



Personal Data Protection Policy

Effective from 14 November 2025

Table of Contents

Scope	4
Definitions	4
Sources of Personal Data	5
Purposes of Processing Personal Data	6
Processing of Personal Data.....	7
Transfer of Personal Data to Foreign Countries	9
Retention Period of Personal Data.....	9
Rights of Data Subjects	9
Security Measures for Personal Data	11
Management of Personal Data Breach Incidents	11
Links to Third-Party Websites	12
Amendments to the Personal Data Protection Policy	12
Compliance with the Personal Data Protection Policy and Contact Information	12
Governing Law	13

Personal Data Protection Policy

Precise Corporation Public Company Limited and its subsidiaries (the “Company”) attach great importance to and respect the right to privacy, including the security of personal data of data subjects. In order to ensure that data subjects are confident that their personal data is protected, the Company has therefore prepared this Personal Data Protection Policy (the “Policy”) as a guideline for the protection of personal data, so that personal data received from data subjects will be used only for the intended purposes and in compliance with law.

The Company places strong emphasis on the protection of personal data and recognizes that the processing of personal data within the Company must be carried out in accordance with the following principles:

- **Lawfulness, Fairness, and Transparency**

The Company will process personal data only where there is a lawful basis for doing so and will clearly define the methods for collecting and using personal data.

- **Purpose Limitation**

The Company will process personal data solely for the purposes specified and notified at the time of collection, except where the processing is for related purposes or for the performance of clearly defined legal obligations.

- **Data Minimization**

The Company will collect and use only such personal data as is necessary to achieve the purposes of the processing.

- **Accuracy**

The Company will take appropriate steps to ensure that personal data it holds is accurate, complete, and up to date, considering the purposes of the processing.

- **Storage Limitation**

The Company will retain personal data only for as long as is necessary for its use, unless the Company is required to retain it longer in accordance with document retention standards or governmental regulations.

- **Integrity and Confidentiality**

The Company will implement appropriate technical and organizational measures to ensure that personal data it holds is kept secure at an appropriate level.

- **Accountability**

The Company will take appropriate measures to demonstrate that it complies with all the above principles.

Scope

For personal data collected before the Personal Data Protection Act B.E. 2562 (2019) came into force, the Company may continue to collect and use such personal data for the original purposes. Any disclosure or other actions in relation to such personal data, apart from collection and use as mentioned above, shall be carried out in accordance with the Personal Data Protection Act B.E. 2562 (2019).

Definitions

Person

Means a natural person.

Personal Data

Means any information relating to a person which enables the identification of that person, whether directly or indirectly, such as:

*First name–last name, nickname, address, telephone number
National ID number, passport number, social security number, driver’s licence number, Taxpayer identification number, bank account number, credit card number, Email address, occupation, status, position or job title, family status, Employment information, job position, work experience and/or performance appraisals, Education information, vehicle registration, land title deed, house registration*

Signature, voice, voice recordings, pictures, photographs, video recordings, video clips, Information on purchase of products and/or services, IP Address, computer traffic data (log file), LINE ID, Facebook ID, Google ID, Twitter ID, and accounts on other social media platforms, etc.

However, the following information is **not** considered personal data, for example:

- Business contact information that does not identify an individual, such as:
company name, company address, company registration number, office telephone number, work email address, or group email address such as info@company.co.th
- Anonymous data, or pseudonymous data that has been technically processed so that it can no longer identify a person
- Information of deceased persons.

Sensitive

Personal Data

Means personal data of an inherently private nature which is sensitive and may be at risk of unfair discrimination, such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data that similarly affects the data subject as may be prescribed by the Personal Data Protection Committee.

Data Subject

Means the natural person who is the subject of the personal data; it does not mean a person who owns (has “ownership” of) the data, or who created or collected the data. A subject of data must be a natural person only and does not include a **juridical person** (e.g. companies, associations, foundations, or other organizations). Data subjects include the following:

1. Data Subjects Who Are of Legal Age

- Persons aged 20 years or older
- Persons who are married from the age of 17 years or older
- Persons who married before the age of 17 with court permission
- Minors whose legal representative has given consent for them to engage in commercial business, other business, or enter an employment contract, in connection with such business or employment, thereby granting the minor the same status as a person of full age.

In providing any consent, a data subject who is of legal age may give consent by themselves.

2. Data Subjects Who Are Minors

Means persons under 20 years of age who are not of legal age as defined above. For any consent, the consent of the person exercising parental power who has authority to act on behalf of the minor must also be obtained.

3. Data Subjects Who Are Quasi-Incompetent Persons

Means persons whom the court has declared quasi-incompetent due to physical disability, mental infirmity, habitual prodigality or debauchery, addiction to intoxicants, or other similar reasons, such that they are unable to manage their own affairs or may manage their property in a way that could harm themselves or their family. For any consent, the consent of the guardian who has authority to act on behalf of the quasi-incompetent person must first be obtained.

4. Data Subjects Who Are Incompetent Persons

Means persons whom the court has declared incompetent due to insanity. For any consent, the consent of the custodian (guardian) who has authority to act on behalf of the incompetent person must first be obtained.

If consent is obtained from a data subject in a manner that does not comply with the Personal Data Protection Act, such consent shall not be binding upon the data subject.

Data Controller Means a person or juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of personal data.

Data Processor Means a person or juristic person who collects, uses, or discloses personal data on behalf of, or under the instructions of, the Data Controller, and who is not themselves the Data Controller.

Sources of Personal Data

Generally, the Company does not collect personal data except in the following cases:

1. Personal Data Obtained Directly from the Data Subject

The Company collects personal data through the following service processes:

- Processes for using the Company's services or submitting requests to exercise rights with the Company, such as service registration, subscription to receive information or news, job applications, etc.
- Voluntary provision of information by data subjects, such as completing surveys or questionnaires, or communicating via email or other communication channels between the Company and the data subject.
- Data collected from the use of the Company's website through the data subject's browser cookies and from the use of electronic transaction services.

2. Personal Data Obtained from Third Parties

The Company may receive personal data on data subjects from third parties, where the Company believes that such third parties have the right to collect the data subject's personal data and disclose it to the Company.

Purposes of Processing Personal Data

1. The Company may collect, use, and disclose your personal data for the following purposes:
 - 1) To create, improve, manage, and deliver the Company's products, services, benefits, and privileges.
 - 2) To provide services to you, including but not limited to processing any of your transactions.
 - 3) To take steps at your request prior to entering a contract, or to perform a contract to which you are a party with the Company, such as the sale of products and/or services to you or performance of any agreement to which you are a party. This includes managing your account, delivering products, managing accounting and financial matters, after-sales services, product returns, and any actions necessary to ensure that you receive products and/or services as requested.
 - 4) To create databases and records of your service history with the Company through any service channels.
 - 5) To publicize and provide content and information from the Company that is sent to you, including promotional programmes related to such content as may be suitable for you.
 - 6) To analyse and process data for marketing, promotional activities, research, and sales, including publicizing products and services of the Company, its group companies, business partners, business alliances, or other persons through notifications displayed on mobile devices, SMS, or social media.
 - 7) To improve the quality of services, and to improve the Company's websites and applications to better meet user needs and operate more efficiently.
 - 8) To provide channels for receiving feedback and suggestions to improve the Company's programmes and content to better meet your needs.
 - 9) To comply with agreements and various terms and conditions made with you.
 - 10) To comply with laws and regulations of government agencies, such as the Personal Data Protection Act, the Electronic Transactions Act, the Civil and Commercial Code, the Civil Procedure Code, the Criminal Code, the Criminal Procedure Code, etc.

- 11) For marketing, sales promotion, and data analysis, including sending advertisements, public relations, coupons, news, and other information about promotions or special activities directly to you via the website and/or applications. You may opt out of certain types of advertising messages by following the instructions provided.
 - 12) To use for identity verification and qualification checks when you apply to use the Company's services.
2. The Company has no policy to collect sensitive personal data from you.

However, if it becomes necessary for the Company to collect such sensitive personal data, the Company will expressly request your consent before collecting such data, unless there is a legal basis that allows the Company to do so without obtaining consent.
 3. In cases where the Company is required to request identification documents—such as a national ID card, passport, employment record, or other documents that may contain sensitive personal data (e.g., religion, nationality, or blood type). The Company does not wish to collect such information. Therefore, you are requested to redact or obscure those sensitive details before submitting the documents. If you do not do so, the Company reserves the right to redact or obscure such information to protect your sensitive personal data.
 4. You agree not to provide any incorrect and/or misleading information to the Company and agree to notify the Company of any inaccuracies or changes to such information. The Company reserves the right to request any additional documents it deem appropriate to verify the information you have provided.
 5. If you provide the Company with personal data of third parties (such as property owners, beneficiaries, emergency contacts, referees), for example names, addresses, telephone numbers, income of family members, personal information and contact information for emergency purposes or for completing application forms or transactions with the Company, you represent that such information is lawfully obtained. Please inform those individuals of this Personal Data Protection Policy and/or obtain their consent as required.

Processing of Personal Data

1. Collection of Personal Data

The Company will collect personal data only to the extent necessary and appropriate in relation to the type of services used by the data subject or the personal data provided to the Company.

The Company will collect personal data directly from the data subject and recognizes the importance of obtaining the consent of the data subject, as it is the data subject's right to choose whether to consent to the processing requested by the Company. The Company must also inform the data subject where incomplete information or refusal to consent to the collection, use, or disclosure of personal data may limit access to certain services.

The Company may not be required to obtain consent where the processing is based on other lawful grounds (e.g. necessity for the performance of a contract or for compliance with the law).

To enable the Company to offer services that best meet the needs of data subjects, the Company may record communications between the data subject and the Company whether via telephone, email,

communication applications, customer service centers, or any other channel for purposes such as: evidential use, service development and improvement, monitoring satisfaction, staff training, staff performance evaluation, data analysis, and system development for the greatest benefit to data subjects.

2. Use of Personal Data

The Company will use personal data in accordance with the purposes for which the data subject has provided such personal data to the Company. The Company will ensure that the use of personal data is appropriate and will implement appropriate security measures and access controls to safeguard personal data.

3. Disclosure of Personal Data

The Company may disclose your personal data to other persons or entities, provided that the data subject has been informed prior to or at the time of the collection of such personal data, based on the data subject's consent, or as permitted by applicable laws.

The recipients of such personal data will collect, use, and/or disclose the personal data only to the extent relevant and in accordance with this Notice.

The Company may disclose personal data to the following persons or entities:

1) Service Providers

The Company may disclose personal data to service providers that provide services to the Company, including government authorities from which the Company obtains services, such as the service providers listed below. Such service providers may use personal data only to the extent permitted by the Company and in accordance with this Notice. Any disclosure of personal data will be made strictly on a need-to-know basis only.

- The Company's distributors or agents
- Transportation and logistics service providers, including delivery service providers
- Tour companies and tour networks, both domestic and international
- Marketing service providers, including providers of data preparation and statistical analysis
- Advertising, public relations, and communication service providers
- Service providers relating to the preparation, storage, management of documents, and printed materials

2) Business Partners

The Company may disclose personal data to persons or entities that have entered into partnership agreements with the Company, such as business partners, sales agents, and outsourced service providers engaged in the Company's business operations.

3) External Service Providers Acting Under the Company's Control

The Company may disclose personal data to external service providers that provide services and perform duties under the Company's control, including but not limited to:

- Assisting in transaction processing
- Delivering advertisements for the Company's products and services
- Aiding and services to you

Such service providers may include:

- Transactional and financial service providers (e.g., banks, payment service providers)
- Technology service providers (e.g., cloud systems, blockchain systems, SMS delivery services, data analytics services)
- Software developers and information system service providers

4) Other Persons as Required by Law

The Company may be required to disclose personal data to other persons or entities as prescribed by law, including where applicable laws, rules, regulations, orders of government authorities, regulatory agencies, or court orders require the Company to disclose personal data.

In addition, the Company may be required to disclose your personal data to a transferee (including any potential transferee). The rights and obligations of the transferee in relation to your personal data shall be in accordance with this Notice.

Transfer of Personal Data to Foreign Countries

1. The Company may send or transfer personal data to its affiliates or other persons or entities located in foreign countries where necessary for the performance of a contract to which you are a party, or for the performance of a contract between the Company and another person or juristic person for your benefit, or to take steps at your request prior to entering into a contract.
2. The Company may also transfer personal data where necessary to prevent or suppress danger to life, body, or health of you or other persons, to comply with applicable laws, or where necessary for the performance of a task carried out in the public interest.
3. The Company may store personal data on computers, servers, or cloud systems provided by third parties, and may use third-party software, applications, or platforms in the form of software-as-a-service (SaaS) or ready-made platforms for the processing of personal data.
4. The Company will not allow unauthorized persons to access personal data and will require such third parties to implement appropriate security measures to protect personal data.
5. In the event that your personal data is transferred to foreign countries, the Company shall comply with applicable personal data protection laws and implement appropriate measures to ensure that personal data is adequately protected and that data subjects are able to exercise their rights in accordance with the law.
6. The Company shall also require recipients of personal data to implement appropriate safeguards, to process personal data only to the extent necessary, and to take measures to prevent unauthorized or unlawful use or disclosure of personal data.

Retention Period of Personal Data

The Company shall retain personal data only as necessary for the purposes for which it was collected, but not exceeding ten (10) years from the date the data subject last permitted the Company to process such personal data. Where required by law, the Company may retain personal data for a longer period. Once it is no longer necessary, the Company shall delete or destroy such personal data.

Rights of Data Subjects

Data subjects may exercise the following rights in accordance with applicable laws:

1. Right to Withdraw Consent

Where a data subject has given consent for the Company to collect, use, and/or disclose personal data (whether such consent was given before or after the Personal Data Protection Law comes into effect), the data subject has the right to withdraw such consent at any time while the personal data is retained by the Company, unless such right is restricted by law or where a contract providing benefits to the data subject remains in effect.

Where the withdrawal of consent may affect the use of products or services, such as the loss of benefits, promotions, new offers, enhanced products or services tailored to the data subject's needs, or the receipt of useful information, the Company shall inform the data subject of such consequences prior to the withdrawal of consent.

2. Right to Data Portability

The data subject has the right to request access to his or her personal data under the Company's responsibility and to request copies of such personal data, including requesting the Company to disclose how such personal data was obtained.

3. Right to Data Portability

The data subject has the right to receive his or her personal data where the Company has processed such personal data in a format that is readable or usable by automatic means and can be used or disclosed by automated methods. The data subject also has the right to request the Company to send or transfer such personal data in such format to another data controller, where technically feasible.

The personal data referred to above shall be personal data for which the data subject has given consent to the Company to collect, use, or disclose, or personal data that the Company is required to process in order to enable the data subject to use the Company's products and/or services under a contract to which the Company is a party, or to take steps at the request of the data subject prior to using the Company's products and/or services, or other personal data as prescribed by law.

4. Right to Object

The data subject has the right to object at any time to the collection, use, and/or disclosure of personal data where such collection, use, and/or disclosure is carried out for the Company's or a third party's legitimate interests, within the scope that the data subject may reasonably expect, or for the performance of a task carried out in the public interest.

Where the data subject raises an objection, the Company may continue to collect, use, and/or disclose such personal data only where the Company can demonstrate compelling legitimate grounds that override the fundamental rights and freedoms of the data subject, or where such processing is necessary for the establishment, compliance with, or defines of legal claims, as applicable.

In addition, the data subject has the right to object to the collection, use, or disclosure of personal data for marketing purposes, or for scientific, historical, or statistical research purposes.

5. Right to Erasure or Destruction of Personal Data

The data subject has the right to request the erasure or destruction of his or her personal data, or to request that such personal data be made anonymous, where the data subject believes that such personal data has been collected, used, or disclosed unlawfully, or where the Company no longer needs to retain such personal data for the purposes set out in this Notice, or where the data subject has exercised the right to withdraw consent or the right to object as described above.

6. Right to Restriction of Processing

The data subject has the right to request the temporary restriction of the processing of personal data where the Company is in the process of verifying a request for rectification, considering an objection, or in any other case where the Company is required by applicable law to erase or destroy personal data but the data subject requests restriction of use instead.

7. Right to Rectification

The data subject has the right to request the correction of his or her personal data to ensure that such personal data is accurate, up to date, complete, and not misleading.

8. Right to Lodge a Complaint

The data subject has the right to lodge a complaint with the relevant competent authority where the data subject believes that the collection, use, and/or disclosure of his or her personal data is in violation of or non-compliant with applicable laws.

The data subject may exercise such rights by completing the Data Subject Rights Request Form through the channels specified in Section 13 (Compliance with the Personal Data Protection Policy and Contact Information). The exercise of the above rights may be subject to limitations under applicable laws, and in certain cases, the Company may refuse or be unable to comply with such requests, for example, where required to comply with laws, court orders, public interest, or where the exercise of such rights may infringe upon the rights or freedoms of others. Where the Company refuses such request, the Company shall inform the data subject of the reasons for such refusal.

Security Measures for Personal Data

1. The security of personal data is important to the Company. The Company shall implement appropriate technical and administrative security measures to protect personal data against loss, unauthorized access, use, or disclosure, misuse, alteration, and destruction, by using security technologies and procedures such as encryption and access controls, to ensure that only authorized persons can access personal data. Such people are required to be trained on the importance of protecting personal data.
2. The Company has implemented appropriate security measures to prevent the loss of, unauthorized access to, use of, alteration, modification, or disclosure of personal data by persons who have no authority or duties in relation to such personal data. The Company shall review and update such measures as necessary in response to changes in technology to ensure an appropriate level of security.

Management of Personal Data Breach Incidents

The Company has established procedures for managing personal data breach incidents as follows:

1. Where a personal data breach is detected or a complaint regarding a personal data breach is received, the person who detects or receives such complaint shall report the incident to the Chairperson of the Company's Personal Data Working Committee or the Data Protection Officer, in order to conduct an investigation, coordinate with the responsible units to identify the cause of the personal data breach, and report the incident to the relevant supervisory authorities as required by applicable laws.
2. Where the cause of the personal data breach is identified as follows:
 - **The Company's systems:**

The Company shall coordinate with the Information Technology Department to suspend or temporarily shut down the relevant systems to correct and remedy the errors or notify the external system service provider to take immediate corrective actions.

- **The Company's personnel:**

The Company shall immediately suspend such person's access to personal data and establish an investigation committee in accordance with the Company's measures.

- **External service providers:**

The Company shall require the external service provider to investigate the cause and report back to the Company within 24 hours from the time the Company provides the relevant information. During such period, the Company shall temporarily suspend the transfer of personal data to such external service provider until the issue has been resolved.

3. For personal data that has been leaked, the Company shall take appropriate actions to manage such data and mitigate damage to the greatest extent possible, in accordance with legal procedures or other appropriate measures, as applicable.
4. The Company shall periodically inform the complainant of the progress regarding damage mitigation, the cause of the incident, and the correct and preventive measures implemented by the Company at each stage.

Links to Third-Party Websites

When using the Company's applications or websites, there may be links to social networks, platforms, or other websites operated by third parties. The Company will only link to websites that maintain personal data protection standards. However, the Company is not responsible for the content or personal data protection standards of such third-party websites.

Any personal data provided by the data subject to third-party websites will be collected by such third parties and will be subject to their respective privacy notices or personal data protection policies (if any).

Amendments to the Personal Data Protection Policy

The Company may revise or amend this Personal Data Protection Policy from time to time without prior notice to data subjects, to ensure appropriateness and efficiency in providing services. Data subjects are therefore encouraged to review this Personal Data Protection Policy each time they visit or use the Company's services or websites.

Compliance with the Personal Data Protection Policy and Contact Information

If a data subject has any questions, concerns, or suggestions regarding this Personal Data Protection Policy or the Company's compliance with this Policy, the Company is pleased to respond to such inquiries and to receive feedback for the purpose of improving personal data protection and the Company's services. Data subjects may contact the Company using the contact details provided below.

- **Precise Corporation Public Company Limited**

*1842 Bangkok–Nonthaburi Road, Wong Sawang, Bang Sue,
Bangkok 10800, Thailand*

Tel: +66 (0) 2-910-9700



Data Protection Officer (DPO)

*1842 Bangkok–Nonthaburi Road, Wong Sawang, Bang Sue,
Bangkok 10800, Thailand*

Tel: +66 (0) 2-910-9700

Email: pcc_dpo@precise.co.th

Governing Law

This Personal Data Protection Policy shall be governed by and construed in accordance with the laws of Thailand. The courts of Thailand shall have exclusive jurisdiction over any disputes that may arise in connection with this Policy.