



PERSONAL DATA PROTECTION POLICY

Revision: 01

Effective Date: 25/03/2026

Approved by: **Mr. Akapol Dilokwattanakul**

Title: Vice President

CHANGE TRACKING

Effective Date	Revision	Description of Change



PERSONAL DATA PROTECTION POLICY

MỤC LỤC

I. PURPOSE	3
II. SCOPE OF APPLICATION.....	3
III. REFERENCE DOCUMENTS.....	3
IV. DEFINITION AND ABBREVIATIONS	3
V. CONTENT.....	5
5.1 Purpose of Processing Personal Data.....	5
5.1.1 For Employees & Job Applicants	5
5.1.2 For Partners and Customers	5
5.2 Personal Data Processing Activities	6
5.2.1 Methods of Collecting Personal Data	6
5.2.2 Storage, Deletion, and Destruction of Personal Data	6
5.2.3 Transfer/Sharing	7
5.3 Organizations and Individuals Involved in Personal Data Processing.....	7
5.4 Start and End Time of Personal Data Processing	7
5.5 Possible Unintended Consequences or Damages	7
5.6 Rights and Obligations of Data Subjects	8
5.6.1 Rights of Data Subjects.....	8
5.6.2 Obligations of Data Subjects	9
5.7 Company's Commitment to Personal Data Processing	9
5.8 Contact Information for Personal Data Processing.....	9
5.9 Activity: "Notification and Consent of Data Subjects"	10
5.10 Handling Violations	10



PERSONAL DATA PROTECTION POLICY

I. PURPOSE

This document is established to protect personal data and the responsibility of organizations and individuals involved in personal data protection: a) The Personal Data Protection Policy (hereinafter referred to as the “Policy”) represents **Pataya Food Industries Viet Nam Limited (PFV or the company)**’s commitment to respecting and protecting the personal data of each individual. This Policy covers all personal data collected and used by PFV. b) Once accepted by employees, applicants, partners, and customers, this Policy constitutes an agreement between the personal data subject and the Company in the process of establishing, maintaining, and developing relationships and transactions, upon the subject’s consent. c) This Policy demonstrates the emphasis on and respect for privacy, confidentiality, and security of personal data, ensuring compliance with data protection laws.

II. SCOPE OF APPLICATION

- Applicable to applicants submitting job applications; employees and consultants of the Company.
- Applicable to the Company’s partners and customers.

III. REFERENCE DOCUMENTS

- Law No. 91/2025/QH15 on Personal Data Protection
- Decree No. 356/2025/NĐ-CP on Personal Data Protection

IV. DEFINITIONS AND ABBREVIATIONS

- Company or PFV: **Pataya Food Industries (Viet Nam) Limited**
- Provider: Employees of the Company, job applicants, partners, and customers who provide personal data to the Company.
- Partner: Includes suppliers, organizations/individuals providing goods or services to the Company, and business cooperation partners.
- Personal Data: Personal data refers to information in the form of symbols, letters, numbers, images, sounds, or similar forms in electronic environments associated with a specific individual or helping to identify a specific individual. Personal data includes basic personal data and sensitive personal data.
- Basic Personal Data includes: a) Full name, middle name, birth name, and other names (if any); b) Date of birth, date of death, or date of disappearance; c) Gender; d) Place of birth, place of birth registration, permanent residence, temporary residence, current address, hometown, and contact address;



PERSONAL DATA PROTECTION POLICY

- a) Nationality;
- b) Personal image;
- c) Phone number, personal identification number, citizen identification number, identity card number, passport number, driver's license number, vehicle license plate number;
- d) Marital status;
- e) Information on family relationships (parents, children, spouse); information on dependents registered with state agencies such as tax authorities and social insurance;
- f) Information on personal account numbers; social insurance book number, personal income tax code;
- g) Personal email address information;
- h) Other information associated with a specific individual or helping to identify a specific individual not included in the definition of "sensitive personal data" below.

Sensitive personal data refers to personal data associated with an individual's privacy, which, if infringed, will directly affect the rights and legitimate interests of the individual, including: a) Data revealing racial origin, ethnic origin; b) Political, religious, or belief-related opinions; c) Information on private life, personal secrets, family secrets; d) Health status; e) Biometric data, genetic characteristics; f) Data revealing sexual life, sexual orientation of the individual; g) Criminal or legal violation data collected and stored by law enforcement agencies; h) Location of the individual determined through positioning services; i) Information on username and password for accessing the individual's electronic identification account; images of identity cards, citizen identification cards, or identity documents; j) Username and password for accessing bank accounts; bank card information, data on bank account transaction history; financial, credit information and other information on financial activities, securities, insurance transactions of customers at credit institutions, foreign bank branches, payment intermediary service providers, securities, insurance, and other authorized organizations; k) Data tracking behavior and activities using telecommunications services, social networks, online media services, and other services in cyberspace; l) Other personal data required by law to be kept confidential or subject to strict security measures.

Personal data protection: activities to prevent, detect, stop, and handle violations related to personal data in accordance with the law.

Data subject: the individual to whom the personal data refers.

Personal data processing: one or more activities impacting personal data, such as collecting, recording, analyzing, verifying, storing, editing, disclosing, combining, accessing, retrieving, recovering, encrypting, decrypting, copying, sharing, transmitting, providing, transferring, deleting, destroying personal data, or other related actions.

Consent of the data subject: the clear, voluntary, affirmative expression of allowing the processing of the data subject's personal data.



PERSONAL DATA PROTECTION POLICY

Personal data controller: the organization or individual deciding the purpose and means of processing personal data.

Personal data processor: the organization or individual processing personal data on behalf of the controller, through a contract or agreement with the controller.

Personal data controller and processor: the organization or individual simultaneously deciding the purpose, means, and directly processing personal data.

Third party: organizations or individuals other than the data subject, personal data controller, personal data processor, and personal data controller and processor, who are authorized to process personal data.

V. CONTENT

5.1 Purpose of Processing Personal Data

5.1.1 For Employees & Job Applicants

- Verify applicants and employees.
- Contact/provide/send messages, correspondence, letters, or other notifications to applicants or other relevant parties.
- Establish, perform, and terminate employment relationships.
- Serve human resources management and administration activities such as HR management, payroll, insurance contributions, performance evaluation, etc.
- Provide employees' personal data to third parties for processing, such as salary transfers, tax declarations, periodic health checks, training, purchasing health insurance and unemployment insurance, participation in bidding, etc.
- Provide data to competent state authorities and/or other cases in accordance with legal requirements (e.g., issuing invoices, personal income tax documents, etc.).
- Carry out other purposes related to the Company's business activities that the Company deems appropriate from time to time.

5.1.2 For Partners and Customers

- Perform contracts and agreements entered into.
- Receive and resolve complaints, improve the quality of goods, products, and services.
- Contact partners to exchange information, provide documents or other materials related to transactions and the provision of products/services.
- Evaluate any proposals related to rights, interests, or obligations under contracts between partners and the Company.
- Serve other purposes related to the Company's business activities that the Company deems appropriate from time to time.
- For any other purposes required or permitted by laws, regulations, guidelines, and/or requests of competent state authorities.

5.2 Personal Data Processing Activities the Company will store methods of obtaining consent from data subjects regarding the identification of consent, the time, and the content agreed upon, including: a) In writing; b) By recorded phone call; c) Consent syntax via text message; d) Via email, on websites, platforms, applications with technical consent settings; e) By other appropriate methods that can be printed or copied in writing, including electronic or verifiable formats.



PERSONAL DATA PROTECTION POLICY

5.2.1 Methods of Collecting Personal Data

a) The Company may collect personal data of “Data Subjects” from one or more of the following sources, including but not limited to:

- Directly from the Provider: collected during interactions, work, interviews, face-to-face meetings, contract execution, etc., and provided by the Provider.
- From the Company’s websites: collected when the Provider accesses any Company website or uses any features/resources available on or through the website.
- From communications with the Provider: collected when the Provider and the Company interact via email, phone calls, electronic communications, or other means (including but not limited to surveys, investigations, or data collection conducted by the Company).
- From competent state authorities: collected from government agencies in Vietnam.
- From public sources: collected from publicly available sources such as phone directories, advertisements/flyers, publicly available online information, posted information at workplaces, etc.
- From suppliers, service providers, partners, affiliates, and third parties related to the Company’s business activities.
- From other sources where the Provider consents to share/provide personal data, or sources required or permitted by law.

b) When providing another person’s personal data to the Company, the Provider warrants, guarantees, and is responsible to the Company that:

- The information provided to the Company is complete, and any changes or errors in the personal data provided will be promptly notified to the Company.
- The individual (data subject) has been informed and has given lawful consent/approval or valid authorization for: (i) providing personal data to the Company, (ii) allowing the Company to process personal data for the purposes stated in this Policy. The Provider agrees that the Company is not responsible for verifying the legality or validity of such consent, approval, or authorization, and the responsibility for storing proof lies with the Provider. The Company is exempt from liability and has the right to claim compensation for damages and costs arising when the Provider fails to comply with these commitments.
- Other warranties to the Company regarding personal data processing as stated in the Personal Data Commitment document signed between the Provider and the Company from time to time.

5.2.2 Storage, Deletion, and Destruction of Personal Data

- Personal data is stored by the Company in Vietnam through its database systems. The Company takes reasonable measures within its capacity to protect the personal data of data subjects and commits not to sell, lease, or illegally trade the personal data of data subjects.
- The Company will delete or destroy stored personal data upon receiving a request from the data subject, except in cases where the law does not permit deletion. Accordingly, the Company will delete personal data as follows:
- Upon receiving a request to withdraw consent for processing personal data, restrict processing, or object to processing in accordance with the proper procedures of the data subject, the personal data controller or controller-cum-processor must respond within 02 working days, provide full information to the data subject on the procedure to cease processing, and implement within 15 days.



PERSONAL DATA PROTECTION POLICY

- Upon receiving a request to delete personal data in accordance with the proper procedures of the data subject, the personal data controller or controller-cum-processor must respond within 02 working days, provide full information to the data subject on the procedure, and implement within 20 days.
- Upon receiving a request to view, edit, or correct personal data, or to provide personal data in accordance with the proper procedures of the data subject, the personal data controller or controller-cum-processor must respond within 02 working days, provide full information to the data subject on the procedure, and implement within 10 days. • Depending on the method of data storage at each point in time, the Company will delete the data subject's personal data by deleting electronic files or shredding paper documents.
- In the absence of a deletion request from the data subject, the Company may, at its discretion, continue to store and protect personal data for management purposes and delete it when deemed necessary.

5.2.3 Transfer/Sharing

- The transfer/sharing of data to relevant parties has been described in Section 5.1.
- The transfer/sharing of data will be carried out in accordance with the procedures, methods, and current legal regulations.

5.3 Organizations and Individuals Involved in Personal Data Processing

5.3.1 Depending on the circumstances, the Company may act as the personal data controller or as the controller-cum-processor.

5.3.2 Within the scope permitted by law, the data subject understands that the Company may share personal data for the purposes stated in this Policy with the following organizations and individuals involved in personal data processing:

- Employees of the Company, subsidiaries, and affiliates of the Company.
- Organizations and individuals that are partners or contractors of the Company.
- Any individual or organization acting as a representative or authorized party of the data subject.
- Consulting firms, auditors, lawyers, notaries, and other parties acting on behalf of the Company.
- Competent state authorities as required by law.
- Organizations and individuals involved in personal data processing are obliged to maintain confidentiality of personal data in accordance with this Policy and applicable laws.

5.4 Start and End Time of Personal Data Processing

- The start time of personal data processing is when the Company lawfully begins to receive and/or collect personal data until the processing purpose has been fulfilled.
- The Company may be required to store personal data even after contracts between the parties have ended, in order to fulfill obligations under the law and/or at the request of competent state authorities.

5.5 Possible Unintended Consequences or Damages

5.5.1 The Company always values and strives to ensure the confidentiality and security of the data subject's personal data. The Company uses various measures to protect and prevent unauthorized access, use, or sharing of personal data. However, the Company cannot guarantee absolute confidentiality of personal data in certain cases such as:

- Hardware or software errors during data processing causing loss of personal data.



PERSONAL DATA PROTECTION POLICY

- Security vulnerabilities beyond the Company's control, or system attacks by individuals/organizations leading to data breaches.
- Data subjects disclosing their own personal data due to carelessness, fraud, or accessing websites/downloading applications containing malware.
- Other unforeseen consequences or damages caused by objective reasons.

5.5.2 Cyberspace (the internet) is not a completely secure environment, and it cannot be absolutely guaranteed that personal data shared over the internet will always remain confidential. When transmitting data via the internet, data subjects should only use secure systems to access websites, applications, or devices. Data subjects are responsible for safeguarding their authentication information for each website, application, or device securely and confidentially.

5.5.3 In the event of unintended consequences or damages, within the scope permitted by law, the Company will notify the competent authorities and relevant parties within the legally prescribed timeframe and will make efforts to mitigate and prevent damages to the best of its ability.

5.6 Rights and Obligations of Data Subjects

5.6.1 Rights of Data Subjects

a) Data subjects have the following rights:

- **Right to be informed and to consent:** Data subjects have the right to be informed and to consent or refuse consent for the processing of their personal data, except where otherwise provided by law. Through this Policy, data subjects are informed about the Company's personal data processing activities. Data subjects express consent for the Company to process their personal data by confirming consent using the Policy's confirmation form. Confirmation may be given by signing, confirming via email, or confirming via the Company's link.
- **Right to withdraw consent:** Data subjects have the right to withdraw their consent, except where otherwise provided by law.
- **Right to erasure:** Data subjects have the right to erase or request erasure of their personal data, except where otherwise provided by law.
- **Right to restrict processing:** Data subjects have the right to request restriction of processing of their personal data, except where otherwise provided by law.
- **Right of access and rectification:** Data subjects have the right to access, view, edit, or request correction of their personal data, except where otherwise provided by law.
- **Right to data portability:** Data subjects have the right to request provision of their personal data, except where otherwise provided by law.
- **Right to object:** Data subjects have the right to object to the processing of their personal data in accordance with the law.
- **Right to self-protection.**
- **Right to lodge complaints, denunciations, or initiate lawsuits.**
- **Right to claim compensation for damages.**

b) Notes when exercising data subject rights:

- Except for the right to be informed and to consent, data subjects may exercise other rights by submitting a request to the Company. Requests must include basic information such as: requester's details, specific request content (e.g., type of data to be provided, corrected, erased), reasons, and other relevant information (e.g., whether documents should be provided in electronic or paper form, delivery address, etc.).



PERSONAL DATA PROTECTION POLICY

- The Company will process legitimate and valid requests of data subjects within the timeframe required by law. However, for security purposes, the Company may require data subjects to verify their identity before processing their requests.
- If a data subject withdraws consent, requests erasure, or exercises other rights over any or all personal data, this may affect the Company's ability to provide/maintain contractual relationships with the data subject. Therefore, the rights exercised under Section 5.6.1 shall be deemed unilateral termination of any relationship between the data subject and the Company, and may result in breaches of obligations/commitments under contracts between the data subject and the Company. Accordingly, the Company shall not be liable for any resulting losses, and the Company's legal rights shall remain fully reserved.
- The Company may refuse to fulfill data subject requests in certain cases, including but not limited to: (i) The data subject fails to provide or provides insufficient documents to verify identity; or (ii) Legal provisions do not permit the Company to fulfill the data subject's request.

5.6.2 Obligations of Data Subjects

- Protect their own personal data; request relevant organizations or individuals to protect their personal data.
- Respect and protect the personal data of others.
- Provide complete and accurate personal data when consenting to personal data processing.
- Participate in promoting and disseminating skills for personal data protection.
- Comply with legal regulations on personal data protection and participate in preventing and combating violations of personal data protection regulations.

5.7 Company's Commitment to Personal Data Processing

- The Company only collects, processes, and stores personal data of employees, applicants, and partners in accordance with legal regulations and/or contracts, agreements, documents entered into, and/or for legitimate purposes consistent with the law.
- Depending on the Company's role in each specific situation as (i) Personal Data Controller, (ii) Personal Data Processor, or (iii) Personal Data Controller and Processor, the Company will exercise the corresponding rights, responsibilities, and principles of personal data processing in accordance with applicable laws.
- The Company will process and protect personal data provided by data subjects in compliance with Vietnamese law; fully adhere to this Personal Data Protection Policy and other contracts, agreements, or documents established with data subjects.
- The Company collects, stores, and uses personal information provided by data subjects for specific, clear, and lawful purposes, within the scope stated in this Personal Data Protection Policy and in compliance with Vietnamese law.
- The Company considers the personal data of Providers as private and confidential. Except for cases mentioned in this Policy, the Company will not share or disclose Providers' personal data to any other party.

5.8 Contact Information for Personal Data Processing in case Providers have any questions or concerns related to the Personal Data Protection Policy, issues regarding data subject rights, or personal data processing, please contact the Company's HR Department via email at hr_pfv@patayafood.com or directly visit the Company's office for support.



PERSONAL DATA PROTECTION POLICY

5.9 Activity: “Notification and Consent of Data Subjects” When the Company receives personal data from data subjects, they will be notified of this Policy to read and confirm through one of the following channels: The Company’s website or confirmation sent by the Company’s HR Department.

5.10 Handling Violations in reference to the Company’s Reward and Disciplinary Policy, depending on the severity of violations of the provisions in this document, violators will be subject to disciplinary measures ranging from reprimands and warnings to termination of employment.

Can Tho, date 25 month 03 year 2026

Company Representative



AKAPOL DILOKWATTANAKUL

VICE PRESIDENT