

# **Personal Data Protection Policy**

## **Thaifoods Group Public Company Limited**

### **1. Principles and Rationale**

Thaifoods Group Public Company Limited (the "Company") places importance on the personal data protection and the duties to be complied with according to the Personal Data Protection Act, B.E. 2562 ("Personal Data Protection Act"), which is the law to specify the rights and duties of the Company in collecting, using, or disclosing the personal data of the persons related to the Company's operation. Thus, the Personal Data Protection Policy to be enforced in the organization (the "Policy") is prepared to direct the approaches and methods in which the Company and the employees, as the personal data controller, can manage the personal data of the customers, suppliers, workers, and third parties. This shall be enforced for all personal data processed by the Company in all activities. This shall also be enforced with the directors, executives, and employees of the Company at all levels.

### **2. Definitions**

<b>“Data Subject”</b>	means	An ordinary person who is the owner of the personal data according to the Personal Data Protection Act.
<b>“Personal Data”</b>	means	Data related to a person which can identify such person whether directly or indirectly but not include the data of the deceased particularly.
<b>“Data Processing”</b>	means	The collection, use, or disclosure of personal data according to the Personal Data Protection Act.

### **3. Personal Data Collection**

#### **3.1 Personal data possibly collected by the Company**

The Company collects personal data in various areas, considering the data usage objectives for the normal operation of the Company which may include:

- General data, such as name, surname, telephone number, email, address, ID number (such as an ID card, passport, driving license, or tax payer ID), birthdate, race, nationality, weight, height, and a photo
- Occupation data, education data, work experience and employment data, work assessment data, criminal records, medical records, and a family profile
- History of contacts for entering transactions or contracts with the Company
- Account number, salary, financial status, tax payment, credit card number, car registration number
- Data related to the computer equipment and program that are used by the data subject in accessing the tasks, including the IP address of the browser, language, operational system, application, and history of website visits, as well as the data related to Cookies.
- Visual record in the CCTV system

### **3.2 Channels for Data Collection**

The Company may collect the personal data of the subject both directly and indirectly, including through the following channels:

- The data that is given directly by the subject or the representative of the data subject to the Company or the Company's representative directly.
- The data that the Company received from the subsidiaries, affiliates, or business partners of the Company legitimately.
- The data that the Company receives from any other data sources that are reliable, such as public agencies, banks.
- The data that the Company receives from general public data sources in a legal manner.

### **4. Period of Personal Data Storage**

The Company will collect the personal data in the period as necessary for the processing of personal data within the scope and objectives related to the Company's business operation. After that, the Company will destroy such data in a standardized manner, except in the case that the Company is legally responsible to store such data or for the protection of the Company's rights in the period as specified by law.

### **5. Objectives in the Use and Disclosure of Data**

#### **5.1 Objectives in the Use and Disclosure of data**

The Company will use and disclose the personal data for the objectives in the Company's normal business operation, possibly including for:

- Entering into the contract or performing the duties following the contract between the Company and the personal data subject.
- Performing the operation for which the Company is needed for a legitimate interest, considering the fundamental rights of the personal data.
- Presenting the data about products and services, including the improvement, development, and remaining quality of products and services for which the data subject is the contract party with the Company.
- Communicating, such as sending the notification, and responding when contacted by the data subject.
- Offering new products and services. In the event that the data subject does not intend to be contacted about the marketing activities or sales activities, the data subject can notify the Company of the demand via the channel specified by the Company.
- Complying with the objectives in recruiting and selecting the human resources.
- Identifying the contact persons for the Company and for the objectives in security protection.
- Performing the duties of the Company under relevant laws.

## **5.2 Persons possibly be Disclosed of Data**

The Company may disclose the personal data of the subject for its legitimate interests. The personal data of the subject can be disclosed or transferred to the organization, public agencies, or third parties, including:

- Affiliates or subsidiaries of the Company
- Third-party service providers, such as service providers of data collection or analysis, human resource service providers
- Government agencies that supervise the Company's business operations
- Advisors such as financial advisors or legal advisors
- Other data controllers requested by the data subject for the Company to send or transfer the data to

The Company will take appropriate actions to protect against/prevent loss, unauthorized access to the data, use, modification, disclosure, and illegal use of the data by the persons to whom the Company discloses the personal data, as mentioned above.

In the case that the Company has to reveal the personal data to the recipient abroad, the Company will disclose the personal data only in cases permitted by the personal data protection law and other relevant laws.

## **6. Data Safety**

The Company has a standard data security system with classification and determination of the level of confidentiality, data management methods, rights of data access, security in the physical and corporate environment, and operational performance related to the processing of the information and communication equipment. This is to ensure that the data processed by the Company is safe and to prevent personal data violations.

## **7. Rights of the data subject**

7.1 The rights of the data subject are as follows:

- (1) Right to be notified in case the Company collects personal data
- (2) Right to access relevant one's own personal data, request a personal copy, and request disclosure of the acquisition in case of not receiving prior consent from the data subject
- (3) Right to receive or request the Company to send or transfer personal data to other personal data controllers when being able to do so by automatic methods
- (4) Right to oppose the collection, use, or disclosure of relevant personal data
- (5) Right to request the Company to delete, destroy, or make the personal data of the data subject non-identifiable
- (6) Right to request the Company to suspend the use of one's own relevant personal data
- (7) Right to request the Company to operate one's own relevant personal data correctly, be updated, be completed, and not cause a misunderstanding

## **8. Contact**

The Company provides the personal data protection officers to be responsible for giving advice and coordinating with the personal data subject on the Company's compliance with the Personal Data Protection Act. The contact details are as follows:

Personal data protection officers

Contact channel: Compliance Division

Email: [dpo@tfg.co.th](mailto:dpo@tfg.co.th)

## **9. Policy Review and Improvement**

The Company will determine to review this policy regularly, at least once a year or when there is a significant change in terms of laws, relevant personnel, and nature of Company's business operation. This shall be in compliance with the laws and practical approaches of The Office of the Personal Data Protection Committee.

Announcement on January 1st, 2026