

Privacy Policy for Directors, Subcommittees,
and Advisors to the Board

Project Planning Service Public Company Limited and Its Subsidiaries

1. Introduction

Project Planning Service Public Company Limited and its subsidiaries (hereinafter referred to in this Policy as "PPS") recognize the importance of personal data and other related information (collectively referred to as the "Data") concerning the Company's directors, subcommittee members, and board advisors (collectively referred to as "you"). This Policy is intended to assure you that PPS is committed to maintaining transparency and accountability in the collection, use, and disclosure of your Data in accordance with the Personal Data Protection Act B.E. 2562 (2019) (the "PDPA") as well as other applicable laws. This Privacy Policy for Directors, Subcommittees, and Advisors to the Board ("Policy") has been established to inform you of the details concerning the collection, use, disclosure, deletion, and destruction of your personal data (collectively referred to as "Processing") as carried out by PPS, including its officers and relevant personnel acting on behalf of or in the name of PPS. The contents of this Policy are as follows:

2. Definitions

"Director"	refers to a director of Project Planning Service Public Company Limited.
"Subcommittee Member"	refers to a person appointed as a member of a subcommittee by the Board of Directors of Project Planning Service Public Company Limited.
"Advisor to the Board"	refers to a person appointed as an advisor by the Board of Directors of Project Planning Service Public Company Limited.
"Personal Data"	refers to any information relating to an individual that enables the identification of such individual, whether directly or indirectly, and includes sensitive personal data, but does not include the data of deceased persons.
"Sensitive Personal Data"	includes information regarding race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union membership, genetic data, and biometric data (e.g., fingerprint scans, facial recognition data, or iris scans).

3. Scope of Policy Application

This Privacy Policy applies to the personal data of Directors, Subcommittee Members, and Advisors to the Board throughout their term of service as stipulated by law.

4. Sources of Personal Data Collected by PPS

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

- 1) PPS collects personal data from Directors, Subcommittee Members, Advisors to the Board, and individuals nominated for such positions. This data may be collected directly from you or from government agencies, regulatory authorities, and publicly available sources, as follows:
 - a) During the nomination process, PPS collects personal data from national identification cards or government-issued documents that can be used to verify identity, such as full name, gender, ID number, passport number, photograph, date of birth, nationality, place of birth, and height.
 - b) For individuals serving as Directors, Subcommittee Members, and Advisors to the Board, PPS collects additional data such as remuneration payment records, bank account numbers, email addresses, educational background, occupation, work history, self-evaluation results, and any other data required by applicable laws.
- 2) Personal data collected directly from you via various channels, such as applications, registrations, personal data disclosure forms for nominated directors or chairpersons, or personal profiles.
- 3) PPS Personal data collected from third-party sources, where such sources are legally authorized or have obtained consent from the data subject to disclose the data to PPS.
- 4) Personal data obtained from public records.
- 5) PPS Personal data obtained from government authorities and/or regulatory agencies exercising legal authority. Additionally, if you provide PPS with personal data of third parties, you are responsible for informing such persons of the details in this Policy and obtaining their consent, where required, before disclosing their personal data to PPS.

5. Legal Basis for Personal Data Collection

PPS determines the legal basis for collecting your personal data in accordance with applicable laws. The legal bases upon which PPS relies for the collection of personal data include the following:

Legal Basis for Data Collection	Details
1. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in PPS.	For the public interest or the exercise of rights by a government official.
2. For the performance of duties as required by law.	To enable PPS to comply with applicable laws and regulatory requirements.
3. It is necessary for legitimate interests.	For the legitimate interests of PPS and others, where such interests are not overridden by the fundamental rights and freedoms of the data subjects.
4. It is necessary for the establishment, exercise, or defense of legal claims.	For the establishment of rights, the exercise or enforcement of legal claims, or the defense against legal claims.
5. For the prevention or suppression of harm to a person's life, body, or health	To prevent or suppress harm to a person's life, body, or health.
6. Your consent	For the collection, use, or disclosure of personal data in cases where PPS is required to obtain your consent, and such purpose has been informed to you prior to the request for consent — for example, the collection of sensitive personal data for purposes not exempted under Section 24 or Section 26 of the Personal Data Protection Act.

In cases where PPS is required to collect your personal data for the purpose of fulfilling your role, complying with legal obligations, or for the necessity of maintaining your position throughout your term, your refusal to provide such data or objection to the processing thereof for the stated purposes may result in PPS being unable to fulfill your requests, in whole or in part.

6. Types of Personal Data Collected by PPS

PPS may collect or obtain the following types of data, which may include your personal data. The collection depends on the context, the nature of your relationship with PPS, and other relevant considerations affecting the collection of such data. The categories of personal data listed below are intended as a general framework for the types of personal

data that PPS may collect.

Types of Personal Data	Details and Examples
1. Personally Identifiable Information	Personal identification data, including any name-related information or official documents that specifically identify you (including copies of relevant identification documents), such as: title, first name, last name, signature, national identification number, nationality, driver's license number, passport number, household registration information, professional license number (for each profession), social security reference number, and personal insurance number, etc.
2. Personal characteristics data	Detailed personal information, such as date of birth, gender, height, weight, age, marital status, photographs, bankruptcy status, and other related personal details.
3. Contact information	Contact information for reaching you, such as mobile phone number, fax number, email address, and residential mailing address, etc.
4. Work and Education Information	Employment details, including work and education history, such as: Type of employment, Profession Rank, Position, Department, Responsibilities, Expertise, History of holding positions, Work history Employment start date, Employment end date, Achievements, Bank account number, Educational institution, Educational qualifications, Academic results, Terms and conditions, Status as director, subcommittee member, and board advisor, Position held, Workplace location, Employment history, Reason for resignation, etc.
5. Payment Information	Payment details such as bank account information, taxpayer identification number, and tax deduction information.
6. Sensitive Personal Data	Your sensitive personal data, such as religious beliefs, criminal records, etc.

7. Purposes for Collecting Personal Data

PPS collects your personal data for various purposes, including but not limited to:

- 1) To carry out necessary actions relating to you, such as making payments or providing you with entitled benefits.
- 2) To enable you to perform your duties as a director, sub-committee member, or board advisor within PPS, including but not limited to: issuing power of attorney, appointing representatives, conducting internal audits and investigations in case of complaints, and implementing disciplinary actions when necessary. This also includes appointment procedures and onboarding of directors, sub-committee members, and board advisors.
- 3) To verify and authenticate your identity, for example, to identify, recognize, and confirm your identity.
- 4) To support your role and responsibilities, including providing the necessary tools and equipment required to fulfill your duties.
- 5) To compensate and provide entitled benefits, such as meeting allowances, tax deductions, award cards, discounts, and other director-related benefits.
- 6) To facilitate communication with you, including work-related correspondence, meeting invitations, and emergency contact.
- 7) To fulfill obligations under the company's regulations and to comply with applicable laws and legal requirements.
- 8) To prevent, detect, avoid, and investigate fraud, security breaches, or unlawful activities, which could potentially cause damage to both PPS and the data subjects.
- 9) To manage communications and the relationship between PPS and you.
- 10) To ensure security, such as safeguarding facilities, systems, and individuals.
- 11) To include your information in PPS's official publications, such as posting on the PPS website (as permitted by law) and inclusion in public disclosures in accordance with the practices of a listed public company, including the Annual Report.

PPS may use your sensitive personal data for the following purposes:

- 1) Religion: For the purpose of identity verification and the provision of appropriate welfare benefits (e.g., meal arrangements, granting religious holidays).
- 2) Criminal record: To support appointment considerations and ensure compliance with legal requirements, corporate image management, creation of a watchlist, and for security purposes.

8. Types of Persons to Whom PPS May Disclose Your Personal Data

Under the purposes specified in Section 7, PPS may disclose your personal data to the following types of recipients. The categories listed below represent a general framework for PPS's disclosure of personal data:

Types of Data Recipients	Details
1. Government agencies or authorized entities to whom PPS is required to disclose personal data for the purpose of complying with legal obligations or for other significant purposes (such as actions carried out for the public interest).	Law enforcement agencies, regulatory authorities, or other entities with significant purposes, such as the Cabinet, relevant Ministers, Department of Provincial Administration, Revenue Department, Police Department, Courts, Office of the Attorney General, Department of Disease Control, etc.
2. Committees related to the legal compliance and operations of PPS.	PPS may disclose your information to individuals holding positions as directors in various committees.
3. Business partners	PPS may disclose your information to parties working with PPS, such as service providers you interact with through PPS services, marketing service providers, advertising media, financial institutions, platform providers, telecommunications service providers, and others.
4. Service Providers	PPS may delegate other parties to act as service providers or to support PPS operations, such as data storage providers (e.g., cloud services, document warehouses), system developers, software and application providers, website operators, document delivery services, payment service providers, internet service providers, telephone service providers, Digital ID service providers, social media service providers, risk management service providers,

Types of Data Recipients	Details
5. Other Types of Data Recipients	PPS may disclose your personal data to other types of recipients, such as PPS contacts, family members, non-profit foundations, temples, hospitals, educational institutions, or other relevant agencies. This disclosure is for purposes related to PPS services, training, reward programs, charitable donations, and similar activities.
6. Public Disclosure	PPS may disclose your information to the public when necessary, such as in cases where PPS is required to publish in the Government Gazette or by resolutions of the Cabinet, and in cases mandated by law, such as disclosure on the company's website.
7. External Parties Required by Law	In certain cases, we may need to disclose or share your personal data to comply with legal obligations or regulatory duties. Such parties include law enforcement agencies, courts, regulatory authorities, government agencies, or external parties when we deem it necessary to fulfill legal or regulatory obligations, protect the rights of PPS, the rights of third parties, or individual safety, or to detect, prevent, or address fraud, security, or safety issues.

9. Cross-Border Transfer of Personal Data

In certain cases, PPS may need to transfer or disclose your personal data to overseas locations. For example, this may occur when personal data is transferred to cloud systems with platforms or servers located abroad (such as in Singapore or the United States) to support IT systems based outside Thailand. If PPS needs to transfer your personal data to a foreign country, PPS will ensure that adequate data protection measures are in place, in accordance with international standards, or will take necessary actions to comply with applicable laws for such transfers. This is unless you have been informed and given your consent in cases where the destination country's personal data protection standards are deemed insufficient, based on the list of countries announced by the Personal Data Protection Committee.

10. Retention Period of Your Personal Data

PPS will retain your personal data only as long as it is necessary for the purposes for which it was collected. Specifically, PPS will retain your data throughout your term of office and for an additional five (5) years after your term ends or upon your resignation, whichever applies. Once the retention period expires and your personal data is no longer necessary for the stated purposes, PPS will delete or anonymize your personal data accordingly.

However, in the event of any disputes or legal claims related to your personal data, PPS reserves the right to retain such data until the dispute is finally resolved by a court order or judgment.

11. Security of Personal Data

PPS has implemented measures to protect personal data by restricting access solely to authorized personnel who require such data for the purposes previously notified to the data subject. These individuals are required to strictly adhere to PPS's personal data protection policies and maintain the confidentiality of the personal data they handle. PPS employs organizational and technical security measures that comply with international standards to safeguard personal data.

12. Data Protection Officer

PPS has appointed a Data Protection Officer (DPO) responsible for overseeing compliance with personal data protection laws, providing advice on data collection, use, and disclosure, and coordinating with the Personal Data Protection Committee to ensure alignment with the Personal Data Protection Act B.E. 2562 (2019).

13. Your Rights under the Personal Data Protection Act B.E. 2562 (2019)

The Personal Data Protection Act grants data subjects various rights, which come into effect as stipulated by the law. These rights include:

- 1) **Right to Access Personal Data:** You have the right to request access to, obtain copies of, and be informed about the source of personal data collected by PPS from third parties, except in cases where PPS is legally permitted to deny such requests or where exercising this right may harm others' rights and freedoms.
- 2) **Right to Rectify Personal Data:** You may request correction of inaccurate, incomplete, or outdated personal data to ensure accuracy and completeness.
- 3) **Right to Erasure or Destruction:** You may request PPS to delete or destroy your personal data or anonymize it, subject to legal conditions.
- 4) **Right to Suspend Use:** You may request suspension of personal data use under certain circumstances such as ongoing correction requests, unlawful data processing, or when data is no longer necessary but retained for legal claims.
- 5) **Right to Object to Processing:** You have the right to object to the collection, use, or disclosure of your personal data, except when PPS has lawful grounds to deny the objection.
 - During the period when PPS is conducting an investigation in response to a request from the data subject to correct their personal data to be accurate, complete, and up-to-date.
 - When the personal data of the data subject has been collected, used, or disclosed unlawfully.
 - When the personal data of the data subject is no longer necessary to be retained according to the purpose for which PPS has collected it, but the data subject wishes for PPS to continue retaining such data for the exercise of their legal rights.
 - During the period when PPS is verifying the lawful grounds for collecting the personal data of the data subject or assessing the necessity of collecting, using, or disclosing the personal data for public interest, arising from the data subject's exercise of their right to object to the collection, use, or disclosure of their personal data.

- 6) **Right to Object to the Processing of Personal Data** You have the right to object to the collection, use, or disclosure of your personal data, except in cases where PPS has lawful grounds to refuse your request. For example, PPS may demonstrate that the collection, use, or disclosure of your personal data is justified by overriding lawful grounds, for the establishment, exercise, or defense of legal claims, or for the public interest of PPS.
- 7) **Right to Withdraw Consent** In the event that you have given consent to PPS for the collection, use, or disclosure of your personal data (whether such consent was given before or after the enforcement of the Personal Data Protection Act B.E. 2562), you have the right to withdraw your consent at any time during the period your personal data is retained. However, this right is subject to any legal restrictions that require PPS to retain the data for your benefit.
- 8) **Right to Access, Receive, or Transfer Personal Data** You have the right to request access to your personal data from PPS in a format that is readable or usable by commonly used automatic devices or tools, and to use or disclose your personal data through automated means. You may also request that PPS send or transfer such data in this format to another personal data controller. The exercise of this right is subject to conditions prescribed by law.
- 9) **Right to Know the Existence and Usage of Personal Data** You have the right to inquire about the existence, nature, and purpose of PPS's use of your personal data.
- 10) **Right to Know the Source of Personal Data** You have the right to request disclosure regarding how your personal data was obtained, particularly if it was collected without your consent.

14. Penalties for Non-Compliance with the Personal Data Protection Policy

Failure to comply with this policy may constitute a violation and result in disciplinary action according to PPS's rules and regulations (for PPS employees or personnel) or according to the personal data processing agreement (for personal data processors), depending on the case and your relationship with PPS. You may also be subject to penalties as prescribed under the Personal Data Protection Act B.E. 2562, including related subordinate laws, rules, and orders.

15. Complaints to the Supervisory Authority

If you find that PPS has not complied with the Personal Data Protection law, you have the right to file a complaint with the Personal Data Protection Committee, experts, or any supervisory authority appointed by the Personal Data Protection Committee or under the law. However, before lodging such a complaint, PPS kindly requests that you contact PPS first, so that PPS has the opportunity to be informed of the facts, clarify any issues, and address your concerns at the earliest opportunity.

16. Amendments to the Privacy Policy for Directors, Subcommittee Members, and Board Advisors

PPS may consider revising, amending, or changing this policy as deemed appropriate and will notify you of such changes through the website <https://www.pps.co.th>, with the effective date indicated for each amendment. Nonetheless, PPS recommends that you regularly review the updated policy, especially before disclosing any personal data to PPS.

17. Contact for Inquiries or Exercising Your Rights

If you have any questions, suggestions, or concerns regarding the collection, use, or disclosure of personal data by PPS, or regarding this policy, or if you wish to exercise your rights under the Personal Data Protection law, you may contact us at:

1) Data Controller

Project Planning Service Public Company Limited

Address: 381/6 Soi Rama 9 58 (Soi 7 Seri 7), Rama 9 Road,

Suan Luang Subdistrict, Suan Luang District, Bangkok 10250, Thailand

Phone: +66 (0) 2718 2785-9 ext. 108

Email: dc@pps.co.th

2) Data Protection Officer: DPO

Mr. Veera Yenpreecha

Project Planning Service Public Company Limited

Address: 381/6 Soi Rama 9 58 (Soi 7 Seri 7), Rama 9 Road,

Suan Luang Subdistrict, Suan Luang District, Bangkok 10250, Thailand

Phone: +66 (0) 2718 2785-9 ext. 345

Email: dpo@pps.co.th

Privacy Policy for Directors, Subcommittee Members, and Advisors

Revision No. 3

Effective as of November 12, 2025



(Mr. Prasong Tharachai)

Chairman of the Board