar integration of Microsoft Outlook: (i) Authentication information to acquire calendar information from Microsoft Outlook (ii) Calendar information (iii) Recorded data 2) When using calendar integration of Google Calendar: (i) Authentication information to acquire calendar information from Google Calendar: (ii) Calendar information (iii) Recorded data 3) Recorded data in the case of connecting through URL integration	Hyperdoc Inc.	• To acquire and analyze recorded data and meeting information	For more details, please see here: https://www.recall.ai/privacy/	Available	Recorded data: Other than one-week recorded data: Unlimited period of time

Last updated: April 1, 2024