

Personal Data Protection Policy

Pro Inside Public Company Limited

Pro Inside Public Company Limited (the "Company") respects and gives importance to the right to privacy and the protection of the personal data of those connected with, or having an interest in, the Company. The Company has therefore established this Personal Data Protection Policy, to ensure that the Company is transparent and accountable in the collection, use, or disclosure (collectively, "Processing") of your data under the Personal Data Protection Act B.E. 2562 (2019) (the "Personal Data Protection Law"), including other relevant laws, and has also put in place appropriate data security measures that meet applicable standards and comply with legal requirements.

This policy applies to the personal data of persons who have, or may in the future have, a relationship with the Company, namely the personal data of personnel, employees, customers, business partners, business allies, and other stakeholders, which is Processed by the Company, including counterparties or external persons who process personal data on behalf of, or in the name of, the Company ("Personal Data Processors"). The Company has also put in place appropriate data security measures, consistent with accepted standards, to give relevant parties confidence that the protection of personal data of all the Company's personnel, customers, business partners, and business allies is secure, safe, and in compliance with legal requirements. This policy sets out the following key principles and scope of operation:

1. This policy establishes the key principles and framework for the Company's protection of personal data, so that all operations comply with the Company's duties and responsibilities as a data controller under the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws.
2. This policy applies to all Processing of personal data occurring within the scope and purposes of the Company, including Processing of personal data carried out by external persons or juristic persons, or by external equipment or systems, within such scope and purposes.
3. This policy does not cover Processing of personal data carried out by the Company's personnel solely for their own personal benefit or for the activities of that person's family, unrelated to the Company's scope and purposes.
4. Compliance with this policy must be carried out in accordance with the practice guidelines, policies, or discussion papers to be issued in further detail under this policy, including other announcements or regulations of the Company relating to information management. Details, practice guidelines, and definitions shall be referenced against TDPG3.0 (Thailand Data Protection Guidelines 3.0) and other practice guidelines adopted by the Company.

Definitions

Term	Description
Personal Data	Any information relating to a person that can identify that person, whether directly or indirectly, such as first name, surname, national ID number, telephone number, email, location data, or online data (IP Address, Cookie ID).
Sensitive Personal Data	Personal data as specified by law, such as race, ethnic origin, health data, biometric data, genetic data, political opinion, religious belief, or other data that could significantly affect the data subject.
Processing	Any operation relating to personal data, such as collection, use, disclosure, transfer, storage, correction, destruction, analysis, or any process performed on personal data.
Data Subject	A person who is the owner of personal data, whether a customer, business partner, service user, employee, external person, or a visitor to the Company's website.
Data Controller	A person or juristic person with the authority to make decisions regarding the collection, use, or disclosure of personal data. In this context, Pro Inside Public Company Limited is the Data Controller.
Data Processor	A person or juristic person that processes personal data on behalf of the Data Controller, such as a cloud service provider, an IT contractor, or a call centre service provider.
Data Protection Officer (DPO)	A person appointed by the Company to oversee compliance with the Personal Data Protection Act B.E. 2562 (2019), to provide advice, conduct reviews, and coordinate with the Office of the Personal Data Protection Committee, and to serve as a contact channel for data subjects.
Data Transfer	The sending or disclosure of personal data to an external party, whether domestically or internationally.

Term	Description
Personal Data Breach	An incident in which personal data is used or disclosed inappropriately due to an error by personnel or in a working process, such as granting the wrong user group access rights, or recording or sending a file containing personal data to an unrelated person.
Consent	The explicit indication of intent by a data subject to permit the Company to collect, use, or disclose personal data for the purposes clearly notified.
Record of Processing Activities (ROPA)	A document recording details of the Company's data processing activities, such as the purpose, parties involved, data types, data retention period, and security measures, as required by the Personal Data Protection Act B.E. 2562 (2019).

Personal Data Protection Principles

The Company's Processing of personal data — whether data of personnel, customers, business partners, business allies, or other stakeholders — must be consistent with the following principles:

1. Processing of personal data must be lawful, fair, and transparent (Lawfulness, fairness and transparency).
2. Processing of personal data must be within the specified scope and purpose, and must not be used or disclosed beyond the scope and purpose of that data processing (Purpose limitation).
3. Processing of personal data must be limited to what is necessary, relevant, and adequate for the scope and purpose of that data processing (Data minimization).
4. Personal data processed must be accurate, and data shall be kept up to date where necessary (Accuracy).
5. Personal data shall be retained only for as long as necessary for the purpose of that data processing (Storage limitation).
6. Processing of personal data must include measures to maintain data security (Integrity and confidentiality).

Duties and Responsibilities

1. The Board of Directors has the duty to consider approving the Personal Data Protection Policy and to oversee compliance with the Personal Data Protection Act B.E. 2562 (2019) and relevant laws, acting through the Audit Committee, which has the duty to oversee and monitor compliance with the policy and related regulations.
2. Management must establish rules, practice guidelines, and measures for the storage, collection, use, and disclosure of personal data appropriate to the Company's context, consistent with the policy, relevant laws, and international standards, and shall provide an organizational structure with responsible persons and appropriate roles, to oversee operations in compliance with the policy and related practice guidelines.
3. All units and employees at every level are responsible for complying with this policy and for using personal data over which the Company is the data controller with care, and for learning, understanding, and strictly complying with the law, code of business conduct, regulations, policies, practice guidelines, and various measures of the Company. Where conduct is discovered that may fall within the scope of a violation of this policy, it must be reported through the whistleblowing channel designated by the Company, with the Company's Data Protection Officer and working group responsible for monitoring, investigating, and ensuring compliance with the law.
4. Personal data processing activities must be recorded in the Record of Processing Activities (ROPA) in the format specified by the Data Protection Officer. Any initiation, amendment, improvement, or termination of a personal data processing activity by a unit must be proposed for the opinion of the Data Protection Officer working group, using the ROPA form.
5. Where there are relevant legal considerations, including the need for any document, agreement, or form, the relevant unit must consult the Data Protection Officer, which may include a joint meeting with the Data Protection Officer working group.

Data Protection Officer

The Data Protection Officer has the following duties:

1. Establish and monitor implementation of the Company's personal data protection policy and measures, to ensure that Processing of personal data complies with the Personal Data Protection Act B.E. 2562 (2019) and related rules.
2. Prepare practice guidelines and manuals for compliance with this policy, for use in training and as guidance for units and employees, including guidance for maintaining the Record of Processing Activities so that the Office of the Personal Data Protection Committee can conduct inspections.

3. Provide advice to various units, as well as the Company's employees, on compliance with this policy.
4. Inspect the operations of various units, as well as the Company's employees, regarding the Processing of personal data, to ensure compliance with this policy.
5. Coordinate and cooperate with the Office of the Personal Data Protection Committee where there are issues relating to the Company's Processing of personal data, including in respect of the Company's employees' compliance with this policy.
6. Maintain the confidentiality of personal data that they become aware of or obtain in the course of performing duties under this policy.
7. Report directly to the Board of Directors and the Chief Executive Officer where there are problems in performing duties under this policy.
8. Support and assist with personal data protection impact assessments for various units.
9. Provide advice on personal data protection matters, and act as the contact point for data subjects to receive requests and act on the exercise of data subjects' rights.
10. Monitor, investigate, and resolve complaints relating to personal data protection.
11. Maintain records relating to personal data breach incidents and notify the Office of the Personal Data Protection Committee as required by law.
12. Record opinions on various issues discussed relating to the Company's Processing of personal data.
13. Serve as the contact and coordination point for matters relating to the Company's Processing of personal data.
14. Carry out other tasks as assigned under this policy.

Personal Data Breach

1. A personal data breach incident may occur where personal data is disclosed to, or accessed by, an unauthorized person, or where personal data is used in a manner the data subject could not reasonably have anticipated.
2. Upon receiving notice of, or discovering an indication of, a personal data breach, the Data Protection Officer will assess the credibility of the incident, verify the facts, and implement appropriate measures to mitigate the impact and prevent future personal data breach incidents.
3. Where the assessment indicates an impact on the data subject's rights, the Data Protection Officer will notify the personal data breach incident to the data subject and the Office of the Personal

Data Protection Committee, as required by relevant law and announcements, in accordance with the following criteria:

Impact on the Rights and Freedoms of the Data Subject	Action Taken
No risk	– Record the personal data breach incident.
Risk	– Record the personal data breach incident. – Notify the Office of the Personal Data Protection Committee within 72 hours.
High risk	– Record the personal data breach incident. – Notify the Office of the Personal Data Protection Committee within 72 hours. – Notify the data subject promptly, together with the remediation approach.

1. Where an information technology system or related work process is unable to function, the employee or unit that discovers the incident shall notify the IT department within 4 hours of becoming aware of the incident, and the IT department shall coordinate with the Data Protection Officer to take appropriate action.
2. For other incidents relating to a personal data breach, the employee or unit that discovers the incident shall notify the Data Protection Officer directly as soon as possible, so that appropriate action can be taken.

Compliance with This Policy

1. A violation of, or failure to comply with, this policy and related measures shall be regarded as a serious disciplinary offence, which shall be subject to further relevant disciplinary action.
2. An employee or other person involved in Processing personal data within the Company's scope and purposes may be personally liable under the law for their conduct, depending on the nature and severity of the incident that occurs.

Review and Amendment

The Data Protection Officer shall review and propose amendments to this policy and related measures at least every 2 years, taking into account the criteria and methods announced by the Personal Data Protection Committee, as well as any rules, regulations, and other announcements that may arise in the future affecting the Company's protection of personal data.

Practice Guidelines for the Personal Data Protection Policy

The Company has established practice guidelines consistent with the organization's Personal Data Protection Policy, set by the person responsible for compliance, as follows:

1. Personal data protection guidelines for personnel
2. Personal data protection guidelines for business partners
3. Personal data protection guidelines for shareholders
4. Personal data protection guidelines for participants in marketing activities
5. Personal data protection guidelines for users of the Pro Inside website
6. Personal data protection guidelines for external persons
7. Practice guidelines for complaints relating to personal data
8. Data retention policy
9. Cookie policy

Reporting Tips or Complaints

Upon discovering conduct reasonably believed to violate this policy and related practice guidelines, personnel, customers, business partners, business allies, and all of the Company's employees must report the tip or complaint in accordance with the Whistleblower Policy. Complainants and whistleblowers shall be protected, and their information kept confidential, with no effect on their employment position, both during the investigation process and after it concludes.

1. By e-mail, to: whistle-blower@proinside.co.th
2. By post, addressed to: the Audit Committee, Pro Inside Public Company Limited, No. 55, A.A. Capital Ratchada Building, 5th Floor, Ratchadapisek Road, Din Daeng, Din Daeng, Bangkok 10400
3. Online, at: <http://www.proinside.co.th/contact/whistleblowing>

For inquiries or requests for advice or guidance on compliance with this policy, or with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws, please contact the Legal and Compliance function at: whistle-blower@proinside.co.th, or contact the Data Protection Officer at: DPO@proinside.co.th

Mr. Wisudhi Srisuphan

Chairman of the Board