# PRIVACY POLICY

## PRIMO SERVICE SOLUTION PUBLIC COMPANY LIMITED

**PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED**
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
**T** 02 081 0000 **E** info@primo.co.th
WWW.PRIMO.CO.TH

**Record of revision**

| Revision No. | Announcement's date | Details for revision |
|---|---|---|
| **00** | 11/08/2026 | First announced |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**PRIVACY POLICY**

**PRIMO SERVICE SOLUTION PUBLIC COMPANY LIMITED**

This Policy shall apply to Primo Service Solutions Public Company Limited and its subsidiaries. In the event that any regulation, rule, or operating manual is inconsistent or conflicts with this Policy, such regulation, rule, or operating manual shall be revoked to the extent of such inconsistency, and this Policy shall prevail. This Policy shall be effective from 11 August 2026 onwards.

## 1. Introduction

Primo Service Solutions Public Company Limited and its subsidiaries (collectively, the "Company") recognize the importance of protecting personal data and other information relating to data subjects (collectively, the "Data"), in order to ensure that data subjects can have confidence in the Company's transparency and accountability in collecting, using, or disclosing personal data in accordance with the Personal Data Protection Act B.E. 2562 (2019) (the "Personal Data Protection Law"), as well as other applicable laws.

This Personal Data Protection Policy and Guidelines (the "Policy") has therefore been established to ensure that employees at all levels, officers, and relevant persons acting on behalf of or for the Company are aware of and comply with the Policy. The Policy sets forth the following key principles and requirements

## 2. Scope and Objectives

This Policy shall apply to employees at all levels, officers, and relevant persons acting on behalf of or for the Company in connection with activities involving the collection, use, or disclosure of Personal Data. Such activities shall be conducted in accordance with the following seven key principles:

1) Lawfulness, Fairness, and Transparency
2) Purpose Limitation
3) Data Minimization
4) Accuracy and Completeness
5) Storage Limitation
6) Confidentiality and Integrity of Personal Data
7) Accountability

The objectives of this Policy are to ensure that the Company's activities are conducted in a secure, reliable, and trustworthy manner, to protect the Personal Data of employees, customers, business partners, business alliances, visitors, and other persons having legal relationships with the Company, and to prevent any damage arising from the fraudulent exploitation or misuse of Personal Data.

## 3. Definition

| Vocabulary | Definition |
|---|---|
| Company | Primo Service Solutions Public Company Limited and its subsidiaries |
| Subsidiary, subsidiaries | limited company or public limited company under the control of Primo Service Solutions Public Company Limited. |

| Vocabulary | Definition |
|---|---|
| Employee, employees | any person working for the Company at any level, including directors, executives, permanent and temporary employees, personnel, workers, interns, and probationary employees, whether engaged under an employment contract or otherwise directly engaged by the Company. |
| Data Subject | a person who is the subject of the Personal Data collected, used, or disclosed by the Company, or a person to whom such Personal Data relates. |
| Personal Data | any information relating to a person that enables the identification of such person, whether directly or indirectly, excluding information of deceased persons in particular |
| Sensitive Personal Data | Personal Data of a sensitive nature that may give rise to a risk of unfair discrimination and therefore requires special care and protection. Such data includes racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, trade union membership, genetic data, biometric data, or any other information that may affect the Data Subject in a similar manner, as prescribed by the Personal Data Protection Committee. |
| Criminal Record Data | Personal Data relating to the investigation or inquiry of criminal offenses, criminal proceedings, or the serving of criminal sentences, which constitutes official information or information certified by a government authority having the legal power and duty to conduct such proceedings, regardless of whether such proceedings have been concluded. Examples include criminal background check documents issued by the Criminal Records Division, as well as indictments, petitions, applications, statements, and other documents submitted in criminal proceedings |
| Data Controller | an individual or juristic person who has the power and duty to make decisions regarding the collection, use, or disclosure of Personal Data, including employees, departments, or officers authorized or assigned to act on behalf of such individual or juristic person |
| Data Processor | an individual or juristic person who collects, uses, or discloses Personal Data pursuant to the instructions or on behalf of the Data Controller, provided that such individual or juristic person is not the Data Controller in respect of such activities |
| Personal Data Processing | any operation or set of operations performed on Personal Data, whether or not by automated means, such as collecting, copying, organizing, storing, updating, altering, using, restoring, disclosing, transferring, disseminating, or destroying Personal Data |
| Personal Data Source | the source from which Personal Data of a Data Subject is obtained or received |
| Third party, Third parties | any individual or juristic person other than the Data Subject, Data Controller, or Data Processor who is engaged or contracted to process Personal Data on behalf of the Company |
| Data Protection Officer: DPO | a person appointed to provide advice on and monitor the operations of the Data Controller, Data Processor, or employees to ensure compliance with the Personal Data Protection Act. |
| Record of Processing Activities: RoPA | a document that records details of all Personal Data collected, used, or disclosed by each department, Personal Data processing activities, data retention measures and retention periods, the rights of Data Subjects and procedures for exercising such rights, as well as any refusal of or objection |

| Vocabulary | Definition |
|---|---|
| | to requests made by Data Subjects to exercise their rights, and other relevant information |
| Personal Data Breach | a breach of security measures that results in the loss of, unauthorized or unlawful access to, use of, alteration of, modification of, or disclosure of Personal Data, whether arising from an intentional or deliberate act, negligence, an unauthorized or unlawful act, a computer-related offense, a cyber threat, an error, defect, or accident, or any other cause |
| Privacy Notice | a notice provided to Data Subjects regarding the purposes and methods of the Company's collection, use, disclosure, processing, and storage of Personal Data |
| Cookie | small data files generated by a website and stored on a user's computer or electronic device, which may contain Personal Data, information about the user's activities, and user preferences for the purpose of enhancing the user's experience when using the Company's website |

## 4. Categories of Personal Data Collected, Used, or Disclosed by the Company

In conducting its various activities, the Company, its employees, or the Data Controller may collect or obtain various types of Personal Data, depending on the activities involved and the context of the relationship between the Data Subject and the Company. Such Personal Data may be categorized as follows:

| Categories of Personal Data | Details and Examples |
|---|---|
| Personal Identification Data | Information that identifies or is used to identify a Data Subject, including information contained in official documents identifying the Data Subject, such as title, first name, last name, alias, national identification number, taxpayer identification number, passport number, nationality, address, house registration information, driver's license information, signature, social security number, or other official documents that can be used to identify the Data Subject. |
| Personal Characteristics Data | Information relating to the characteristics of a Data Subject, such as date of birth, sex, height, weight, age, marital status, military service status, personal capabilities, photographs, fingerprints, facial scans, and other similar information. |
| Contact Information | Information used to contact or communicate with a Data Subject, such as registered residential address, mailing address, telephone number, facsimile number, email address, location or map of the address, username on online platforms, account name or username used to identify the Data Subject through software or applications, and other electronic communication channels or contact information. |
| Employment and Education Information | such as employment details, work history, educational history, type of employment, occupation, rank, position, duties, areas of expertise, work permit status, references, emergency contact information, history of positions held, salary information, employment commencement and termination dates, performance evaluation results, work performance, educational institutions, educational qualifications, academic results, graduation date, workplace entry and exit records, working hours and attendance records, and other similar information. |

| Categories of Personal Data | Details and Examples |
|---|---|
| Insurance Policy Information | Information relating to an employee's insurance policy, such as the insurer, insured person, beneficiary, policy number, type of insurance policy, coverage amount, claim information, and other related information. |
| Transaction or Financial Information | Transaction or financial information, such as account name, bank account number, etc. |
| Company Service Usage Information | Information relating to the use of the Company's products or services, such as username, password, Personal Identification Number (PIN), Single Sign-On (SSO) ID, One-Time Password (OTP), Internet Protocol (IP) address, computer traffic data (logs), location data, photographs, videos, audio recordings, usage behavior and activities on websites operated by the Company or its applications, internet usage and connections to other websites, information collected through Cookies or similar technologies, Device ID, device type, browser information, operating system information, and website user statistics collected for analysis and presentation in various forms, such as the number of users, geographical distribution of users, devices or operating systems used, duration of use, and other detailed analytics. |
| Other personal data | Other Personal Data, such as marketing analytics and statistical data, video footage, Closed-Circuit Television (CCTV) footage, audio and video recordings collected when a Data Subject contacts the Company, records of conversations and communications, and records of transactions conducted via telephone, video calls, or other electronic devices, as well as communications with the Company through other channels not otherwise specified above. |
| Sensitive Personal Data | Sensitive Personal Data of a Data Subject, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, mental health information, medical information, trade union membership, genetic data, and biometric data (meaning Personal Data resulting from the use of techniques or technologies relating to an individual's physical or behavioral characteristics that enable such individual to be uniquely identified or authenticated, such as facial recognition data, iris recognition data, or fingerprint recognition data), as well as any other information that may affect the Data Subject in a similar manner, as prescribed by the Personal Data Protection Committee. |
| Personal information about criminal records | Information relating to the investigation or inquiry of criminal offenses, criminal proceedings, or the serving of criminal sentences, such as employee criminal background checks conducted prior to employment, and Personal Data appearing in indictments, petitions, applications, statements, or other documents submitted in criminal proceedings. |

## 5. Roles and Responsibilities of Internal Departments

### 1) Board of Director

Responsible for supporting and promoting the Company's operations to ensure compliance with applicable laws, rules, regulations, requirements, orders, notifications, measures, and guidelines, as well as policies, customary practices, professional standards, ethics, and procedures

relevant to the business operations of the Group, including the appointment of the Company's Data Protection Officer (DPO).

**2) Corporate Governance and Sustainable Committee**

Responsible for providing support and assistance to the Board of Directors in overseeing the Company to ensure compliance with applicable laws, rules, regulations, requirements, standards, and guidelines governing the Company's business operations, by establishing appropriate policies and procedures for the Company's business operations, including provisions relating to good corporate governance in accordance with good governance principles.

**3) Risk Management Committee**

3.1) Evaluate the effectiveness of the Company's compliance with the Personal Data Protection Policy and report the evaluation results to the Board of Directors on a regular basis at least once a year. In addition, oversee and ensure that risks relating to Personal Data are properly managed and that appropriate risk management measures are in place.

3.2) Establish and review operational standards and guidelines to ensure that the Company's operations comply with applicable laws and the Company's Personal Data Protection Policy.

**4) Board of Directors of Subsidiaries**

Responsible for acknowledging the Policy and ensuring that all employees under their supervision strictly comply with the Policy.

**5) Senior Management**

Responsible for reviewing and approving orders, notifications, manuals, or internal guidelines within their respective departments, and overseeing employees and workers within their departments to ensure that personal data protection activities are carried out properly and in compliance with the Policy, operating procedures, orders, notifications, or internal guidelines of their respective departments concerning personal data protection.

**6) The Internal Audit Department has the following duties:**

6.1) Establish the objectives, direction, and scope of internal audit activities to support the management and operations relating to compliance with the Personal Data Protection Law, taking into consideration the effectiveness of risk management and the adequacy of the Company's internal control system.

6.2) Audit the Company's compliance with personal data protection requirements within the scope of internal audit activities, in accordance with internal audit standards, the ethical standards applicable to internal auditors, and internal audit manuals or guidelines based on international standards.

6.3) Review relevant documents and processes and assess the effectiveness of security measures for systems relating to Personal Data.

6.4) Report the audit results to the Audit Committee of the Group.

**7) Information Technology Department**

Responsible for supporting and providing appropriate, adequate, effective, and accurate information technology systems that comply with applicable legal requirements for use in personal data protection processes and the internal operations of relevant departments, in order to facilitate operations and promote compliance with the requirements of the Personal Data Protection Law.

**8) Legal Department**

Responsible for reviewing and amending contractual provisions or agreements between companies within the Group, as well as agreements between the Company and customers or transaction counterparties, directors, executives, employees, workers, business partners or contractual counterparties, external service providers, and business alliances, to ensure that the management and processing of Personal Data are carried out in accordance with the requirements of the Personal Data Protection Law.

**9) Resources & Administration Department**

Responsible for supporting and managing training programs to provide all new employees with knowledge and understanding of the Personal Data Protection Law, as well as providing refresher training for existing employees on the Company's Personal Data Protection Policy, operating procedures, orders, notifications, guidelines, and manuals relating to personal data protection. Training attendance records shall be maintained as evidence, and employees shall be required to attend refresher training at the prescribed intervals. In addition, responsible for managing the Personal Data of the Company's directors, executives, employees, and workers under the responsibility of the relevant department in accordance with the Company's personal data security measures.

**10) Employees have the following duties:**

10.1) Give due importance to and strictly comply with the Personal Data Protection Law, the Company's policies, regulations, orders, notifications, guidelines, and operating manuals relating to personal data protection.

10.2) Attend personal data protection training in accordance with the training schedule and whenever designated to attend such training. Employees shall give due importance to and fully cooperate with the Company's personal data protection training requirements.

10.3) Immediately report to their supervisor or manager and notify the Data Protection Officer (DPO) upon becoming aware of any leakage or breach of Personal Data.

10.4) Refrain from disclosing any Personal Data that they become aware of or obtain in the course of their duties to any other person, except as permitted or required by law.

10.5) If an employee becomes aware of any conduct that may constitute a violation of this Policy, they shall report such conduct through the Company's whistleblowing and complaints channels.

**11) Data Controller**

They are responsible for handling and processing personal data in accordance with the requirements prescribed under applicable personal data protection laws, subordinate legislation, rules, regulations, and relevant orders, and shall strictly comply with this Policy.

**12) Data Protection Officer: DPO**

The Data Protection Officer (DPO) shall have the following duties and responsibilities:

12.1) Provide advice and guidance to employees, departments, and personnel within the Company to ensure that the collection, use, disclosure, and processing of personal data are carried out correctly and in compliance with applicable laws.

12.2) Monitor and audit the operations of employees, data controllers, data processors, as well as external parties, external companies, or contractors, in relation to the collection, use, or disclosure of personal data in compliance with applicable laws, including, for example, conducting a Data Protection Impact Assessment (DPIA) to assess the risks of personal data breaches within the Company.

12.3) Coordinate and cooperate with the Personal Data Protection Office (PDPC) in the event of any issues relating to personal data within the Company, including handling data subject requests and complaints.

12.4) Promote and foster a culture of personal data protection within the Company.

12.5) Maintain the confidentiality of personal data that the DPO becomes aware of or obtains in the course of performing their duties.

## 6. Collection of Personal Data

The Data Controller shall obtain consent from the Data Subject prior to or at the time of collecting Personal Data, in accordance with lawful purposes and methods. The Data Controller shall rely on an appropriate legal basis for the collection of Personal Data and collect only such Personal Data as is necessary for the Company's operations and intended purposes. The Data Controller shall also inform the Data Subject of the details required by applicable laws, including the purposes for which the Personal Data will be collected, used, or disclosed, as well as the Data Subject's rights to withdraw consent, the consequences of refusing to provide consent, and the rights to request access to, obtain a copy of, or request the disclosure, rectification, modification, deletion, or destruction of Personal Data, or to object to the collection, use, or disclosure of Personal Data. Where consent is required, the Data Controller shall obtain such consent prior to or at the time of collecting Personal Data. In cases where explicit consent is required by law, the Data Controller shall obtain explicit consent from the Data Subject accordingly.

For the collection of Sensitive Personal Data, including race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, trade union information, genetic data, biometric data, and any other data that may similarly affect the Data Subject, as prescribed by the Personal Data Protection Committee, the Data Controller shall obtain explicit consent from the Data Subject in writing or through an electronic system. The Data Controller shall process Sensitive Personal Data with special care and caution, as such data carries a higher risk of being used for unfair discrimination against the Data Subject.

In addition, in cases involving the collection of Personal Data of minors, incompetent persons, or quasi-incompetent persons, the Data Controller shall obtain consent from the legal guardian or other person legally authorized to act on behalf of such person prior to collecting such Personal Data. If it is subsequently discovered that the Company has collected Personal Data of a minor, incompetent person, or quasi-incompetent person without obtaining consent from the legal guardian or other person legally authorized to act on behalf of such person, and the Company has no other lawful basis for the collection, use, or disclosure of such Personal Data, the Data Controller shall promptly delete and destroy such Personal Data.

The Data Controller shall collect Personal Data from the following sources:

1) Collection of Personal Data directly from the Data Subject, including:

- Conducting transactions, completing forms, providing opinions or feedback, or making inquiries through the Company's website, mobile applications, email, in-person interactions, or any other means;
- Participating in marketing activities, lucky draws, events, and other activities;

- Receiving services through websites, applications, or E-Commerce service providers;

- Providing supporting documents for business contracts or employment contracts with the Company;

- Providing supporting documents for job applications;

- The recording of still images or video footage through closed-circuit television (CCTV) cameras at premises under the Company's control;

- Visiting the Company's website, whether intentionally or unintentionally; and other similar sources.

2) Collection of Personal Data from other sources, including:

- Collecting Personal Data from publicly available sources, business information sources, commercial information sources, or social media, regardless of whether the Data Subject has disclosed such information personally or has consented to any person to disclose such Personal Data;

- Collecting Personal Data from third parties, such as family members, emergency contacts, beneficiaries, guarantors, employment-related contacts, job application websites, references, recruitment agencies, government agencies, educational institutions, securities depositories, banks, or persons authorized to offer the Company's debentures for sale, regardless of whether the Data Subject has disclosed such information personally or has consented to any person to disclose such Personal Data; and other similar sources.

In cases the Company is required to collect Personal Data from a source other than the Data Subject, the Company shall inform the Data Subject of such collection and obtain consent from the Data Subject without undue delay and within 30 (thirty) days from the date of collection, unless otherwise prescribed by law.

## 7. Lawful Basis for the Processing of Personal Data

The Company shall determine and apply the appropriate lawful basis for the collection and processing of the Data Subject's Personal Data, taking into consideration the nature and context of the relevant services, including the following:

| Lawful Basis for the Processing of Personal Data | Details |
|---|---|
| Legal Obligation | This lawful basis applies where the Company is required to process Personal Data in order to comply with its legal obligations, including compliance with provisions of laws, notifications, regulations, or orders issued by competent government authorities, such as:<br>- Collecting computer traffic data as required under the Computer-Related Crime Act B.E. 2560 (2017);<br>- Disclosing financial information to the Revenue Department as required under applicable tax laws; and<br>- Complying with court orders. |
| Legitimate Interests | This lawful basis applies where the processing of Personal Data is necessary for the legitimate interests of the Company or another person, provided that such interests are not overridden by the fundamental rights and freedoms of the Data Subject with respect to their Personal Data. |

| Lawful Basis for the Processing of Personal Data | Details |
|---|---|
| | Examples include processing Personal Data for the security of the Company's buildings and premises, or processing Personal Data for the Company's internal business operations. |
| Vital Interests | This lawful basis applies where the processing of Personal Data is necessary to prevent or mitigate danger to the life, body, or health of an individual. For example, using medical or treatment information to monitor and prevent the spread of infectious diseases in accordance with government policies. |
| Contractual Necessity | This lawful basis applies where the processing of Personal Data is necessary for the Company to perform its obligations under a contract or to take steps at the request of the Data Subject prior to entering into a contract with the Company. Examples include employment contracts, contracts for hire of work, memoranda of understanding (MOUs), sale and purchase agreements, service agreements, or other types of contracts. |
| Historical, Research, or Statistical Purposes | This lawful basis applies where the processing of Personal Data is necessary for the Company to prepare or support the preparation of historical, research, or statistical records as assigned to or required of the Company. For example, providing information to government agencies as required by applicable laws. |
| Consent | This lawful basis applies where the Company is required to obtain consent from the Data Subject for the collection, use, or disclosure of Personal Data. Prior to obtaining consent, the Company shall inform the Data Subject of the purposes for which the Personal Data will be collected, used, or disclosed, both prior to and at the time of collecting the Personal Data. Examples include the collection of Sensitive Personal Data, such as race, religion, blood type, health information, criminal records, facial scans, fingerprints, or other biometric data, for purposes that are not exempt from the consent requirement under the lawful bases for processing Personal Data described above. |

In cases the Company is required to collect Personal Data for the performance of a contract, compliance with a legal obligation, or taking necessary steps prior to entering into a contract, if the Data Subject refuses to provide the Personal Data or objects to the processing of such Personal Data for the aforementioned purposes, the Data Controller shall inform the Data Subject that such refusal or objection may result in the Company being unable to fully or partially perform the requested activities or provide the services requested by the Data Subject.

## 8. Purposes for the Collection, Use, or Disclosure of Personal Data

The Data Controller shall collect, use, or disclose the Personal Data of Data Subjects for purposes necessary for the Company's operations, including procurement, entering into contracts, financial transactions, communication and coordination, and conducting various activities to achieve the Company's business objectives and comply with applicable laws and regulations.

The Data Controller shall inform the Data Subject of the purposes for the collection, use, or disclosure of Personal Data prior to or at the time of collecting such Personal Data, including the following:

1) To carry out activities necessary for the Company's business operations;

2) To provide services, manage the Company's services, and improve the quality of products and services to meet customers' needs;

3) To conduct the Company's business transactions;

4) To control, operate, monitor, supervise, and manage services in order to facilitate and provide services in accordance with the needs of the Data Subject;

5) To retain and update information relating to the Data Subject, including documents that refer to or contain information relating to the Data Subject;

6) To prepare and maintain records of processing activities as required by applicable laws;

7) To analyze data, including identifying and resolving issues relating to the Company's services;

8) To carry out activities necessary for the internal administration and management of the organization, including recruitment, selection of directors or persons holding various positions, and assessment of qualifications;

9) To prevent, detect, avoid, investigate, and address fraud, security breaches, prohibited or unlawful acts, or any acts that may cause damage to the Company or the Data Subject;

10) To verify and authenticate the identity of the Data Subject and verify information when the Data Subject applies for the Company's services, contacts or uses the Company's services, or exercises rights under applicable laws;

11) To improve and develop the quality of products and services to keep them up to date;

12) To assess and manage risks;

13) To send notifications, confirmations of instructions or transactions, communications, and other information to the Data Subject;

14) To prepare and deliver relevant and necessary documents or information;

15) To verify identity and prevent spam, unauthorized activities, or unlawful activities;

16) To monitor and analyze how Data Subjects access and use the Company's services, both collectively and individually, for research and analytical purposes;

17) To carry out activities necessary for the Company to fulfill its obligations toward regulatory or supervisory authorities, law enforcement authorities, or under the Company's legal obligations, including tax authorities;

18) To carry out activities necessary for the legitimate interests of the Company, another person, or another relevant legal entity in connection with the Company's operations;

19) To prevent or mitigate danger to the life, body, or health of individuals, including monitoring and preventing the spread of infectious diseases;

20) To prepare documents for activities relating to public interest, research, or statistical purposes that the Company is assigned to undertake by government agencies;

21) To comply with applicable laws, notifications, orders, or other legally binding requirements, or to undertake activities relating to legal proceedings, including processing information pursuant to court orders and exercising rights relating to the Personal Data of the Data Subject; and

22) To record fingerprint images or facial images for the purpose of verifying the identity of employees when recording their entry to and exit from the Company's workplace, as well as for maintaining the security of employees and the Company's property.

The Company shall not collect, use, or disclose Personal Data for purposes that are different from those notified to the Data Subject, except where:

1) The Company has informed the Data Subject of the new purpose and/or obtained the Data Subject's consent; or

2) Such collection, use, or disclosure is necessary to comply with applicable personal data protection laws or other relevant laws.

## 9. Disclosure of Personal Data

In case the Company is required to disclose the Personal Data collected to other Data Controllers, Data Processors, or external persons or entities for the purposes previously notified to the Data Subject, where consent has been obtained from the Data Subject, or where such disclosure is otherwise permitted by law, including to government agencies or competent authorities as required by law, the Company may disclose such Personal Data as necessary for the Company's business operations and to facilitate the exercise of the Data Subject's rights.

Such recipients may include, but are not limited to:

1) Subsidiaries or companies within the Company's group;

2) Shareholders, including their executives, whether individuals or legal entities, as well as companies within the shareholders' corporate group;

3) Event organizers, public relations agencies, members of the media, or sponsors of events or exhibitions;

4) Hotels or other venue service providers and their representatives involved in events or exhibitions;

5) Subcontractors, service providers, suppliers, and agents acting on behalf of or engaged by the Company, including banking or financial service providers, internet hosting, application, cloud, or data network service providers, event registration service providers, domestic and international travel service providers, security service providers, audit firms, legal service providers, insurance service providers, and other relevant service providers;

6) Market research service providers, email or mailing management service providers, and representatives or agents who sell or promote products and services on behalf of the Company, as well as other service providers necessary for the Company's business operations;

7) Thailand Securities Depository Co., Ltd., acting as a registrar;

8) Banks or financial institutions with which the Company conducts transactions;

9) Any person who purchases or sells, or intends to purchase or sell, the Company's business or any part thereof, including parties involved in a merger, acquisition, or purchase of another business or company;

10) Any person or government agency as required by law, pursuant to a court order, or any other person or entity having lawful authority; and

11) Regulatory authorities, government agencies, private organizations, or state-owned enterprises responsible for supervising or regulating the Company's business operations under applicable laws, where such laws require the Company to disclose the Personal Data to such entities.

The Data Controller shall disclose or transfer Personal Data only to the extent necessary to achieve the specified purposes and shall ensure that an agreement is entered into with other Data Controllers or Data Processors, using the standard contractual template prepared by the Legal Department.

Such agreement shall specify the terms and conditions governing the disclosure or transfer of Personal Data and require the Data Processor or such person or entity to maintain the confidentiality of the Personal Data and not use the Personal Data for any purposes other than those specified by the Company.

## 10. Transfer or Transmission of Personal Data to Foreign Countries

In case the Company is required to transfer or transmit Personal Data to persons or entities located outside Thailand based on an applicable lawful basis or the consent of the Data Subject, such as transferring Personal Data to cloud systems with platforms or servers located overseas, or supporting information technology systems located outside Thailand, the Data Controller shall take appropriate measures to ensure that the destination country provides a level of Personal Data protection equivalent to or higher than the standards applicable in Thailand.

The Data Controller shall also ensure that the recipient of the Personal Data has appropriate measures in place to protect such Personal Data in accordance with applicable laws and regulations.

## 11. Retention and Retention Period of Personal Data

The Data Controller shall retain Personal Data in either hard copy or electronic form, depending on the nature of or manner in which the Personal Data is obtained. The Data Controller shall implement appropriate security measures for the storage of Personal Data to prevent unauthorized access, destruction, alteration, modification, disclosure, loss, or any unauthorized processing of Personal Data, as well as to prevent Personal Data breaches. The Company shall implement measures to authenticate and verify the identity of authorized persons who are permitted to access and perform any activities relating to Personal Data in accordance with the Company's Information Technology Security Policy, such as requiring password-protected access to Personal Data. The Data Controller shall retain Personal Data only for as long as necessary to fulfill the purposes for which such Personal Data was collected, used, or disclosed. Personal Data shall be retained for the applicable retention period for as long as the Company continues to have a lawful basis or legal right to collect, use, or disclose such Personal Data, or for the period prescribed by applicable laws or the applicable statutory limitation period, subject to a maximum retention period of 10 (ten) years from the date on which the Data Subject's transactions or relationship with the Company are terminated.

Upon the expiry of the applicable retention period or when the Personal Data is no longer necessary for the purposes for which it was collected, the Data Controller shall delete, destroy, or anonymize such Personal Data so that the Data Subject can no longer be identified, in accordance with the methods and standards for the deletion or destruction of Personal Data prescribed by the Personal

Data Protection Committee, applicable laws, or internationally recognized standards. However, in cases there is a dispute concerning the exercise of rights or legal proceedings relating to Personal Data, the Data Controller may be required to retain such Personal Data until the dispute or legal proceedings have been finally resolved by a final order or judgment.

If the retention period has expired or the Personal Data is no longer necessary for the purposes for which it was collected, the Data Controller shall delete, destroy, or anonymize such Personal Data so that it can no longer be used to identify the Data Subject, in accordance with the following procedures:

(1) Upon expiration of the applicable retention period, the Data Controller shall monitor and verify the expiry of such retention period and submit the matter to the Data Protection Officer (DPO) for review and approval of the destruction of the Personal Data.

(2) Then the Data Subject exercises the right to request the deletion or destruction of Personal Data, the Data Protection Officer (DPO) shall review and approve the destruction of such Personal Data.

Once the Data Protection Officer (DPO) has approved the destruction of Personal Data, the Data Controller may proceed with the deletion, destruction, or anonymization of such Personal Data so that the Data Subject can no longer be identified.

For Personal Data stored in hard copy, the Personal Data shall be destroyed by using a document shredder or other appropriate destruction methods. For Personal Data stored in electronic form, the Personal Data shall be deleted from the relevant systems and network drives, or anonymized in such a manner that the Data Subject can no longer be identified. Once the Data Controller has completed the deletion, destruction, or anonymization of the Personal Data, the Data Controller shall notify the Data Protection Officer (DPO) of the outcome and provide supporting evidence of the deletion, destruction, or anonymization.

In case the deletion, destruction, or anonymization was requested by the Data Subject, the Data Controller shall also notify the Data Subject of the outcome. The Data Controller shall also record such actions in the Record of Processing Activities (ROPA).

## 12. Data Subject Rights

Data Subjects shall have the following rights in relation to their Personal Data:

1) The right to withdraw consent where the Data Subject has previously provided consent;

2) The right to be informed of the details regarding the collection, use, or disclosure of their Personal Data (Privacy Notice);

3) The right to access and obtain a copy of their Personal Data;

4) The right to request the transfer of their Personal Data to another person or entity;

5) The right to object to the collection, use, or disclosure of their Personal Data;

6) The right to request the deletion, destruction, or anonymization of their Personal Data so that it can no longer be used to identify the Data Subject;

7) The right to request the restriction of the use of their Personal Data; and

8) The right to request the rectification of their Personal Data.

Data Subjects may exercise the rights described above by submitting a request to the Data Controller. The Data Controller shall process such request without undue delay and, in any event, within 30 (thirty) days from the date of receipt of the request. In the event of any uncertainty or doubt regarding the decision or appropriate action to be taken in response to a Data Subject's request, the Data Controller

shall consult with the Data Protection Officer (DPO) for advice and guidance to ensure that the request is handled correctly and in compliance with applicable laws.

The Data Controller may refuse a Data Subject's request to exercise their rights where such refusal is permitted or required by applicable law or a court order, or where the exercise of such right may adversely affect the rights and freedoms of other individuals. In such cases, the Data Controller shall inform the Data Subject of the reasons for refusing the request.

In addition, the Data Controller shall retain records and supporting evidence relating to requests made by Data Subjects to exercise their rights as required by applicable laws for a period of 1 (one) year from the date on which the Company has completed its consideration and processing of the Data Subject's request.

## 13. Personal Data Security Measures

The Company shall implement appropriate security measures for the collection, use, or disclosure of Personal Data, covering all relevant components of the information systems. Access to Personal Data shall be restricted to specific employees or personnel, or persons who are authorized, assigned, or otherwise have a legitimate need to access and use such Personal Data for the purposes previously notified to the Data Subject.

Such persons shall strictly comply with the Company's Personal Data protection measures to prevent the loss, unauthorized access, use, alteration, modification, or disclosure of Personal Data without authorization or in violation of applicable laws. They shall also maintain the confidentiality of Personal Data of which they become aware in the course of performing their duties and responsibilities.

In addition, the Company shall take into consideration and implement security measures in accordance with the Company's Information Technology Security Policy and applicable personal data protection laws in order to maintain the Confidentiality, Integrity, and Availability (CIA) of Personal Data.

## 14. Personal Data Breach or Personal Data Leakage

In the event of a Personal Data Breach or Personal Data leakage, the Data Controller shall take the following actions:

1) Promptly conduct a preliminary investigation into the Personal Data Breach, to the extent reasonably practicable, to determine whether there are reasonable grounds to believe that a Personal Data Breach has occurred. The Data Controller shall consider all relevant facts and circumstances and assess whether the Personal Data Breach is likely to adversely affect the rights and freedoms of individuals.

2) If during the investigation referred to in Clause 1), it is determined that the Personal Data Breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Controller shall promptly take appropriate measures, or instruct the Data Processor or relevant parties to take appropriate measures, to prevent, contain, or remediate the breach, so as to promptly terminate the breach or prevent further adverse impacts, to the extent reasonably practicable.

3) Report the incident to the relevant supervisor and the Data Protection Officer (DPO) as soon as possible in order to jointly determine appropriate remedial measures and a plan for mitigating any resulting damages.

4) Where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Controller shall promptly notify the Data Subject of the Personal Data Breach and the measures or remedies to be taken.

5) The Data Controller shall also implement necessary and appropriate measures to contain, respond to, remediate, and recover from the Personal Data Breach, as well as to prevent and mitigate the impact of similar Personal Data Breaches from occurring in the future.

In the event that a Personal Data Breach or Personal Data leakage is likely to adversely affect the rights and freedoms of individuals, the Data Protection Officer (DPO) shall notify the Personal Data Protection Committee (PDPC) of the breach in writing or through electronic means or any other method prescribed by the PDPC, within 72 (seventy-two) hours from the time the breach becomes known.

## 15. Record of Processing Activities (ROPA)

The Company requires the Data Controller and Data Processor to prepare and maintain a Record of Processing Activities (ROPA) in accordance with the form prescribed by the Company, so that the Data Subject, the Data Protection Officer (DPO), and the Personal Data Protection Committee (PDPC) can inspect and verify such records. The records may be maintained in written or electronic form.

The ROPA shall include at least the following information:

1) Details of the Personal Data collected;
2) The purposes for which each category of Personal Data is collected;
3) Information relating to the Data Controller;
4) The retention period of the Personal Data;
5) The rights and procedures for accessing Personal Data, including the conditions regarding persons who are authorized to access Personal Data and the conditions for such access; and
6) The use or disclosure of Personal Data in accordance with the purposes notified to the Data Subject.

## 16. Penalties

The Data Controller, Data Processor, employees, and any other persons are prohibited from using Personal Data without authorization or using Personal Data in any unlawful manner.

This prohibition also applies where persons responsible for carrying out any activities relating to the Company's business operations neglect or fail to perform their duties, improperly perform their duties, fail to comply with the Company's policies or Information Technology Security Measures, or fail to comply with Personal Data protection measures prescribed by applicable laws.

Any such acts or omissions may constitute a violation and may result in disciplinary action in accordance with the Company's regulations, as well as penalties prescribed under applicable personal data protection laws, including subordinate legislation, rules, regulations, and relevant orders.

In addition, a Data Processor may also be held liable for breach of the applicable contract or Data Processing Agreement (DPA).

## 17. Whistleblowing and Complaints

If an employee or any other person becomes aware of or witnesses any conduct that may constitute a violation of this Policy, they shall report such matter through the Company's whistleblowing and complaints channels in accordance with the Company's Whistleblowing and

Complaints Policy. The complainant or whistleblower shall be protected, and all information relating to the report shall be kept confidential. No adverse impact shall be imposed on the complainant's or whistleblower's employment status or position, either during the investigation process or after the investigation has been completed.

**18. Policy Review**

The Company shall review, update, and amend this Policy from time to time, or at least once every 2 (two) years, to ensure that it remains consistent with applicable practices, requirements, rules, regulations, and laws. In the event that this Policy is updated or amended, the Company shall publish the revised Policy on its website and through other communication channels of the Company as soon as practicable, so that employees are informed of and comply with the revised Policy. Any such amendments shall be deemed to form an integral part of this Policy.

**19. Contact Information**

If you have any questions, suggestions, or concerns regarding the Company's collection, use, or disclosure of Personal Data, or this Policy, or if a Data Subject wishes to exercise their rights under applicable personal data protection laws, please contact:

Data Protection Officer (DPO)

Contact Address: Primo Service Solutions Public Company Limited

496 Moo 9 Soi Bearing 16, Sukhumvit 107 Road, Samrong Nuea, Muang Samut Prakarn District, Samut Prakarn 10270

Email: DPO@primo.co.th

Telephone: 02-081-0000

This Policy shall be effective from 11 August 2026 onwards.

| | |
|---|---|
| **(Mrs. Suphin Mechuchep)** | **(Mr. Marote Vananan)** |
| **Chief Executive Officer** | **Chairman of the Board** |
| **Primo Service Solutions Public Company Limited** | **Primo Service Solutions Public Company Limited** |