



PPP GREEN COMPLEX

Privacy Policy

PPP Green Complex Public Company Limited

1. Introduction

PPP Green Complex Public Company Limited (hereinafter referred to in this Policy as the "Company") recognizes the importance of personal data and other information relating to data subjects (collectively, "Information"). To ensure that data subjects can be confident that the Company operates with transparency and accountability in the collection, use, or disclosure of data subjects' Information in accordance with the Personal Data Protection Act B.E. 2562 (the "Personal Data Protection Law") and other relevant laws, this Privacy Policy (the "Policy") has been prepared to explain to data subjects the details regarding the collection, use, or disclosure (collectively, "Processing") of personal data carried out by the Company, including by officers and related persons acting on behalf of the Company, as set out below.

2. Scope of Application of this Policy

This Policy applies to the personal data of persons who have a relationship with the Company, whether currently or in the future, whose personal data is Processed by the Company, its officers, contract employees, business units, or other units operated by the Company, and includes counterparties or third parties who process personal data on behalf of the Company (the "Personal Data Processor") under the Company's products and services, such as websites, systems, applications, documents, or other forms of service controlled by the Company (collectively, the "Services").

Persons having a relationship with the Company under the preceding paragraph include:

- 1) Individual customers;
- 2) Officers or employees;
- 3) Business partners and service providers who are individuals;
- 4) Directors, authorized representatives, agents, attorneys, shareholders, employees, or other persons with a similar relationship with juristic persons related to the Company;
- 5) Users of the Company's products or services;
- 6) Visitors to or users of the website www.pppgc.co.th, including related systems, applications, devices, or other communication channels controlled by the Company;
- 7) Other persons whose personal data is collected by the Company, such as job applicants, family members of officers, guarantors, and beneficiaries under insurance policies.

Items 1) to 6) are collectively referred to as the "Data Subjects."

In addition to this Policy, the Company may issue a privacy notice (the "Notice") for its specific products or services, in order to inform data subjects who are users of such services about the personal data being processed, the purposes and lawful grounds for processing, the retention period, and the rights of the data subject with respect to that specific product or service.

In the event of any material conflict between the content of a Notice and this Policy, the Notice relating to that particular service shall prevail.

3. Definitions

- **"Company"** means PPP Green Complex Public Company Limited.
- **"Personal Data"** means information relating to a natural person which enables the identification of that person, whether directly or indirectly, but does not include the information of deceased persons.
- **"Sensitive Personal Data"** means personal data as stipulated under Section 26 of the Personal Data Protection Act B.E. 2562, including data on race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union data, genetic data, biometric data, or any other data which affects the data subject in a similar manner as announced by the Personal Data Protection Committee.
- **"Processing of Personal Data"** means any operation performed on personal data, such as collection, recording, copying, organizing, retention, updating, alteration, use, retrieval, disclosure, transfer, dissemination, combination, deletion, or destruction.
- **"Data Subject"** means a natural person who is the owner of personal data collected, used, or disclosed by the Company.
- **"Data Controller"** means a person or juristic person who has the authority to make decisions regarding the collection, use, or disclosure of personal data.
- **"Data Processor"** means a person or juristic person who processes personal data, including collection, use, or disclosure, on the instructions of, or on behalf of, a Data Controller; provided that such person or juristic person is not thereby deemed to be a Data Controller.

4. Sources of Personal Data Collected by the Company

The Company collects or obtains various types of personal data from the following sources:

- 1) Personal data that the Company collects directly from the data subject through its service channels, such as during the application, registration, job application, contract signing, documentation, survey process, or use of products, services, or other service channels controlled by the Company, or when the data subject communicates with the Company at its premises or through other contact channels controlled by the Company.
- 2) Data collected by the Company from the data subject's use of the Company's website, products, or other services under contract or mission, such as tracking the data subject's behavior in using the Company's website, products, or services through the use of cookies, or from software on the data subject's device.
- 3) Personal data that the Company collects from sources other than the data subject, where such source has the authority, a lawful reason, or has obtained the data subject's consent to

disclose the data to the Company, such as the linking of government digital services for the purpose of providing integrated public benefit services to the data subject directly, or receiving personal data from other government agencies in connection with the Company's mission to establish a central data exchange center to support government agencies in providing services to the public through digital systems, as well as personal data exchanged with contractual counterparties as necessary for providing services under a contract.

In addition, this includes cases where the data subject provides the Company with the personal data of a third party. In such cases, the data subject is responsible for informing such third party of the details under this Policy or the relevant Notice, as applicable, and for obtaining that person's consent where consent is required for the disclosure of information to the Company. If the data subject refuses to provide information necessary for the Company to provide its services, this may result in the Company being unable to provide all or part of such services to the data subject.

5. Legal Basis for the Collection of Personal Data

The Company considers and determines the legal basis for collecting the personal data of data subjects as appropriate to, and in the context of, the services provided. The legal bases used by the Company for collecting personal data include:

Legal Basis	Details
Performance of a task in the public interest / exercise of official authority	To enable the Company to perform tasks in the public interest under its mission as authorized by law.
Compliance with a legal obligation	To enable the Company to comply with laws governing the Company, such as: the Personal Data Protection Act B.E. 2562, including related rules, regulations, orders and Cabinet resolutions; collection of computer traffic data under the Computer-Related Crime Act B.E. 2560; the Public Organization Act B.E. 2542; tax laws; and compliance with court orders, among others.
Legitimate interests	For the legitimate interests of the Company or another person, where such interests are not overridden by the data subject's fundamental rights, such as security of the Company's premises, or processing for the Company's internal operations.
Prevention or suppression of danger to life, body or health	To prevent or suppress danger to the life, body, or health of a person, such as providing an application to monitor an epidemic under government policy.
Performance of a contract	To perform the Company's obligations under a contract, or take steps at the data subject's request prior to entering a contract, such as employment, procurement of work, memoranda of cooperation, or other agreements.
Archiving in the public interest, research or statistics	To prepare or support the preparation of historical archives, research, or statistics as assigned to the Company, such as compiling service usage statistics.
Consent of the data subject	For collection, use, or disclosure requiring consent, having informed the data subject of the purpose beforehand, such as collecting sensitive personal data outside the exceptions under Section 24 or 26 of the Act, or marketing products/services of business partners.

Where the Company needs to collect a data subject's personal data for the performance of a contract, compliance with a legal obligation, or steps necessary to enter into a contract, if the data subject refuses to provide such personal data or objects to the processing for the purposes of the relevant activity, this may result in the Company being unable to carry out the activity or provide the service requested by the data subject, in whole or in part.

6. Types of Personal Data Collected by the Company

The Company may collect or obtain the following data, which may include the personal data of data subjects, depending on the service used or the relationship the data subject has with the Company. The categories below represent only a general framework; only categories relevant to the specific product, service, or relationship shall apply.

Category	Details and Examples
Identification Data	Title, first name, last name, middle name, nickname, signature, national ID number, nationality, driving licence number, passport number, house registration data, professional/occupational licence number, social security number, etc.
Personal Characteristics	Date of birth, gender, height, weight, age, marital status, military service status, photographs, spoken language, behavioral data, preferences, bankruptcy status, incompetent/quasi-incompetent status, etc.
Contact Data	Home and mobile telephone number, fax number, email, mailing address, online usernames (Line ID, MS Teams), residential location map, etc.
Employment and Education Data	Employment type, occupation, rank, position, duties, expertise, work permit status, reference persons, taxpayer ID, position/employment history, salary, start/resignation date, performance results, welfare, work products, bank account number, educational institution, qualifications, results, graduation date, etc.
Insurance Policy Data	Insurer, insured, beneficiary, policy number, type of policy, coverage amount, claims data, etc.
Social Relationship Data	Political status, political office, directorships, relationship with the Company's officers, service contracts with, or interests in dealings with, the Company, etc.
Data on Use of the Company's Services	Account name, password, PIN, Single Sign-On (SSO) data, OTP, computer traffic data, location data, photographs, videos, voice recordings, usage behavior on Company websites/apps (e.g. www.pppgc.co.th), search history, cookies, device ID/type, connection details, browser data, language settings, operating system, etc.
Sensitive Personal Data	Race, religion, disability, political opinion, criminal record, biometric data (facial recognition), health-related data, etc.

7. Cookies

The Company collects and uses cookies and other similar technologies on websites under its control, such as www.pppgc.co.th, or on the data subject's device, depending on the service used.

This is carried out for security purposes in providing the Company's services and to give data subjects a convenient and good user experience. Such data is also used to improve the Company's website to better meet data subjects' needs. Data subjects may set or delete cookies themselves through their web browser settings.

8. Personal Data of Minors, Incompetent Persons and Quasi-Incompetent

Persons

Where the Company becomes aware that personal data requiring consent for collection belongs to a data subject who is a minor, an incompetent person, or a quasi-incompetent person, the Company will not collect such personal data until it has obtained consent from the person exercising parental authority, the guardian, or the curator, as applicable, in accordance with the conditions prescribed by law.

Where the Company was not previously aware that a data subject was a minor, an incompetent person, or a quasi-incompetent person, and later discovers that it has collected such person's personal data without the required consent, the Company will promptly delete or destroy such personal data, unless it has another lawful ground, apart from consent, for the collection, use, or disclosure of such data.

9. Purposes of Collection of Personal Data

The Company collects personal data for a number of purposes, depending on the type of product, service, or activity used, and the nature of the relationship with the data subject. The purposes below represent only a general framework; only purposes relevant to the specific product, service, or relationship shall apply:

- 1) To carry out actions necessary for the successful completion of a task assigned to the Company, or as necessary for the exercise of legal authority the Company has under relevant laws;
- 2) To provide and manage the Company's services, including services under contracts with data subjects or in accordance with the Company's mission;
- 3) To conduct the Company's business transactions;
- 4) To control, use, monitor, verify, and manage services in order to facilitate and meet the needs of data subjects;
- 5) To retain and update information relating to data subjects, including documents referring to them;
- 6) To maintain records of personal data processing activities as required by law;
- 7) To analyze data, including resolving issues relating to the Company's services;
- 8) To carry out actions necessary for internal administration, including recruitment, selection of directors or officeholders, and qualification assessments;
- 9) To prevent, detect, avoid, and investigate fraud, security breaches, or prohibited or unlawful acts that may cause damage to the Company and/or data subjects;
- 10) To verify identity, authenticate, and check information when a data subject applies for, or contacts the Company for, services, or exercises legal rights;

- 11) To improve and develop the quality of products and services to keep them up to date;
- 12) To assess and manage risk;
- 13) To send notifications, confirm orders, communicate, and provide information to data subjects;
- 14) To prepare and deliver relevant and necessary documents or information;
- 15) To verify identity and prevent spam or unauthorized or unlawful acts;
- 16) To examine how data subjects access and use the Company's services, in aggregate and individually, and for research and analysis purposes;
- 17) To carry out actions necessary to comply with the Company's obligations to regulatory or tax authorities, law enforcement, or other legal obligations;
- 18) To carry out actions necessary for the legitimate interests of the Company or other persons/juristic persons involved;
- 19) To prevent or suppress danger to the life, body, or health of a person, including epidemic surveillance;
- 20) To prepare historical documents for the public interest, research, or statistics as assigned to the Company; and
- 21) To comply with laws, notifications, or orders in force, or conduct legal proceedings, including actions relating to data pursuant to a court order, and to exercise rights relating to data subjects' data.

10. Types of Persons to Whom the Company Discloses Personal Data

For the purposes set out in Section 9 above, the Company may disclose the personal data of data subjects to the following categories of persons. The categories below represent only a general framework; only categories relevant to the specific product, service, or relationship shall apply:

Category of Recipient	Details
Government agencies or authorities (for legal compliance or other important purposes)	Law enforcement agencies or agencies with regulatory authority or other important purposes, such as the Revenue Department, the Royal Thai Police, the courts, the Office of the Attorney General, the Department of Disease Control, the Ministry of Digital Economy and Society, etc.
Committees involved in the Company's legal compliance	Persons holding directorships on various committees, such as the board of directors, shareholders' committee, etc.
Counterparties administering officer benefits	Third parties engaged to manage benefits, such as insurance companies, hospitals, payroll service providers, banks, telephone service providers, etc.
Business partners	Persons collaborating with the Company to provide services to data subjects, such as service providers contacted through the Company's services, marketing/advertising providers, financial institutions, platform providers, telecommunications providers, etc.

Category of Recipient	Details
Service providers	Persons engaged to provide services on the Company's behalf or support its operations, e.g. data storage (cloud, document warehousing), software/application/website developers, document delivery, payment services, internet/telephone providers, Digital ID providers, social media providers, risk management providers, external consultants, transport providers, etc.
Other categories of recipients	The Company's contacts, family members, non-profit foundations, temples, hospitals, educational institutions, or other agencies, for purposes such as service matters, training, awards, or charitable donations, etc.
Public disclosure	Disclosure to the public where necessary, such as where the Company must publish information in the Government Gazette or pursuant to a Cabinet resolution, etc.

11. Cross-Border Transfer of Personal Data

In certain cases, the Company may need to send or transfer data subjects' personal data to a foreign country to carry out the purposes of providing services, such as sending personal data to a cloud system whose platform or servers are located overseas (e.g. Singapore or the United States), to support information technology systems located outside Thailand. This depends on the particular service used by, or activity relevant to, the data subject.

However, as of the preparation of this Policy, the Personal Data Protection Committee has not yet announced a list of destination countries with adequate standards of personal data protection. Accordingly, where the Company needs to send or transfer personal data to a destination country, the Company will ensure that the data transferred is subject to adequate protection measures in accordance with international standards, or will comply with the conditions enabling the lawful transfer of such data, including:

- 1) Compliance with a law that requires the Company to send or transfer personal data abroad;
- 2) Having notified the data subject and obtained consent, where the destination country does not have adequate protection standards, in accordance with the list of countries announced by the Personal Data Protection Committee;
- 3) Where necessary for the performance of a contract to which the data subject is a party with the Company, or to comply with the data subject's request prior to entering into such contract;
- 4) Where it is an act in compliance with a contract between the Company and another person or juristic person for the benefit of the data subject;
- 5) To prevent or suppress danger to the life, body, or health of the data subject or another person, where the data subject is unable to give consent at that time; or
- 6) Where necessary for carrying out a task for an important public interest.

12. Retention Period of Personal Data

The Company will retain data subjects' personal data for as long as it remains necessary for the purposes for which it was collected, as specified in this Policy, a Notice, or under relevant law.

Once such period has elapsed and the data is no longer necessary for such purposes, the Company will delete, destroy, or anonymize the personal data so that it can no longer identify the data subject, in accordance with the format and standards for deletion or destruction announced by the Committee or under the law, or international standards. However, in the case of a dispute, exercise of rights, or legal proceedings relating to a data subject's personal data, the Company reserves the right to continue retaining such data until the dispute is finally resolved by an order or judgment.

13. Provision of Services by Third Parties or Sub-processors

The Company may engage or procure a third party (a "Data Processor") to process personal data on its behalf or in its name. Such third parties may offer various types of services, such as hosting, outsourcing, or cloud computing services, or other forms of work engagement.

Where the Company assigns a third party to process personal data as a Data Processor, the Company will put in place an agreement specifying the rights and duties of the Company as a Data Controller and of the Data Processor, including the details of the types of personal data assigned for processing, the purposes, the scope of processing, and other relevant terms. The Data Processor may process personal data only within the scope specified in the agreement and in accordance with the Company's instructions, and may not process the data for any other purpose.

Where a Data Processor engages a sub-processor to process personal data on its behalf, the Company will require the Data Processor to enter into an agreement with the sub-processor, in a form and to a standard no lower than that of the agreement between the Company and the Data Processor.

14. Security Measures for Personal Data

The Company has measures in place to protect personal data by restricting access to only those officers or authorized/assigned persons who need such access for the purposes previously notified to the data subject. Such persons must strictly adhere to the Company's personal data protection measures and maintain the confidentiality of personal data of which they become aware in the course of their duties. The Company maintains organizational and technical security measures that meet international standards and comply with those announced by the Personal Data Protection Committee.

In addition, when the Company sends, transfers, or discloses personal data to a third party, whether under its mission, a contract, or another form of agreement, the Company will establish appropriate security and confidentiality measures in compliance with the law, to ensure that personal data collected by the Company remains secure at all times.

15. Links to External Websites or Services

The Company's services may contain links to third-party websites or services, which may have their own privacy policies that differ in substance from this Policy. The Company recommends that data subjects review the privacy policy of any such website or service before accessing it. The Company has no involvement in, or control over, the personal data protection measures of such websites or services, and cannot be responsible for the content, policies, damages, or actions arising from third-party websites or services.

16. Data Protection Officer

The Company has appointed a Data Protection Officer to monitor, oversee, and provide advice on the collection, use, or disclosure of personal data, including coordinating and cooperating with the Office of the Personal Data Protection Committee, to ensure compliance with the Personal Data Protection Act B.E. 2562.

17. Rights of Data Subjects under the Personal Data Protection Act B.E. 2562

The Personal Data Protection Act B.E. 2562 grants data subjects a number of rights, which will take effect once the relevant provisions of the law come into force. The details of such rights are as follows:

- 1) **Right of access** – Data subjects have the right to access, receive a copy of, and request disclosure of the source of their personal data collected by the Company without their consent, except where the Company has the right to refuse such request on legal grounds or by court order, or where doing so would adversely affect the rights and freedoms of others.
- 2) **Right to rectification** – If a data subject finds that their personal data is inaccurate, incomplete, or not up to date, they have the right to request correction to make it accurate, current, complete, and not misleading.
- 3) **Right to erasure or destruction** – Data subjects have the right to request that the Company delete or destroy their personal data, or anonymize it so that it can no longer identify them, subject to the conditions prescribed by law.
- 4) **Right to restriction of processing** – Data subjects have the right to request restriction of the use of their personal data in the following cases:
 - a) During the period the Company is verifying a data subject's request for correction of personal data;
 - b) Where the data subject's personal data has been collected, used, or disclosed unlawfully;
 - c) Where the data subject's personal data is no longer necessary for the purposes for which the Company collected it, but the data subject requires the Company to continue retaining it for the establishment, exercise, or defense of legal claims; or
 - d) During the period the Company is verifying whether it has an overriding legitimate ground to continue collecting, using, or disclosing the data, or examining the necessity of doing so for the public interest, following the data subject's exercise of the right to object.
- 1) **Right to object** – Data subjects have the right to object to the collection, use, or disclosure of their personal data, except where the Company has a lawful ground for refusing such request (e.g. where the Company can demonstrate an overriding legal ground, or for the establishment, compliance with, or exercise of legal claims, or for the Company's public interest).
- 2) **Right to withdraw consent** – Where a data subject has given consent for the collection, use, or disclosure of personal data (whether given before or after the Personal Data Protection Act B.E. 2562 came into force), the data subject has the right to withdraw such consent at any time during the period the data is retained by the Company, unless restricted by law, or where the Company is required to continue retaining the data, or where a contract benefiting the data subject remains in effect.

3) **Right to data portability** – Data subjects have the right to request their personal data from the Company in a format that is readable or commonly used by automatic tools, and to have it used or disclosed by automated means, including requesting the Company to send or transfer such data to another data controller, subject to the conditions prescribed by law.

18. Penalties for Non-Compliance with this Privacy Policy

Failure to comply with this Policy may constitute a breach subject to disciplinary action under the Company's rules (for officers or employees of the Company), or under the personal data processing agreement (for Data Processors), as applicable to the case and the relationship the data subject has with the Company, and may also result in penalties under the Personal Data Protection Act B.E. 2562, as well as related subordinate legislation, rules, regulations, and orders.

19. Complaints to the Supervisory Authority

If a data subject finds that the Company has not complied with the personal data protection law, the data subject has the right to file a complaint with the Personal Data Protection Committee or the supervisory authority appointed by the Committee or under the law. However, before filing such a complaint, the Company requests that the data subject first contact the Company, so that the Company may have the opportunity to learn the facts, provide clarification, and resolve the data subject's concerns.

20. Amendment of this Privacy Policy

The Company may review, revise, or amend this Policy as it deems appropriate, and will notify data subjects through the website www.pppgc.co.th, indicating the effective date of each revised version. The Company nevertheless recommends that data subjects regularly check for updated versions of this Policy through the relevant application or activity-specific channel operated by the Company, particularly before disclosing personal data to the Company.

Continued use of the Company's products or services after a new Policy takes effect shall be deemed acknowledgment of, and agreement to, the new Policy. If a data subject does not agree with the details of this Policy, the data subject should discontinue use of the services and contact the Company for further clarification.

21. Contact for Inquiries or Exercise of Rights

If a data subject has any questions, suggestions, or concerns regarding the Company's collection, use, and disclosure of personal data, or regarding this Policy, or wishes to exercise their rights under the personal data protection law, the data subject may contact:

1) Data Controller

Name: PPP Green Complex Public Company Limited

Address: 321 Moo 5, Chang Raek Sub-district, Bang Saphan Noi District, Prachuap Khiri Khan 77170

Telephone (Head Office): +66 32 909 611

Email: info@pppgc.co.th

2) Data Protection Officer (DPO)

Address: 321 Moo 5, Chang Raek Sub-district, Bang Saphan Noi District, Prachuap Khiri Khan 77170

Telephone (Head Office): +66 32 909 611

Email: dpo@pppgc.co.th