

Privacy Policy

Pro Inside Public Company Limited

Pro Inside Public Company Limited Privacy Policy

Scope and Objectives

1. This Policy sets out the key principles and guidelines for the Company's personal data protection to ensure that all operations comply with the Company's duties and responsibilities as a personal data controller under the Personal Data Protection Act B.E. 2562.
2. This Policy applies to all personal data processing that occurs within the scope and purposes of the Company, including the processing of personal data carried out by external individuals or entities, or by external devices or systems within such scope and purposes.
3. This Policy does not cover the processing of personal data of the Company's personnel that is carried out solely for personal gain or for the activities of the family of such individuals, which are unrelated to the scope and purposes of the Company.
4. Compliance with this Policy must be carried out in accordance with the guidelines or policies or consultations to be issued in detail later under this Policy, including other announcements or regulations of the Company related to information management. Details, guidelines and meanings should be referenced in accordance with TDPG3.0 (Thailand Data Protection Guidelines 3.0) and other relevant guidelines.

Personal Data Protection Principles

The Company's processing of personal data must be carried out in accordance with the following principles;

1. The processing of personal data is lawful, transparent and auditable (Lawfulness, fairness and transparency)
2. The processing of personal data is within the specified scope and purposes and is not used or disclosed outside the scope and purposes of the data processing (Purpose limitation)
3. The processing of personal data is only necessary, relevant and sufficient for the scope and purposes of the data processing (Data minimization)
4. The processing of personal data is accurate and the data is kept up-to-date where necessary (Accuracy)
5. The storage of personal data is for the period necessary for the data processing (Storage limitation)
6. The processing of personal data has measures to maintain data security (Integrity and confidentiality)

Duties and Responsibilities

1. The Board of Directors has an administrative duty to be responsible for the implementation in accordance with the Personal Data Protection Act B.E. 2562 and related laws, through the Audit Committee, which is responsible for overseeing and monitoring compliance with the policies and related regulations.
2. All units and employees are responsible for implementing this policy, with the Company's Personal Data Protection Officer and the Working Group to monitor and ensure compliance with the law.
3. Personal data processing activities must be recorded in the Personal Data Processing Activity Log as specified by the Personal Data Protection Officer. Any initiation, amendment, improvement or termination of any personal data processing activities of the unit must be submitted for the opinion of the Working Group of Personal Data Protection Officers in accordance with the Personal Data Processing Activity Log.
4. In the event of any relevant legal considerations, including the need for any documents, agreements or forms, the unit must discuss with the Personal Data Protection Officer, which may include a joint meeting with the Working Group of Personal Data Protection Officers.

Data Protection Officer

The Data Protection Officer has the following duties:

1. Determine and monitor the implementation of the Company's personal data protection policy and measures to ensure that the processing of personal data complies with the Personal Data Protection Act B.E. 2562 and related regulations.
2. Prepare guidelines and manuals for compliance with this policy for training and use as guidelines for various departments and employees, including guidelines for recording personal data processing activities for inspection by the Personal Data Protection Committee.
3. Provide advice to various departments and employees of the Company on compliance with this policy.
4. Audit the operations of various departments and employees of the Company on the processing of personal data in accordance with this policy.
5. Coordinate and cooperate with the Personal Data Protection Committee in cases of problems regarding the processing of personal data of the Company and employees in compliance with this policy.
6. Do not disclose the confidentiality of personal data that you know or have obtained as a result of performing duties under this policy.
7. Report directly to the Board of Directors and the Chief Executive Officer in cases of problems in performing duties under this policy.

8. Support and assist in the assessment of the impact on personal data protection of various departments.
9. Provide consultation on personal data protection and serve as a point of contact for personal data owners to receive requests and take action on the exercise of their rights.
10. Follow up, investigate and resolve complaints regarding personal data protection.
11. Keep records of personal data breach incidents and report to the Personal Data Protection Committee as required by law.
12. Record opinions on various issues of discussion regarding the Company's personal data processing.
13. Act as a point of contact and coordination regarding the Company's personal data processing.
14. Perform other duties as assigned in accordance with this policy.

Violation of Personal Data Protection

1. A personal data breach may occur in the event that personal data is disclosed or accessed by an unauthorized person, or in the event that personal data is used in a manner that the data owner could not reasonably expect by law.
2. The personal data protection officer will assess the reliability of the reported information and investigate all incidents related to the violation of personal data protection in accordance with the law to take appropriate measures to mitigate the impact and prevent future personal data breaches.
3. In cases appropriate to the circumstances and severity of the incident, the personal data protection officer will report the personal data breach incident to the data owner and the Personal Data Protection Committee Office as prescribed by relevant laws and announcements, in accordance with the following criteria:

Impact on the rights and freedoms of personal data owners	Action
No Risk	- Record of personal data breach incidents
Risk	- Record of personal data breach incidents - Notify the Personal Data Protection Committee Office within 72 hours
High Risk	- Record of personal data breach incidents - Notify the Personal Data Protection Committee Office within 72 hours - Notify the data owner with the remedy as soon as possible

4. If the information technology system or related processes are unable to function, the employee or department that encounters the incident shall notify the Information Technology Department within 4 hours from the time of becoming aware of the incident, and the Information Technology Department shall coordinate with the Data Protection Officer to take appropriate action.
5. In the event of other incidents related to the breach of personal data, the employee or department that encounters the incident shall notify the Data Protection Officer directly as soon as possible to take appropriate action.

Practices

1. Any violation of this Policy and related measures shall be considered a serious disciplinary offence and shall be subject to the relevant disciplinary action.
2. Employees or other persons involved in the processing of personal data within the scope and purposes of the Company may be personally liable under the law for their actions depending on the nature and severity of the incident.

Review and Amendment

The Data Protection Officer shall review and propose amendments to this Policy and related measures at least every 2 years, considering the criteria and methods announced by the Personal Data Protection Committee, including other rules, regulations and announcements that may be issued in the future that affect the protection of personal data of the Company.

Guidelines for Personal Data Protection Policy

The Company has established guidelines to comply with the organization's personal data protection policy, which are determined by those responsible for overseeing compliance, as follows:

1. Guidelines for personal data protection for personnel
2. Guidelines for personal data protection for business partners
3. Guidelines for personal data protection for shareholders
4. Guidelines for personal data protection for participants in marketing activities
5. Guidelines for personal data protection for users of the Pro Inside website
6. Guidelines for personal data protection for external parties
7. Guidelines for complaints regarding personal data
8. Data retention policy
9. Cookie policy

Approved by the Board of Directors Meeting No. 3/2024

On February 27, 2024