Unique Plastic Industry Company Limited ("**The Company**") recognize the importance of personal data protection in accordance with the Personal Data Protection Act B.E. 2562 (2019), including any amendments thereto (the "Personal Data Protection Law"). Accordingly, the Company has established this Personal Data Protection Policy (PDPA) to set forth the fundamental principles and general guidelines applicable to the Company's key operational activities. The scope of application of this Policy is as follows:

1. Scope of Application

(1) This Policy shall apply to the personal data of Unique Plastic Industry Public Company Limited and its subsidiaries (collectively referred to as the "Company").

(2) The Company's individual customers, including prospective customers (potential future customers), existing customers, and former customers.

(3) Employees, personnel, officers, representatives, shareholders, authorized persons, directors, contact persons, agents, and other individuals related to the Company's juristic-person customers, including prospective customers (potential future customers), existing customers, and former customers.

(4) Individuals who are not customers of the Company but who conduct transactions, engage in activities, or maintain any relationship with the Company, such as external service providers, business partners, contractual counterparties, or shareholders of the Company, as the case may be.

2. Objectives

This Personal Data Protection Policy has the following objectives:

(1) To define the roles and responsibilities of departments, management, and employees who are involved in the processing of personal data.

(2) To establish procedures and standards for security measures to ensure the protection of personal data.

(3) To prescribe guidelines for employees' practices in compliance with the Personal Data Protection Law.

(4) To enhance confidence in the security and protection of personal data among individuals, customers, business partners, service users, and other stakeholders or parties concerned with personal data.

3. **Definitions / Terms and Definitions**

Term	Meaning
The Company	Unique Plastic Industry Public Company Limited and its subsidiaries
Person	A natural person
Personal data	Information relating to a person which enables the identification of such person, whether directly or indirectly. The Company may collect, use, and/or disclose the personal data of the data subject obtained directly from the data subject (e.g., the Company's registration platforms) or obtained or accessed from other sources (e.g., the Department of Business Development, Ministry of Commerce; the Department of Provincial Administration, Ministry of Interior; the Department of Consular Affairs, Ministry of Foreign Affairs; credit information companies; the Legal Execution Department; financial institutions; professional advisors; social media; third-party online platforms; or other public sources), or through affiliated companies, service providers, business partners, government authorities, or other third parties.
Sensitive Data	Personal data that is inherently private and sensitive in nature and may pose a risk of unfair discrimination, such as data concerning race, ethnicity, political opinions, beliefs in a cult, religion or philosophy, sexual behavior, criminal records, health data, disabilities, trade union information, genetic data, biometric data, or any other data which may similarly affect the data subject, as prescribed by notifications issued by the Personal Data Protection Committee.

Term	Meaning
Data Subject	An individual who owns the personal data, excluding cases where such individual owns the data in terms of ownership or is the creator or collector of such data. The data subject shall refer only to a natural person and shall not include a "juristic person" established under law, such as a company, association, foundation, or any other organization. For the purposes hereof, data subjects include the following persons: 1. Data subjects who are sui juris, meaning: 1.1 A person who has attained the age of 20 years; or 1.2 A person who has entered into marriage upon attaining the age of 17 years; or 1.3 A person who has entered into marriage before attaining the age of 17 years with court approval; or 1.4 A minor whose legal representative has given consent for the minor to engage in commercial or other business activities, or to enter into an employment contract under a labor contract, in connection with such business operations or employment, whereby such minor shall be deemed to have the status equivalent to a person who is sui juris. In this regard, any consent given by a data subject who is sui juris may be given by such data subject personally. 2. Data subjects who are minors, meaning persons under 20 years of age who are not sui juris under Item 1. In giving any consent, consent must be obtained from the person exercising parental power who is legally authorized to act on behalf of the minor. 3. Data subjects who are quasi-incompetent persons, meaning persons whom the court has ordered to be quasi-incompetent due to physical disability, mental infirmity, habitual prodigality, habitual intoxication, or other similar causes, rendering them unable to manage their own affairs or conduct their business in

Term	Meaning
	a manner that may cause deterioration to their own property or that of their family. In giving any consent, consent must be obtained in advance from the guardian who is legally authorized to act on behalf of such quasi-incompetent person. 4. Data subjects who are incompetent persons, meaning persons whom the court has ordered to be incompetent due to mental disorder. In giving any consent, consent must be obtained in advance from the curator who is legally authorized to act on behalf of such incompetent person. In this regard, any consent obtained from a data subject that does not comply with the Personal Data Protection Law shall not be binding upon the data subject.
Data Controller	A person or juristic person who has the authority and duty to make decisions regarding the collection, use, or disclosure of personal data.
Data Processor	A natural person or a juristic person who carries out the collection, use, or disclosure of personal data in accordance with the instructions of or on behalf of the Data Controller. For the avoidance of doubt, a person or juristic person who performs such actions shall not be deemed a Data Controller.
Data Protection Officer: DPO	A person appointed by the Company to perform the duties of a Data Protection Officer in accordance with the Personal Data Protection Act B.E. 2562 (2019).
Processing of Personal Data	Any operation or set of operations performed on personal data, whether or not by automated means, including but not limited to the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data.

Term	Meaning
Other Definitions	In the event that any term is not defined in this Personal Data Protection Policy, such term shall be construed and applied in accordance with the definitions prescribed under the Personal Data Protection Act B.E. 2562 (2019).

4. Personal Data Protection

The Company places significant importance on and emphasizes the protection of personal data, recognizing that the processing of personal data within the Company must be carried out in accordance with the following principles:

(1) Lawfulness, Fairness, and Transparency: The Company shall process personal data only where there is a lawful basis supporting such processing, and shall clearly define the methods for collecting and using personal data.

(2) Purpose Limitation: The Company shall process personal data solely for the purposes specified and notified at the time the personal data is collected, unless such processing is carried out for a related purpose or constitutes the performance of duties explicitly required by law.

(3) Data Minimization: The Company shall collect and use personal data only to the extent necessary to achieve the purposes of personal data processing.

(4) Accuracy: The Company shall take appropriate measures to ensure that the personal data retained is accurate, complete, and up to date, taking into account the purposes of the processing.

(5) Storage Limitation: The Company shall retain personal data only for as long as necessary, except where retention is required to comply with document retention standards or applicable governmental regulations.

(6) Integrity and Confidentiality: The Company shall implement appropriate technical and organizational measures to ensure that personal data is maintained with an appropriate level of security.

(7) Accountability:The Company shall take appropriate actions to be able to demonstrate compliance with the above principles.

5. Collection of Personal Data

The Company shall collect personal data of data subjects through various channels as follows:

5.1 Personal Data Provided Directly by the Data Subject: In general, the Company collects personal data directly from the data subject. This typically occurs when the data subject communicates with the Company in order to make inquiries, provide opinions or feedback, or submit complaints via the Company's website, applications, telephone, or email; or for the purpose of purchasing products, engaging, or using services from the Company and entering into contracts with the Company; offering products, performing work, or providing services to the Company and entering into contracts; participating in marketing activities or other activities, and similar circumstances.

5.2 Personal Data Collected Automatically by the Company: The Company may automatically collect certain technical information relating to devices, activities, and access patterns, including browsing history data of the data subject.

5.3 Personal Data Obtained from Third Parties: The Company may, from time to time, receive personal data of data subjects from third parties, such as from public sources, sources relating to the data subject's business, or commercial sources, whether the data subject has provided such personal data directly or has given consent to any person to disclose such personal data, including the Company's service providers or government authorities, as the case may be.

5.4 Conditions for the Collection of Personal Data: The collection of personal data shall be carried out under specified purposes and only to the extent necessary within the scope of such purposes or for benefits directly related to the purposes of collection. The Company shall inform the data subject prior to or at the time of collection by providing the following details:

1. The purposes of collection;
2. The retention period of personal data;
3. The categories of persons or entities to whom the personal data may be disclosed;
4. The Company's contact information or communication channels;
5. The rights of the data subject;
6. The impacts of not providing personal data in cases where the data subject fails to provide personal data as required by law or for entering into or performing a contract.

Notwithstanding the foregoing, in cases where the consent of the data subject is not required, the collection, use, and disclosure of personal data shall be carried out on the basis of the following lawful bases under Section 24 of the Personal Data Protection Act:

1. Archival / Research / Statistical Basis – where it is necessary for the achievement of purposes relating to the preparation of historical documents or archives for the public interest, or for research or statistical purposes, provided that appropriate safeguards have been implemented to protect the rights and freedoms of the data subject;
2. Vital Interests Basis – where it is necessary to prevent or suppress danger to the life, body, or health of a person;
3. Contractual Basis – where it is necessary for the performance of a contract to which the data subject is a party, or for taking steps at the request of the data subject prior to entering into such contract;
4. Public Interest Basis – where it is necessary for the performance of a task carried out in the public interest by the data controller, or for the exercise of official authority vested in the data controller;
5. Legitimate Interests Basis – where it is necessary for the legitimate interests of the data controller or of another person or juristic person other than the data controller, unless such

interests are overridden by the fundamental rights and freedoms of the data subject in relation to personal data; and

6. Legal Obligation Basis – where it is necessary for compliance with a legal obligation of the data controller.

In the case of sensitive personal data (Sensitive Data), the processing shall be carried out in accordance with the criteria prescribed under Section 26 of the Personal Data Protection Act, which requires explicit consent, unless an exemption is provided by law, as follows:

1. Vital interests basis: where it is necessary to prevent or suppress danger to the life, body, or health of a person, and the data subject is incapable of giving consent.
2. Vital interests in emergency situations: where there is a necessity to use sensitive personal data, such as blood type or health data, in cases where the data subject is unable to give consent, for example, where the data subject has suffered an accident. In this regard, where consent can be obtained, such consent should be obtained in advance, in accordance with Section 24 for general personal data and Section 26 for sensitive personal data.
3. Legitimate activities of non-profit organizations: where the processing is carried out in the course of legitimate activities of a foundation, association, or any other non-profit organization, with appropriate safeguards in place.
4. Publicly disclosed data with explicit consent: where the sensitive personal data has been manifestly made public by the data subject with explicit consent.
5. Legal claims basis: where it is necessary for the establishment of legal claims, compliance with legal claims, the exercise of legal claims, or the defense of legal claims.
6. Legal compliance in specific fields: where it is necessary to comply with the law specifically relating to preventive medicine or occupational medicine, the assessment of an employee's working capacity, medical diagnosis, the provision of health or social care services, medical treatment, health management, or systems and the use of social welfare services, public interest in the area of public health, labor protection, social security, national health security, welfare relating to medical treatment of persons entitled under the law, protection of victims

of motor vehicle accidents, or social protection, as well as scientific, historical, or statistical research, or other important public interests.

5.5 Collection of Personal Data of Persons with Legal Incapacity

5.5.1 In the case where the data subject is a minor, meaning a person under twenty (20) years of age and not having attained legal capacity pursuant to Clause 3, any consent given in this regard shall require the consent of the person exercising parental power or the legal guardian who has the lawful authority to act on behalf of such minor.

5.5.2 In the case where the data subject is a quasi-incompetent person, meaning a person who has been adjudged by the court to be a quasi-incompetent person due to physical disability, mental infirmity, unsoundness of mind, habitual reckless or extravagant behavior, addiction to intoxicants, or any other similar causes, to the extent that such person is unable to manage his or her own affairs or may conduct affairs in a manner that could cause detriment to his or her own property or that of his or her family, any consent given in this regard shall require the prior consent of the curator who has the lawful authority to act on behalf of such quasi-incompetent person.

5.5.3 In the case where the data subject is an incompetent person, meaning a person who has been adjudged by the court to be an incompetent person due to insanity, any consent given in this regard shall require the prior consent of the guardian who has the lawful authority to act on behalf of such incompetent person.

Notwithstanding the foregoing, any consent obtained from a data subject that is not in compliance with the Personal Data Protection Law shall not be binding upon the data subject.

5.6 Collection of Sensitive Personal Data

The Company shall not collect sensitive personal data unless it is necessary to do so and explicit consent has been obtained from the data subject, except in cases where the law permits the collection of such data without obtaining consent, as specified in Clause 5.4

5.7 Collection of Third-Party Personal Data

In the event that the data subject provides the Company with personal data of a third party, such as emergency contact persons or reference persons, including but not limited to names, surnames, addresses, telephone numbers, family income, and other personal or contact information for emergency contact purposes, application forms, or transactions conducted by the data subject with the Company, the Company shall require the data subject to certify that such data has been lawfully obtained. The data subject shall also inform such third parties of this Personal Data Protection Policy and/or obtain consent from such third parties, as applicable.

5.8 Collection of Cookie Usage Data

The Company may collect and use cookies in order to store information relating to website usage, which shall be recorded on the computer devices and/or communication devices used by the data subject.

Cookies shall not cause any harm to the data subject's computer devices and/or communication devices. In this regard, the personal data of the data subject may be collected to enhance the online service experience by remembering language preferences, customizing usage settings according to the data subject's preferences, verifying individual characteristics, security information, and services of interest to the data subject. Cookies may also be used to measure the volume of access to online services.

The Company may adjust content based on the data subject's usage by considering past and current browsing behavior and may also use such information for advertising or public relations purposes. The data subject may find additional details in the Company's "Cookie Policy."

5.9 Collection of CCTV Data

The Company collects data from closed-circuit television (CCTV) systems for the purpose of protecting the health and personal safety of data subjects, including their property, as well as for safeguarding the Company's buildings, facilities, and assets from damage, obstruction, destruction, or other criminal acts, and for other related purposes. Such collection shall be carried out without obtaining consent from the data subject, based on the lawful basis of legitimate interest.

6. Retention and Retention Period of Personal Data

The Company shall retain the personal data of data subjects as follows:

1. Personal data shall be stored in documentary form and/or in electronic form.

2. Personal data shall be stored in locations with restricted access, including on servers and/or on online databases (Cloud Storage) provided by service providers within the Company's group.

The Company shall retain personal data of data subjects only for as long as necessary, taking into account the necessity and purposes for which the Company is required to collect, use, and process such personal data, including compliance with applicable laws.

The criteria used to determine the retention period include the duration during which the Company maintains a relationship with the data subject. The Company may continue to retain such personal data for the period necessary to comply with applicable laws or statutory limitation periods, for the establishment of legal claims, compliance with or exercise of legal claims, defense of legal claims, or for other reasons in accordance with the Company's internal policies and regulations.

The Company shall continue to collect, use, and disclose personal data of data subjects even after the data subject has terminated the relationship with the Company, to the extent necessary in accordance with legal requirements for legitimate interests, or shall retain such data in a form that does not enable identification of an individual, whether directly or indirectly, such as anonymous data or pseudonymous data, which has been rendered non-identifiable through technical means.

The Company may retain personal data of data subjects for as long as necessary to achieve the purposes of processing personal data as specified in this Privacy Notice. In this regard, the Company shall retain personal data of data subjects for a period not exceeding ten (10) years from the date on which the data subject terminates the relationship with the Company or from the date of the last contact with the Company. However, the Company may retain such personal data for a longer period where permitted by law.

In order to comply with relevant retention periods and statutory limitation periods, the Company shall store personal data of data subjects in an appropriate form according to the type of personal data. Notwithstanding the foregoing, the Company may be required to retain personal data of data subjects even after the expiration of the statutory limitation period, for the legitimate interests of the data controller, unless such interests are outweighed by the fundamental rights and freedoms of the data subject.

The Company shall conduct periodic reviews to delete or destroy personal data, permanently anonymize personal data, or otherwise restrict the processing of personal data once the retention period has expired, where such data is no longer relevant or exceeds what is necessary for the purposes of collection, or where the Company is required to comply with a request from the data subject to delete such personal data.

Personal data for which the data subject has given consent for processing, or for which the Company is permitted to collect, store, use, and disclose based on the purposes for which consent has been obtained, shall be retained in the Company's storage systems for a period of ten (10) years from the date on which the data subject provides such consent.

7. Use or Disclosure of Personal Data

The use or disclosure of personal data shall be carried out in accordance with the purposes notified to the data subject prior to or at the time of collection, or where such use or disclosure is necessary for purposes directly related to the purposes of the collection of personal data, and shall require the consent of the data subject, unless otherwise exempted by law or where such use or disclosure is required for compliance with applicable laws.

Any person or juristic person who receives personal data as a result of the data subject's consent to disclosure, or who acts as a data processor, shall use the personal data solely for the purposes agreed to by the data subject with the Company and in accordance with the purposes notified to the Company by such person or juristic person only.

For the purpose of carrying out the objectives set out in this Privacy Notice, the personal data of the data subject may be disclosed or transmitted to internal departments of the Company and to external persons or entities, as detailed below:

Category of Data Recipients	Details
7.1 Internal to the Company	The personal data of the data subject may be disclosed or transmitted to relevant internal departments of the Company only on a need-to-know basis and strictly to the extent necessary for the specified purposes. Such persons or teams within the Company shall be granted access to the personal data of the data subject only as appropriate and necessary. • Sales personnel or other relevant personnel, with access rights assigned in accordance with their respective roles and responsibilities. • Management or the direct supervisors of the data subject who are responsible for management or decision-making relating to the data subject, or where involvement in human resources procedures is required.

Category of Data Recipients	Details
	• Support departments or teams, including Information Technology, Operations, Procurement, Human Resources, Administration, Accounting, or other departments which may be added or reduced in accordance with the Company's organizational structure from time to time.
7.2 Government Authorities, Regulatory Authorities, or Other Authorities as Prescribed by Law	The personal data of the data subject may be disclosed or transmitted to external organizations as required by law, such as the Revenue Department, the Social Security Office, the Department of Labour Protection and Welfare, the Legal Execution Department, the Ministry of Labour, or any other authority exercising powers under applicable laws.
7.3 External Organizations or Individuals	The Company may disclose the personal data of the data subject to external organizations or individuals who make inquiries for the purpose of verifying transactions relating to the data subject, and in order to provide services or procure products that are consistent with the needs of the data subject, or to the Company's business partners.

8. Transfer or Transmission of Personal Data to Foreign Countries

8.1 The Company may transmit or transfer the Data Subject's personal data to other persons, both domestically and internationally, where necessary for the performance of a contract to which the Data Subject is a party, or for the implementation of a contract between the Company and other persons or juristic persons for the benefit of the Data Subject, or for taking steps at the request of the Data Subject prior to entering into a contract, or for the prevention or suppression of danger to the life, body, or health of the Data Subject or other persons, or for compliance with applicable laws, or where necessary for the performance of a mission carried out in the public interest.

8.2 The Company may store the Data Subject's personal data on computers, servers, or cloud systems provided by third parties, and may use third-party programs or applications in the form of software-as-a-service (SaaS) or platform-as-a-service (PaaS) for the processing of the Data Subject's personal data. In this regard, the Company shall not permit any unauthorized persons to access the personal data and shall require such third parties to implement appropriate personal data security protection measures.

8.3 In the event that it is necessary to transmit or transfer the Data Subject's personal data to a foreign country, the Company shall comply with the Personal Data Protection Law and implement appropriate measures to ensure that the Data Subject's personal data is adequately protected and that the Data Subject is able to exercise his or her rights in relation to such personal data in accordance with the law. The Company shall also require the recipients of the personal data to implement appropriate data protection measures, to process such personal data only to the extent necessary, and to take actions to prevent any unauthorized or unlawful use or disclosure of the personal data by other persons.

9. Roles, Duties, and Responsibilities

The Company requires employees and relevant departments involved in the processing of personal data to give due importance to and strictly comply with the Company's personal data protection policy and practices in the collection, use, or disclosure of personal data. In this regard, the Company designates the following persons or units to supervise and monitor the Company's operations to ensure compliance with this Policy and the applicable personal data protection laws.

9.1 Personal Data Controller

Duties	Details
1.Collection, Use, and Disclosure in Compliance with the Law	The collection, use, and disclosure of personal data must be carried out on the basis of a lawful ground, with notification provided to the data subject, and personal data shall be collected directly from the data subject unless an applicable legal exception applies. This includes the duty to prepare relevant documentation to ensure that the data subject is informed and confident that, upon giving consent to the Personal Data Controller to collect such personal data, the Personal Data Controller will properly manage and protect the personal data of the data subject.
2. Facilitation of the Exercise of Data Subject Rights	The Personal Data Controller shall record requests submitted by data subjects. Where the Personal Data Controller refuses a request for the exercise of data subject rights, the reasons for such refusal shall be recorded in the record of processing activities in accordance with Section 39 of the Personal Data Protection Law.
3. Implementation of Personal Data Security Measures	Appropriate security measures shall be implemented to prevent loss, unauthorized access, use, alteration, modification, or disclosure of personal data. Such measures shall be reviewed as necessary or when technological changes occur, in order to ensure effective and appropriate data security in compliance with the minimum standards prescribed by law.
4. Measures to Prevent Unauthorized Use or Disclosure by Third Parties	Where it is necessary to provide personal data to other persons or juristic persons who are not Personal Data Controllers, such as in the case of transferring personal data to a Data Processor, measures must be implemented to prevent such persons from using or disclosing personal data without authority or in violation of the law.
5. Establishment of Monitoring Systems for	Monitoring systems shall be established to ensure the erasure or destruction of personal data once the retention period has expired, or

Duties	Details
Erasure, Destruction, or Anonymization of Personal Data	where such data is no longer relevant or exceeds what is necessary for the purposes of collection, or upon request by the data subject, or where the data subject has withdrawn consent. This shall not apply where retention is required for the exercise of freedom of expression, the establishment, compliance with, or exercise of legal claims, the defense of legal claims, or compliance with applicable laws.
6. Notification of Personal Data Breaches	In the event of a personal data breach, notification shall be made to the Office of the Personal Data Protection Commission within seventy-two (72) hours from the time the breach becomes known. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the Personal Data Controller shall also notify the data subject of the breach without undue delay, together with appropriate remedial measures.
7. Appointment of a Representative in the Kingdom of Thailand	Where the Personal Data Controller is located outside the Kingdom of Thailand, the Personal Data Controller shall appoint a representative in Thailand by written appointment. Such representative must be located in Thailand and be authorized to act on behalf of the Personal Data Controller without limitation of liability in relation to the collection, use, and disclosure of personal data in accordance with the purposes of the Personal Data Controller.
8. Duty to Maintain Records of Processing Activities (RoPA)	The Personal Data Controller shall maintain records of processing activities to enable data subjects and the Office of the Personal Data Protection Commission to conduct inspections. Such records may be maintained in written form or in electronic systems.
9. Execution of a Data Processing Agreement (DPA)	Where a Data Processor performs personal data processing on behalf of the Personal Data Controller, the Personal Data Controller shall enter into a data processing agreement with the Data Processor to govern and

Duties	Details
	control the performance of the Data Processor's duties as assigned by the Personal Data Controller.
10. Appointment of a Data Protection Officer (DPO)	Where the criteria prescribed by law require the appointment of a Data Protection Officer, the Personal Data Controller shall appoint a Data Protection Officer and notify both the data subjects and the Office of the Personal Data Protection Commission accordingly. Where an organization determines whose personal data is to be collected, what data is to be used, and for what purposes, such organization shall be deemed a Personal Data Controller, whose duties extend beyond merely preparing privacy notices.

9.2 Personal Data Processor

Duties	Details
1. Processing of Personal Data under the Instructions of the Data Controller	To carry out the collection, use, or disclosure of personal data strictly in accordance with the instructions received from the Data Controller only, unless such instructions are contrary to applicable laws or provisions relating to personal data protection.
2. Implementation of Appropriate Security Measures	To implement appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or disclosure of personal data, and to notify the Data Controller of any personal data breach incidents that may occur.
3. Maintenance of Records of Personal	To prepare and maintain records of personal data processing activities in accordance with the criteria and procedures prescribed by notifications issued by the competent committee.

Duties	Details
Data Processing Activities	
4. Execution of a Data Processing Agreement	In performing duties as a Personal Data Processor as assigned by the Data Controller, the Data Controller shall enter into a written agreement with the Personal Data Processor in order to regulate and control the performance of duties of the Personal Data Processor.

9.3 Data Protection Officer (DPO)

Duties	Details
1. Provision of Advice	To provide advice to the Data Controller or the Personal Data Processor, including their employees or contractors, in relation to personal data protection.
2. Monitoring and Audit of Operations	To monitor and examine the operations of the Data Controller or the Personal Data Processor, including their employees or contractors, with respect to the collection, use, or disclosure of personal data.
3. Coordination and Cooperation with the Office	To coordinate and cooperate with the Office in cases where issues arise concerning the collection, use, or disclosure of personal data by the Data Controller or the Personal Data Processor.
4. Confidentiality Obligation	To maintain the confidentiality of personal data that the Data Protection Officer becomes aware of or obtains in the course of performing his or her duties.

10. Security Measures for Personal Data

For the purpose of maintaining confidentiality and ensuring the security of personal data, the Company has implemented the following measures:

10.1 Access Control and Security Management: The Company defines access rights relating to the access, use, disclosure, and processing of personal data, including mechanisms for identification or verification of persons accessing or using personal data. Appropriate security measures, including review processes and assessments of the effectiveness of such security measures, are implemented in strict compliance with the Company's information security policies.

The Company shall securely retain personal data of data subjects by implementing appropriate technical measures and organizational measures to ensure the security of personal data processing and to prevent personal data breaches. The Company has established policies, rules, and criteria for personal data protection, including measures to prevent recipients of personal data from using or disclosing such data beyond the stated purposes or without lawful authority. Such policies, rules, and criteria are reviewed and updated periodically as appropriate and necessary. In addition, executives, employees, contractors, agents, advisors, and recipients of personal data from the Company are required to maintain the confidentiality of personal data in accordance with the confidentiality measures prescribed by the Company.

10.2 Cross-Border Transfer of Personal Data: In the event of transferring personal data to foreign countries, including the storage of personal data in any data systems where the data transferee or data storage service provider is located overseas, the destination country must have personal data protection measures that are equivalent to or higher than those stipulated under this Policy.

10.3 Personal Data Breach Notification and Continuous Improvement: In the event of any violation of the Company's security measures resulting in a personal data breach, the Company shall notify the Office of the Personal Data Protection Committee within 72 hours from becoming aware of such incident,

to the extent practicable. Where such breach poses a risk to the rights and freedoms of data subjects, the Company shall notify the data subjects of the breach together with remedial measures without delay.

The Company shall not be liable for any damages arising from intentional acts, negligence, or failure to comply with security measures by data subjects or other persons who have obtained consent from the data subjects, resulting in the unauthorized use or disclosure of personal data to any third party.

The Company regularly reviews and updates its procedures and security measures relating to personal data protection to ensure that the level of personal data security remains appropriate to the associated risks and to ensure the continuous confidentiality, integrity, availability, and resilience of personal data processing. This includes protection against loss, collection, access, use, alteration, modification, or disclosure of personal data without authorization. Such security measures shall apply to all types of personal data processing, whether conducted in electronic form or in physical document form.

11. Processing of Personal Data

Upon receipt of personal data, the Company shall carry out the following actions with respect to the personal data of the data subject.

11.1 Data Collection Procedures

The Company shall collect and retain personal data in documentary and/or electronic form only to the extent necessary for the provision of services or electronic services, under the Company's purposes and for a period no longer than necessary for the use of personal data in accordance with the specified purposes. Such personal data shall be deemed accurate, complete, and up to date, and the data subject shall have lawfully consented to the provision of such personal data to the Company.

The Company may combine the personal data of the data subject with personal data obtained from other sources only where necessary and only with the consent of the data subject, for the purpose of updating personal data and improving the quality and efficiency of the Company's services.

11.2 Use of Personal Data

The Company shall use personal data where it has been considered beneficial to the Company's operations and business activities, in order to ensure compliance with applicable laws and regulations, or to improve service efficiency, enhance information security standards, manage risks, and prevent activities that may lead to violations of laws, applicable regulations, relevant usage rules, or the Company's website terms and conditions.

Such use shall also include communications with the data subject via telephone, text messages, email, postal mail, or any other channels, as necessary, for inquiries, notifications, verification and confirmation of information, conducting surveys, or providing other information related to the Company's products and services.

11.3 Disclosure of Personal Data

The Company may disclose the personal data of the data subject to its subsidiaries or external parties solely for the purpose of the Company's operations and in accordance with the purposes for which the Company has obtained consent from the data subject.

The Company shall not disclose the personal data of the data subject to any other external parties without the data subject's authorization, except where such disclosure is made to governmental authorities, competent officials, or other persons who are lawfully entitled to receive such personal data, such as courts, police officers, or other persons who are legally entitled to request personal data of the data subject from the Company in accordance with applicable laws.

12. Rights of Data Subjects

12.1 Data subjects shall have the following rights:

(1) Right to Withdraw Consent: Where a data subject has given consent to the Company to collect, use, and/or disclose his or her personal data (whether such consent was given prior to or after the effective date of the Personal Data Protection Law), the data subject shall have the right to withdraw such consent at any time throughout the period during which the personal data remains with the

Company, unless such right is restricted by law or there exists a contract that provides benefits to the data subject.

In this regard, the withdrawal of consent may affect the data subject's ability to use certain products and/or services, such as the loss of benefits, promotions, or new offers, the inability to receive products or services that are better aligned with the data subject's needs, or the inability to receive information that may be beneficial to the data subject. For the benefit of the data subject, it is therefore advisable to study and inquire about the potential consequences prior to withdrawing consent.

(2) Right of Access to Personal Data: A data subject shall have the right to access his or her personal data and to request that the Company provide a copy of such personal data, including the right to request disclosure of the source from which the Company has obtained such personal data. However, the Company may refuse the data subject's request if such access to, or provision of a copy of, the personal data would adversely affect the rights and freedoms of other persons, or where the Company is required to comply with applicable laws or a court order prohibiting the disclosure of such personal data.

(3) Right to Data Portability: A data subject shall have the right to receive his or her personal data where the Company has prepared such personal data in a format that is readable or usable by automatic means or devices and can be used or disclosed by automated means. The data subject shall also have the right to request the Company to transmit or transfer such personal data in such format to another personal data controller where technically feasible, and to receive personal data that the Company has transmitted or transferred in such format directly to another personal data controller, unless such transfer cannot be carried out due to technical reasons.

In this regard, the personal data referred to above must be personal data for which the data subject has given consent to the Company for collection, use, and/or disclosure, or personal data that the Company is required to collect, use, and/or disclose in order to enable the data subject to use the Company's products and/or services in accordance with the data subject's intent as a contracting party with the Company, or for the purpose of carrying out actions at the request of the data subject prior to

the use of the Company's products and/or services, or other personal data as prescribed by the competent authority under the law.

(4) Right to Object to the Processing of Personal Data: A data subject shall have the right to object, at any time, to the collection, use, and/or disclosure of his or her personal data where such processing is carried out for operations that are necessary for the legitimate interests of the Company or of other persons or juristic persons, within the scope reasonably expected by the data subject, or for the performance of a task carried out in the public interest. Where the data subject raises an objection, the Company may continue to collect, use, and/or disclose such personal data only where the Company can demonstrate legitimate grounds that override the fundamental rights of the data subject, or where such processing is necessary for the establishment, compliance with, or exercise of legal claims, or for legal proceedings, as the case may be.

In addition, the data subject shall have the right to object to the collection, use, and/or disclosure of his or her personal data for marketing purposes, or for scientific, historical, or statistical research purposes.

(5) Right to Erasure (Right to be Forgotten): A data subject shall have the right to request the erasure or destruction of his or her personal data, or to request that such personal data be rendered anonymized so that the data subject can no longer be identified, where the data subject believes that such personal data has been collected, used, and/or disclosed unlawfully, or where the Company no longer has a necessity to retain such personal data for the purposes specified in this Privacy Notice, or where the data subject has exercised the right to withdraw consent or the right to object as stated above, except where the Company is required to comply with applicable laws or to retain such personal data for the establishment, exercise of, or defense against legal claims.

(6) Right to Restriction of Processing: A data subject shall have the right to request a temporary restriction on the use of his or her personal data in cases where the Company is in the process of verifying a request for rectification of personal data or an objection raised by the data subject, or in other cases where the Company no longer has a necessity to retain such personal data and is required to erase or

destroy such personal data under applicable laws, but the data subject requests a restriction of use instead.

(7) Right to Rectification: A data subject shall have the right to request that the Company rectify his or her personal data to ensure that such data is accurate, up to date, complete, and not misleading.

(8) Right to Lodge a Complaint: A data subject shall have the right to lodge a complaint with the competent authority under applicable laws where the data subject believes that the collection, use, and/or disclosure of his or her personal data constitutes a violation of, or non-compliance with, applicable laws.

In the event that there are reasonable grounds to believe that the Company has violated the Personal Data Protection Law, the data subject shall have the right to submit a complaint to the Expert Committee appointed by the Personal Data Protection Committee in accordance with the rules and procedures prescribed under the Personal Data Protection Law.

Where a data subject submits a request to exercise his or her rights under the Personal Data Protection Law, upon receipt of such request, the Company shall proceed within the period prescribed by law. Notwithstanding the foregoing, the Company reserves the right to refuse or not to proceed with such request in cases permitted by law.

12.2 Company's Discretion

The Company shall have full rights and sole discretion to accept and proceed with, or to refuse, a data subject's request.The exercise of the data subject's rights under Clause 12.1 may be restricted under applicable laws, and in certain circumstances, the Company may be required to refuse or may be unable to comply with such request, such as where compliance is necessary to adhere to applicable laws or court orders, for public interest purposes, or where the exercise of such rights may infringe upon the rights or freedoms of other persons. In the event that the Company refuses such request, the Company shall inform the data subject of the reasons for such refusal.

Measures for Facilitating the Exercise of Data Subject Rights

The Company shall establish appropriate channels for receiving requests for the exercise of data subject rights in order to facilitate data subjects. The Company shall designate a central unit responsible for reviewing and considering requests for the exercise of data subject rights prior to taking action in response to such requests (**Data Subject Rights Management**), and shall determine the timeframe for complying with such requests, together with promptly notifying data subjects of the results of the actions taken in response to their requests.In addition, the Company shall maintain records of personal data management in cases where requests for the exercise of data subject rights are rejected, for evidentiary purposes when requested by the Office or the data subjects.

Personal Data Breach Notification

(1) In the event that any employee or department discovers that the information technology system and/or a process related to personal data processing is unable to operate due to a personal data breach, such employee or department shall notify the relevant department immediately or within any other timeframe as prescribed under the internal operating procedures. The relevant department shall then coordinate with the Data Protection Officer (DPO) (if any) or the Personal Data Protection Working Group to take appropriate actions. In any other circumstances involving a personal data breach, the employee or department discovering such incident shall directly notify the Data Protection Officer (if any) or the Personal Data Protection Working Group as soon as possible in order to take appropriate actions.

(2) Thereafter, the Data Protection Officer (if any) or the Personal Data Protection Working Group shall investigate all incidents relating to the personal data breach in order to implement appropriate measures to mitigate the impacts and prevent future personal data breaches. Such actions shall include notifying the data subjects and the Office in accordance with the requirements prescribed by law, based on the following criteria:

Impact on the Rights and Freedoms of the Data Subject	Actions
Case where there is no risk	- Record the personal data breach incident.
Case where there is a risk	- Record the personal data breach incident. - Notify the Office within 72 hours.
Case where there is a high risk	- Record the personal data breach incident. - Notify the Office within 72 hours. - Notify the data subject without undue delay, together with appropriate remedial measures.

This Personal Data Protection Policy was approved by the Board of Directors' Meeting No. 1/2024 held on 19 July 2024 and shall be effective from 23 July 2024 onwards.

Announced on 23 July 2024

(Mr. Chawalit Tippawanich)

Chairman of Board of Directors

Unique Plastic Industry Public Company Limited