

Announcement No. 003/2023**Privacy Policy for Customers**

(Revised Version)

Privacy Policy

Ichitan Group Public Company Limited (“Company”) recognizes the importance of personal data protection. Since the protection of personal data is part of corporate social responsibility and forms the foundation for building trustworthy business relationships with customers, the Company adheres to the Personal Data Protection Law and other related legal regulations.

This Privacy Policy has been established to provide an appropriate method for managing personal data and to implement suitable security measures for protecting the personal data of customers. This is to ensure compliance with the Personal Data Protection Act, as well as other relevant laws and regulations.

Executives and employees must process and secure personal data as confidential information and must prevent its loss, misuse, or unauthorized access. Only executives and employees authorized to access personal data within the necessary scope for lawful business purposes and within the scope of their roles and responsibilities are permitted to access such data. Executives and employees are strictly prohibited from using or accessing personal data beyond the scope of their work at the Company. They are also forbidden from disclosing data to unauthorized persons, both inside and outside the Company, or from processing personal data in ways that do not comply with this policy.

1. Definition

Company	means Ichitan Group Public Company Limited
Service Users/Customers	means individuals or legal entities who own personal data and use the services of Ichitan Group Public Company Limited.
Authorized Approvers	means individuals assigned by the Company to have authority to approve within the scope of authority granted by the Company.
System Administrators	means departments or individuals assigned by system owners or personal data owners to oversee specific systems.
System Owners	means business unit, executives or managers responsible for a particular system.
Executives and Employees	means executives, directors, officers, employees, temporary workers and any individuals employed or contracted to work under agreements with Ichitan Group Public Company Limited.
Data Subject	means individuals identifiable through their personal data, whether directly or indirectly. This does not refer to ownership in the property rights or the creators of such data.
Minor	means natural persons under 20 years of age, except for those who are legally married under the law, rendering them of legal age.
Incompetent Person	means individuals who are disabled, mentally unstable, habitually extravagant, addicted to alcohol or drugs, or otherwise incapable of self-management. These individuals are placed under guardianship by court order.
Curator	means the person responsible for taking care of the “quasi-incompetent person” by the public prosecutor who has made a request to the court and the court has ruled to be the “curator” to take care of the “quasi-incompetent person”.
Guardian	means a person who is responsible for taking care of “incompetent persons”, including managing their property and performing other duties on their behalf.
Personal Data	means information about individuals that allows them to be identified, either directly or indirectly. This does not include data about deceased persons specifically (as per Section 6 of the Personal Data Protection Act, B.E. 2562). Examples include names, surnames, email addresses, photographs, fingerprints and ID numbers, which can directly identify a person. Data like location or cookies that indirectly identify a person is also included. Furthermore, basic data that cannot independently identify a person but, when combined with other information, can identify an individual is also considered personal data.
Sensitive Data	means personal data related to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health information, disabilities, trade union membership, genetic data and biometric data.

Biometric Data	means personal data derived from using techniques or technologies related to an individual's unique physical or behavioral traits, enabling identification. Examples include facial recognition data, iris scan data or fingerprint scan data.
Public Data	means personal data disclosed to the public by the data owner, such as social media profiles. When using social media credentials like Facebook, Twitter or Line to connect to or access any of the Company's services, such as social media account IDs, interests, likes, and friends lists, the data owner can control the privacy settings through the account settings provided by the social media service providers.
Data Controller	means person authorized to decide on the collection, use or disclosure of personal data.
Data Processor	means person who stores collects, uses or discloses personal data according to the instructions or on behalf of the data controller.
Data Processing	means any action performed on personal data or a set of personal data, whether by automated means or otherwise, such as collecting, recording, organizing, structuring, storing, altering, retrieving, using, disclosing through transmission, dissemination or otherwise making available, aligning or combining, restricting, erasing or destroying.
Application	means programs or sets of instructions that control the operation of mobile computers and peripheral devices to perform specific tasks. Applications (Apps) must include a user interface (UI) to facilitate user interaction
IP Address	means numerical identifier assigned to each device, such as computers or printers, participating in a computer network using the Internet Protocol for communication.
Cookie	means small data files sent by the Company's website to computers or electronic devices connected to the internet to store personal data. Cookies are sent back to the original website each time the website is revisited.
Office	means Office of the Personal Data Protection Committee.

2. Roles and Responsibilities

2.1 Board of Directors have the duty to oversee the implementation of personal data protection to comply with laws and governmental regulations and appoint or adjust the Personal Data Management Working Group to support the operations of the Board.

2.2 PDPA Steering Committee has been assigned by the Board of Directors to proceed as follows:

- Supervise the operations of the Personal Data Management Working Group.
- Define guidelines for drafting and reviewing policies and frameworks for personal data management.
- Provide recommendations and screen objectives, policies, plans, practices, processes, and documents related to personal data management.
- Monitor and evaluate the performance of personal data management.
- Appoint or adjust the Personal Data Management Working Group to support the Board's operations as appropriate.
- Invite relevant units to provide clarifications or insights beneficial to operations.
- Oversee compliance with the policy and have the authority to approve changes, amendments or reviews of this policy.

2.3 The senior management shall have the duty to manage and control operations concerning the collection, use and disclosure of personal data to comply with laws and regulations including to ensure the implementation of effective data security measures.

2.4 Employees shall strictly comply to this policy, operational regulations, company directives and all relevant laws and regulations.

3. General Provisions

General Requirements

3.1. Personal data protection under this policy applies to the personal data of individual customers.

3.2 The company shall appoint a Data Protection Officer (DPO) to review this policy at least once a year or whenever significant changes affect the implementation of this policy. Any changes will be announced on the Company's website.

3.3 The Company collects, uses, or discloses personal data only with the consent of the data subject, either prior to or at the time of data processing, unless the company anonymizes the data or has a legal basis to do so, such as:

- Necessity for the performance of a contract.
- Compliance with legal obligations.
- Necessity for legitimate interests, within reasonable expectations of the data subject.
- Necessity for public interest missions.
- Prevention or mitigation of harm to life.
- Preparation of historical or archival documentation for public interest purposes.

3.4 The Company collects personal data only as necessary for lawful purposes and informs the data subject of the details of the data collection as required by law.

3.5 The Company shall delete, destroy or anonymize personal data after the retention period has expired or exceeds the necessity for the purpose of collecting the personal data or as requested by the owner of the personal data or as the owner of the personal data withdraws consent, unless there is a legitimate reason under law or government regulations that requires the Company to continue to retain such personal data.

3.6 The Company takes care of personal data safely, including taking into account the privacy of the owner of personal data and maintaining the confidentiality of personal data.

4. Requesting consent from the data subject

4.1 Requesting consent to collect, use or disclose personal data from the data subject must be done clearly, in writing or via electronic system, except where such consent cannot be requested by such method. Requesting consent by other methods must have reliable evidence that the data subject has expressed their intention to give consent.

4.2 The data subject must be informed of the purpose of collecting, using or disclosing personal data in a clear and understandable manner, without deceiving or misleading the owner of personal data regarding the purpose, and with utmost consideration of the owner of personal data in giving consent.

4.3 In the case where the data subject is a minor who has not reached the age of majority by marriage or does not have the status of a person who has reached the age of majority, requesting consent from the person exercising parental authority who has the authority to act on behalf of the minor.

4.4 In the case where the data subject is incompetent, consent shall be requested from the guardian who has the authority to act on behalf of the incompetent.

4.5 In the case where the owner of personal data is quasi-incompetent, consent shall be requested from the curator who has the authority to act on behalf of the quasi-incompetent.

4.6 In case where the data subject or the person with authority according to no. 4.3, 4.4 and 4.5 wishes to withdraw the consent previously given, it must be processed as requested by the data subject as effortlessly and smoothly as giving consent. If the withdrawal of consent affects the data subject in any way, the data subject must be informed of the impact of such withdrawal of consent.

4.7 The Company shall collect, use or disclose personal data only for the purposes notified to the data subject. The collection, use or disclosure of personal data that varies from the purposes notified shall not be processed, unless the new purpose has been notified to the data subject with the consent prior to collection, use or disclosure.

5. Purpose of Collecting Personal Data

5.1 The collection of personal data must have a purpose for utilizing such data in the Company's operations in various aspects, under the provisions of laws or governmental regulations.

5.2 When collecting personal data, the data subject must be informed before or at the time of collection regarding the following details:

- The purpose of collecting personal data for its use or disclosure.
- The necessity for the data subject to provide personal data to comply with laws or to enter into a contract, and the potential consequences of not providing the personal data.

- The personal data to be collected and the duration of its retention.
- The types of persons or entities to whom personal data may be disclosed, including the names of such persons or entities (as applicable).
- The rights of the data subject under the law.
- Information regarding the Company and the Data Protection Officer, including contact details and methods of contact.

5.3 The personal data collected must be accurate and complete based on the information provided by the data subject. If the data changes, it must be updated to ensure accuracy.

5.4 For the collection of sensitive personal data, explicit consent must be obtained from the data subject unless there is a legal basis for such collection, and approval must be sought from the authorized approver.

5.5 For the collection of personal data from sources other than the data subject directly, the data subject must be informed within 30 days from the date of data collection and consent must be obtained unless there is a legal basis for such collection, with approval sought from the authorized approver.

5.6 The collection of personal data must include recording details of the purpose of collecting each type of personal data, information regarding the data controller, the retention period of the data, the rights and methods of accessing personal data, and conditions regarding individuals entitled to access the personal data, as well as other details as required by law, to allow the data subject or relevant authorities to verify the data.

6. Access to and Use of Personal Data

6.1 Employees of the Company may access or use personal data only as necessary for their work and in accordance with the rights granted by the Company. If employees need to access personal data beyond the rights granted by the Company, they must seek approval from the authorized person.

6.2 Employees of the Company must use personal data only for the purposes for which the data was collected or as consented to by the data subject, unless there is a legal basis for its use.

6.3 System administrators and system owners must authorize access to personal data only to employees of the Company who have the rights as determined or who have received approval from the authorized person.

7. Methods of Collection

The company collects personal data through the following processes:

7.1 Personal data obtained directly from the data subject

Before engaging in various activities with the Company or any other operations, the Company will inform the data subject of the reasons and necessity for collecting, using or disclosing personal data beforehand (or at the time of collection) in all cases. The Company will also inform the data subject if their personal data may be disclosed to third parties as mentioned above. If the data subject is informed and consents to the collection, use or disclosure of their personal data, they may express their consent in writing, via computer systems, or other electronic devices provided by the Company. The Company ensures that the consent process allows the data subject to give consent freely, is easily accessible, and clearly explains the purpose of consent in accordance with legal standards.

7.2 Personal data obtained from affiliated companies

7.3 Personal data obtained from third parties, such as agents, stores or companies providing data collection services, business partners, or affiliates.

7.4 Personal data obtained from website visits, such as the name of the internet service provider and the IP address (IP Address) used to access the internet, the date and time of the website visit, the pages viewed during the website visit, and the address of websites directly linked to the Company's website.

7.5 Personal data obtained from public records and non-public records that the Company is legally entitled to collect.

7.6 Personal data obtained from government agencies or regulatory authorities exercising their legal authority.

8. Disclosure and Receipt of Personal Data

8.1 The disclosure of personal data to individuals or organizations outside the company must receive consent from the data subject and approval from the Personal Data Protection Steering Committee (PDPA Steering Committee), except when it is in compliance with laws or regulations.

The Company will disclose personal data to external individuals and/or organizations or agencies only under the following circumstances:

8.1.1 Authorized intermediaries, such as transportation companies, companies providing data storage and collection services, companies for system development and maintenance for various activities of the Company.

8.1.2 Business partners, business affiliates, subsidiaries and/or external service providers to offer benefits and other services of the company to the data subjects, including the development and improvement of the Company's products or services, such as data analysis, data processing, IT services and infrastructure preparation, customer service platform development, sending emails/SMS, website development, mobile application development, satisfaction surveys and research. In such cases, a confidentiality agreement will be in place and the entities must maintain personal data protection standards recognized as acceptable.

8.1.3 Government agencies, the government or other organizations as required by law for compliance with laws, orders or requests and to coordinate with relevant agencies regarding legal compliance.

8.2 The receipt of personal data from individuals or organizations outside the Company must ensure that the personal data has a lawful basis and must be approved by the PDPA Steering Committee, except when it is in compliance with laws or regulations.

The Company will collect data directly provided by the data subject or through its services or operations via all channels, including the following:

8.2.1 Data obtained when the data subject registers or fills out an application to participate in various activities of the Company or other services of the Company, such as name, surname, national ID card number or other identification cards, phone number, date of birth, address, email, etc.

8.2.2 Data from membership registration, participation in activities or account creation containing personal data provided to the Company for access to services via the Company's platforms, such as mobile applications or websites, including online accounts or application

accounts for company services and personal data provided for applications such as activity participation or contacting the Company via the website or other channels as determined by the Company.

8.2.3 Data from subscribing to newsletters, surveys or participating in activities such as satisfaction, interests or consumer behavior.

8.2.4 Data regarding transactions with the Company or its affiliates, such as job applications, agent applications or bid submissions, including credit or debit card information, bank account numbers or other payment information, as well as payment dates and times, depending on the type of transaction.

8.2.5 Data from visits or usage of the Company's websites, affiliate websites or applications operated by the Company, including social media usage and interactions with online advertisements, software version and type used for accessing the websites, type of device used for accessing services such as personal computers, laptops or smartphones, operating system and platform type, IP address of the device, location data and data regarding services and products viewed or searched by the data subject.

8.2.6 Data from the records of communications between the data subject and the Company, stored in formats such as service recipient logs, satisfaction assessments, research and statistics, voice recordings or CCTV footage when the data subject contacts the Company, such as customer service centers. It also includes data provided via research media such as SMS, social media, applications or email.

8.2.7 Social media profile data when using social media credentials such as Facebook, Twitter and Line to connect or access the Company's services, including social media account IDs, interests, likes and friends list. Data subjects can control this privacy setting through their social media account settings provided by the respective social media platforms.

8.2.8 Inquiries via mail, fax, email or phone from customers, including post-sale verification. Telephone inquiries will be recorded for accuracy. Such personal data may be used to maintain good customer relations, such as verifying investigations and responding to inquiries. It may also be anonymized for sales and educational purposes, such as contacting medical personnel, notifications and reporting to government agencies.

8.3 If the Company engages external individuals or organizations to collect, use or disclose personal data on behalf of the Company (data processors), it must use data processors with appropriate and equivalent personal data security measures in line with the Company's security policies for managing external IT service providers. There must be agreements in place to control the operations of the personal data processors in compliance with the law by specifying the purpose or instructions for collecting, using or disclosing personal data clearly. Measures must be established to prevent the personal data processors from collecting, using or disclosing the data obtained from the Company beyond the purpose or instructions specified by the company.

9. Sending or Transferring Personal Data to Overseas

If the company transfers, transmits and/or send information overseas, the Company will establish standards for signing agreements and/or joint venture agreements with organizations that receive personal information. Personal information protection standards are acceptable and comply with relevant laws to ensure that personal information is securely protected, such as:

9.1 In the event that the Company needs to store and/or transfer personal data for storage purposes

9.2 Cloud processing, the Company will consider organizations with international security standards and will store personal data in an encrypted format or other methods that cannot identify the owner of the personal data, etc.

The list of external parties to whom the Company will disclose personal data may increase or decrease. The Company shall always keep the data up-to-date.

10. Security and Confidentiality of Personal Data

In order for the owner of personal data to be confident in the management of the Company to prevent risks that may cause personal data to be unlawfully accessed, leaked, altered or lost, the Company complies with the information security policy, including compliance with internationally accepted standards for information security and business continuity management and in accordance with the law.

The Company has measures to protect the privacy of the data subject by limiting the right to access personal data of the data subject. It will be specified for only individuals who need to use such personal data to present the Company's products and services, such as the Company's employees who are individuals that the Company allows to access such personal data. They must strictly adhere to and comply with the Company's measures to protect personal data, including maintaining the confidentiality of such personal data. The Company has both physical and electronic protection measures in accordance with the applicable regulatory standards to protect personal data.

When the Company enters into a contract or agreement with a third party, the Company will set appropriate measures to protect personal data and maintain confidentiality to ensure that the personal data in the Company's possession will be secure.

11. Rights of Data Subjects

Data subject shall have the following rights:

- The right to request to know the existence, nature of personal data, the purpose of the Company's use of personal data.
- The right to access and request a copy of their personal data, which the Company will have appropriate procedures for the data subject to confirm their identity with the Company first.
- The right to request to correct or change personal data to be correct, up-to-date, complete and not misleading.
- The right to object to the collection, use or disclosure of their personal data, including the right to object to the processing of personal data.
- The right to request to temporarily suspend the use or disclosure of personal data.
- The right to request to delete or destroy personal data or make personal data unidentifiable of the data subject.
- The right to request to disclose the acquisition of their personal data in the case that the user has not given consent to the collection or storage.
- The right to withdraw the consent previously given to the Company to collect, use or disclose personal data. However, the withdrawal of consent shall not affect the collection, use or disclosure of personal data of the data subject who has already given consent in the past.

The Company has specified contact channels to exercise the rights as specified in no. 17. The Company shall proceed and consider the request within 30 days from the date of receipt of the request. However, the Company may refuse to exercise the rights of the data subject as required by law or under the contract made with the Company in cases that will cause the data subject to lose various rights and benefits.

Furthermore, deleting, destroying or processing the personal data in a form that cannot identify the data subject or revoking the consent of the data subject can only be done under the provisions of the law and the contract made with the Company. The exercise of such rights may affect the performance of the contract made with the Company or the provision of other services because the identity of the data subject cannot be identified. Therefore, there may be limitations on some services that require the use of personal data and may deprive the data subject to receive benefits, services and news from the Company.

12. Retention Period and Location of Storage of Personal Data

The Company will retain personal data only as necessary, taking into account the purposes and the necessity for which the Company needs to collect, store and process such data, including compliance with applicable legal requirements. The Company will store personal data after the period in which the data subject has ceased interactions with the Company for a certain period, in accordance with the duration and statutes of limitations under relevant laws. The Company will store personal data in appropriate storage locations depending on the type of personal data. However, the Company may need to retain personal data beyond the statutory limitation period, such as in cases where legal proceedings are ongoing.

The Company will retain all types of personal data collected from data subjects for the duration required by applicable laws, such as accounting and tax laws, which may stipulate different retention periods. Additionally, the Company may retain personal data of data subjects for a longer period if required by law. Once the legally required retention period has expired, the Company will delete, destroy or anonymize the personal data in a cautious and secure manner, prioritizing the interests of the data subjects to the greatest extent possible.

Nevertheless, the Company may delete, destroy or anonymize personal data before the legally required retention period expires if contacted by the data subject requesting the deletion or destroying of their personal data.

The deletion, destroying or anonymization of personal data is subject to a written request from the data subject, following a verification process to confirm the identity of the data subject, similar to the process required when the data subject consents to the collection, use and disclosure of personal data. This is to ensure that the deletion, destroying or anonymization is performed accurately and without error in identifying the data subject.

Additionally, the Company may specify a retention period for certain types of personal data before deletion, destroying or anonymization, such as 1 (one) year from the date of data collection or the last date of interaction with the Company. For instance, this could apply to data of job applicants who were not selected for employment contracts with the Company, visitors to the Company's website through various channels or shareholders who are no longer shareholders of the Company. If the Company anonymizes such personal data, even though it no longer constitutes identifiable personal data, the Company may still retain it for statistical analysis purposes, such as

for staff development, enhancing credit services, launching new products or improving the Company's information technology systems.

If the Company deletes, destroys or anonymizes personal data as requested by the data subject, it may result in limitations that prevent the Company from providing certain services to the data subject in the future. (This does not include services already provided before the deletion, destroying or anonymization of the personal data). Additionally, if such actions incur costs, the Company reserves the right to charge fees necessary and relevant to the requested actions as specified by the data subject.

13. Use of Personal Data for Marketing Purposes

In addition to the aforementioned purposes and under the provisions of the law, the Company shall use personal data for marketing purposes, such as sending promotional materials via postal mail, email or other methods, including conducting direct marketing activities. This is to enhance the benefits that the data subjects receive as customers of the Company by recommending relevant products and services.

The data subject may opt-out of receiving marketing communications from the Company, except for communications related to the data subject and/or services provided by the Company such as receipts.

14. Cookies

The Company uses cookies to collect data on the usage of personal data subjects for purposes such as data collection, statistical compilation, research, trend analysis and improving and managing the operation of the website and/or application. The data collected through cookies does not identify the personal data subject.

15. External Website Links

The Company's website may contain links to third-party websites, which may have personal data protection policies different from those of the Company. Data subjects are encouraged to review the personal data policies of those websites to understand the details of their data protection practices and to decide whether to disclose personal data. The Company shall not be responsible for the content, policies, damages or actions arising from third-party websites.

16. Data Protection Officer

The Company has appointed a Data Protection Officer to oversee the operations related to the collection, use or disclosure of personal data to ensure compliance with the Personal Data Protection Act B.E. 2562 (2019) and the policies, regulations, announcements and orders of the Company. The Data Protection Officer also coordinates and cooperates with the Office of the Personal Data Protection Commission.

17. Questions Regarding the Privacy Policy

If you have any questions or concerns about this Privacy Policy Statement or the management and handling of your data, you may contact us at:

Address: Ichitan Group Public Company Limited
No. 8 T-One Building, 42nd – 44th Floor, Soi Sukhumvit 40,
Phra Khanong Sub-District, Khlong Toei District, Bangkok 10110

Channel:
Email: DPO@ichitangroup.com

18. Contact Channels

If there are any queries regarding the Company's Privacy Policy, the data collected by the Company or if you wish to exercise any of your rights under the Personal Data Protection Act as outlined in no. 11, you may contact us at:

Address: Ichitan Group Public Company Limited
No. 8 T-One Building, 42nd – 44th Floor, Sukhumvit 40 Alley,
Phra Khanong Sub-District, Khlong Toei District, Bangkok 10110

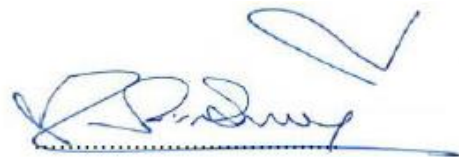
Channel:
Email: DPO@ichitangroup.com

19. Appropriate Authority

If you wish to report a complaint or feel that the Company has not addressed your concerns satisfactorily, you may contact and/or file a complaint with the Office of the Personal Data Protection Commission using the details below:

Office of the Personal Data Protection Commission
Office of the Permanent Secretary, Ministry of Digital Economy and Society
Email: saraban@pdpc.or.th
Tel: 02-142-1033, 02-141-6993

This announcement is made for general acknowledgment and to proceed accordingly.
January 16, 2023



(Tan Passakornnatee)
Chief Executive Officer