

# **Personal Data Protection Policy**

## Objective

Ngernturbo Public Company Limited ("the Company") and subsidiaries recognize the right of privacy. Therefore, we have established guidelines for managing personal data in a secure manner and preventing the violation of personal data rights, in accordance with the Personal Data Protection Act B.E. 2562 (2019). Thus, the collection, use, and disclosure of personal data will be included in this policy. The Company and subsidiaries are committed to managing the collection, use, and disclosure of personal data of customers, policyholders, and the public accurately, appropriately, and transparently, as well as protecting personal data in accordance with the Personal Data Protection Act B.E. 2562 (2019).

## Policy Changes and Review

Policy changes must be approved by the Chief Risk Officer. A policy review is scheduled annually.

## Scope of the Policy

This policy protects the personal data of data subjects, which covers the following groups of individuals:

### 1. Customers of the Company and subsidiaries

- **Individual Customers** refer to former and current customers of the Company and subsidiaries, who are natural persons, including applicants for insurance and policyholders.
- **Business Entity Customers** refer to directors, shareholders, beneficial owners, employees, guarantors, collateral providers, and legal representatives of former and current business entity customers, including other natural persons authorized to act on behalf of business entity customers.

### 2. Individuals who are not customers of the Company and subsidiaries

These individuals include natural persons who do not have products or services with the Company and subsidiaries but may be required to collect, use, or disclose personal data,

such as investors, individuals who have made payments to or received money from customers of the Company and subsidiaries, individuals who have visited the website or application of the Company and subsidiaries or used services at the branches or offices of the Company and subsidiaries, guarantors or collateral providers, beneficial owners, directors or legal representatives of companies using the services of the Company and subsidiaries, debtors or tenants of customers of the Company and subsidiaries, professional advisors, including directors, investors, and shareholders of the Company and subsidiaries and the legal representatives of such individuals, lessors, buyers of property from the Company and subsidiaries, and any individuals involved in conducting business with the Company and subsidiaries or customers of the Company and subsidiaries and job applicants applying to work for the Company and subsidiaries.

## Definitions

The Company	means	Ngernturbo Public Company Limited
Subsidiaries	means	Ngernturbo Insurance Broker Company Limited, Ngernturbo Pay Later Company Limited, NTB Company Limited and Ngernturbo Development Center Company Limited
Personal Data	means	Information related to a person that enables identification of such person, whether directly or indirectly, but not including the information of deceased persons in particular such as name, surname, identification number, telephone number, email, address, date of birth, occupation, photograph, etc., according to the Personal Data Protection Act B.E. 2562 (2019)
Sensitive Data	means	Personal data concerning race, ethnicity, political opinions, beliefs in religion or philosophy, sexual

		behavior, criminal records, health information, disability, trade union information, genetic data, biometric data, or any other data that similarly affects the data subject as defined by the Personal Data Protection Committee
Data Processing	means	Any operation performed on personal data, whether by automated means or not, such as collecting, recording, organizing, structuring, keeping, updating, changing, recovering, using, disclosing, forwarding, publishing, transferring, merging, deleting, destroying
Data Controller	means	a person or juristic person who has the authority to make decisions about the collection, use, or disclosure of personal data, and has appropriate security measures, and regularly reviews them
Data Processor	means	a person or juristic person that collects, uses, discloses personal data in accordance with the instructions or on behalf of the Data Controller
Data Protection Officer (DPO)	means	a person appointed by the Company for coordination, inspection, advice, and supervision of data security

### **Personal Data Protection Policy Consent from Data Subjects**

Ngernturbo Public Company Limited and subsidiaries will not collect, use, or disclose personal data without obtaining consent from the data subject, with policies regarding obtaining consent from the data subject as follows:

## **1. Request for Consent**

- Consent will be requested explicitly, which may be in writing or through an electronic system, unless there is a legal exception that authorizes the Company and subsidiaries to collect, use, or disclose personal data without consent.
- The Company and subsidiaries will inform the purposes of the collection, use, or disclosure of personal data.
- The request for consent will be clearly separated from other content, presented in a format or text that is easy to understand, using simple language that is not misleading or causes the data subject to misunderstand the stated purposes.
- In requesting consent, the Company and subsidiaries will prioritize the data subject's freedom to give consent to the fullest extent. Therefore, in entering into contracts and providing any services, there will be no conditions for consent that are unnecessary or unrelated to entering into the contract and providing such services, unless it is necessary to fulfill a contract to which the data subject is a party, or for processing a request from the data subject prior to entering into a contract, or in cases where the law provides an exemption.

## **2. Withdrawal of Consent**

- Data subjects can withdraw consent at any time and can withdraw consent as easily as granting consent, unless there are legal restrictions or contractual obligations that benefit the data subject limiting the right to withdraw consent. However, the withdrawal of consent by the data subject does not affect the collection, use, or disclosure of personal data for which the data subject has previously given lawful consent.
- If the withdrawal of consent impacts the data subject in any way, the Company and subsidiaries will notify the data subject of the consequences of such withdrawal.

## **Purposes of Collecting, Using, and Disclosing Personal Data**

The collection of customers' personal data is for the performance of the contract that the Company and subsidiaries have with customers, as well as for pursuing the operational objectives of the Company and subsidiaries, including for enhancing the quality and efficiency of services.

The collection of personal data will be retained only for the period necessary to achieve these purposes. If there is a subsequent change in the purpose of collecting personal data, the Company and subsidiaries will notify and obtain consent before collecting, using, or disclosing such data and will not undertake any actions that differ from the stated purposes of data collection, unless the new purpose has been communicated and consent has been obtained, or unless it is required by law.

### **Collection, Use, or Disclosure of Personal Data**

The Company and subsidiaries will collect, use, or disclose personal data only when necessary for legitimate purposes or when there is a legal basis for collecting and using or disclosing personal data, which includes the collection, use, or disclosure of personal data for the performance of legal obligations, for the fulfillment of contracts that the data subject has made with the Company and subsidiaries, for legitimate interests, for any actions based on the data subject's consent, and/or under other legal bases.

The Company and subsidiaries have established a policy for the collection, use, or disclosure of personal data as follows:

1. Before or at the time of collecting personal data, details will be communicated to the data subject as follows:
  - The purpose of collecting personal data for use or disclosure, including purposes for which the law authorizes collection without the data subject's consent.
  - Notification of cases where the data subject is required to provide personal data to comply with the law or as a necessity for entering into a contract, along with the potential consequences of not providing such data.
  - The collected personal data will have a retention period. If the retention period cannot be clearly determined, an expected duration may be specified based on standard collection practices.
  - Types of a person or entities to whom the collected personal data

- Information about the Company and subsidiaries, contact details, and how to contact the Data Protection Officer.
  - Rights of the data subject.
- 2. The Company and subsidiaries will not collect personal data without the data subject's consent except for purposes specified in Section 24 of the Personal Data Protection Act B.E. 2562 (2019).
- 3. The Company and subsidiaries will not collect personal data from sources other than the data subject directly, except when:
  - The data subject has been notified of the collection of personal data from other sources within 30 days from the date of collection and consent has been obtained.
  - The collected personal data is exempt from requiring consent under Section 24 or Section 26 of the Personal Data Protection Act B.E. 2562 (2019).
- 4. The Company and subsidiaries will collect, use, or disclose personal data only in accordance with the purposes notified to the data subject before or at the time of collection. In the event of a change in the purpose of collection, use, or disclosure, the company and subsidiaries will inform the data subject of the new purpose and relevant details, and consent must be obtained before proceeding with the collection, use, or disclosure.
- 5. The Company and subsidiaries will not collect sensitive data, such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data (e.g., facial recognition data, fingerprint data, iris scan data, voice recognition data), or other data that similarly impacts the data subject as determined by the Personal Data Protection Committee, without explicit consent from the data subject. The only exception is when the collection is exempt from requiring consent under Section 26 of the Personal Data Protection Act B.E. 2562 (2019).
- 6. In cases where personal data is transferred or sent to recipients in other countries as part of the regular business operations of the Company and subsidiaries, such as transferring or

storing personal data on servers/clouds abroad, if the destination country does not have adequate data protection standards, the Company and subsidiaries will ensure that the transfer or sending of personal data complies with legal requirements. Additionally, necessary and appropriate measures for personal data protection will be implemented in line with confidentiality standards, such as entering into confidentiality agreements with the data recipients in the respective country.

## **Rights of the Data Subject**

Data subjects can exercise their various rights under the provisions of the law and policies currently in place or as they may be amended in the future, as well as the regulations set by the Company and subsidiaries. In the case where the data subject is under 20 years of age or has limited legal capacity under the law, the rights can be exercised by their parents, guardians, or legal representatives acting on their behalf.

1. **Right to Withdraw Consent:** If consent has been given to the Company and subsidiaries to collect, use, and/or disclose personal data (whether this consent was given before or after the Personal Data Protection Act became effective), the data subject has the right to withdraw their consent at any time during the period the personal data is held by the Company and subsidiaries, unless there are legal restrictions on that right or contractual obligations that benefit the data subject.

In the event of withdrawal of consent, the Company and subsidiaries will inform the data subject of the potential impact on the use of products and/or services.

2. **Right to Access Data:** The data subject has the right to access their personal data held by the Company and subsidiaries, to request a copy of such data, and to request disclosure of how the Company and subsidiaries obtained their personal data.
3. **Right to Data Portability:** The data subject has the right to receive their personal data in cases where the company and subsidiaries have formatted the data to be readable or usable by automated tools or devices, and where the data can be used or disclosed by automated means. Additionally, the data subject also has the right to request the



Company and subsidiaries to send or transfer such personal data to another data controller where technically feasible, and the right to receive personal data that the Company and subsidiaries sent or transferred to another data controller directly, unless it is technically impossible to do so.

This personal data must have consent from the data subject for collecting, using, and/or disclosing, or it must be personal data that is necessary to collect, use, and/or disclose so that the data subject can use the Company's and subsidiaries' products and/or services, where the data subject is a party to a contract, or for processing requests prior to using such products and/or services, or other personal data as specified by the competent authority under the law.

4. **Right to Object:** The data subject has the right to object to the collection, use, and/or disclosure of personal data at any time in cases where the collection, use, and/or disclosure of personal data are carried out for operations necessary under the legitimate interests of the Company and subsidiaries, or of other individuals or legal entities, within the reasonably foreseeable scope, or for public interest task. If the data subject objects, the Company and subsidiaries will continue to collect, use, and/or disclose personal data only if they can demonstrate legal significant reasons that outweigh the fundamental rights of the data subject establishing legal claims, complying with the law, or defending legal proceedings, as applicable.

Additionally, the data subject also has the right to object to the collection, use, and/or disclosure of personal data made for marketing purposes or for purposes related to scientific, historical, or statistical research.

5. **Right to Erasure or Destruction of Data:** The data subject has the right to request the deletion or destruction of personal data, or to make the personal data anonymized, if the data subject believes that the personal data was collected, used, and/or disclosed unlawfully, or believes that the Company and subsidiaries no longer need to retain it for the purposes related to this policy, or when the data subject has exercised their right to withdraw consent or object as previously mentioned.

6. **Right to Restrict Processing:** The data subject has the right to request the temporary restriction of the use of personal data in cases where the Company and subsidiaries are investigating a request to exercise the right to rectify personal data or object, or in any other case where the Company and subsidiaries no longer need to retain the personal data and must delete or destroy personal data according to the relevant laws, but the data subject requests restriction of use instead.
7. **Right to Rectification:** The data subject has the right to request the rectification of personal data to be accurate, up-to-date, complete, and not misleading.
8. **Right to Lodge a Complaint:** The data subject has the right to file a complaint with the relevant legal authority if the data subject believes that the collection, use, and/or disclosure of their personal data is an act that violates or fails to comply with the relevant laws.

The exercise of the aforementioned rights may be restricted under relevant laws, and there may be certain circumstances where the Company and subsidiaries may refuse or be unable to fulfill the data subject's request to exercise such rights. This may include situations where compliance with the law or court orders is required, for public interest reasons, or where the exercise of rights may infringe upon the rights or freedoms of others. If the Company and subsidiaries refuse a request, they must notify the data subject of the reason for the refusal. If the data subject has a request to exercise the aforementioned rights, the reasons for such refusal will be communicated to the data subject.

In cases where the data subject submits a request to exercise the rights mentioned above, and the request cannot be refused, the company and subsidiaries will process the request within 30 days from the date of receipt of the request.

### **Measures in Case of Personal Data Breach**

When a personal data breach occurs, anyone who discovers it must immediately notify the Data Protection Officer (DPO). The Data Protection Officer is required to report the breach to the Office

of the Personal Data Protection Committee within 72 hours from the time the incident is known, if the breach poses a risk to the rights and freedoms of individuals.

However, in cases the breach poses a high risk to the rights and freedoms of individuals, the Data Protection Officer must also inform the data subjects of the incident and provide remediation guidelines.

### **Management of Data Storage and Data Destruction Upon Expiration**

The Company and subsidiaries will retain personal data for a certain duration while the data subject is a customer or has a relationship with the Company and subsidiaries, or for the period required to achieve the purposes outlined in this policy. Further retention may be required or permitted by law (e.g., Financial Institutions Business Law, Securities and Exchange Act, Anti-Money Laundering Law, Counter-Terrorism and Proliferation Financing Law, Accounting Law, Revenue Code, Labor Law, and other laws that the Company and subsidiaries must comply with, both in Thailand and abroad). Such data will be stored for the purpose of verification or dispute resolution within the statute of limitations as prescribed by law, for a period not exceeding 10 years.

In addition, the Company and subsidiaries may need to retain records from CCTV cameras at the head office, branches, or service channels, and/or voice recordings of services provided through the Call Center to prevent fraud and maintain security, as well as to investigate suspicious transactions reported by the data subject or related individuals to the Company and subsidiaries.

Upon the expiration of the necessary retention period or when the data is no longer required, the Company and subsidiaries will delete or destroy personal data, or render it anonymous based on the methods and procedures for deleting or destroying data from the "Policy and Guidelines on the Supervision of the Use of Information and Documents."