primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

Third Parties and Cross Border Data Transfer Policy

Primo Service Solutions 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

primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

Table of Contents

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

1. Introduction/Objectives

The objectives of the Policy on Disclosure of Personal Data to External Parties or the Transfer of Personal Data to Foreign Entities are as follows:

1) To clarify the terms and conditions relating to the disclosure of personal data to third parties (external entities) or the transfer of personal data to foreign countries or international organizations.
2) To establish rules and protective measures for the disclosure of personal data to third parties (external entities) or the transfer of personal data to foreign countries or international organizations.

2. Scope

1) Geographical Scope

This Policy applies to the transfer of personal data collected, used, and disclosed by the Company to external entities or data processors, both domestically and internationally.

2) Content Scope

- This Policy applies to all personnel, including permanent employees, temporary employees, contract employees, workers, as well as departments, business units, and persons or juristic persons under the control of the Company.
- This Policy applies to the Company's partners who are involved in accessing or processing the Company's data.
- This Policy applies to all forms of personal data, including both electronic and non-electronic data.
- This Policy covers the transfer of data to external organizations, personal data processors, government agencies, or persons authorized under laws, regulations, or other legal requirements.

3. Definitions

In this Policy on Disclosure of Personal Data to External Parties or the Transfer of Personal Data to Foreign Entities, the following words or phrases shall have the meanings as defined below:

Personal Data Protection Law	Means the Personal Data Protection Act B.E. 2562 (2019), including any amendments thereto, as well as related rules, regulations, and orders.
Processing of Personal Data	Means any operation performed on personal data or sets of personal data, whether by automated means or not, such as collection, recording, organization, structuring, storage, alteration or modification, retrieval, consideration, use, disclosure by transmission, dissemination, or any other act making such data available, alignment or combination, restriction, deletion, or destruction.
Third-Party Data	Means all forms of data, both electronic and non-electronic, received from or possessed by the Company's partners or external parties.
Personal Data	Means any information relating to a person that enables the identification of such person, whether directly or indirectly, but excluding information relating specifically to deceased persons (Section 6 of the Personal Data Protection Act B.E. 2562 (2019)), such as first name, surname, email, photograph, fingerprint, national identification number, which can directly identify an individual, or the collection of location data or cookies, which enables indirect identification of an individual.
Data Subject	Means a person who can be identified, directly or indirectly, by such personal data.
Company	Means the business group of Primo Service Solutions Public Company Limited as of July 2022, comprising Passion Realtor Co., Ltd., Primo Management Co., Ltd., Crown Residence Co., Ltd., Wyde Interior Co., Ltd., Uno Service Co., Ltd.,

	United Project Management Co., Ltd., UPM Design Studio Co., Ltd., and Hampton Hotel and Residence Management Co., Ltd.
Third Parties	Means a natural person, juristic person, government office, government agency, or any other person other than the data subject, the Company, the personal data processor, or persons authorized by the Company or authorized by the personal data processor to directly process personal data.
Data Controller	Means a person having the authority and duty to make decisions regarding the collection, use, or disclosure of personal data.
Data Processor	Means a person who carries out the collection, use, or disclosure of personal data pursuant to the instructions of, or on behalf of, the personal data controller.

4. Third Parties Policy

The Company shall disclose personal data to external organizations or entities in accordance with the following guidelines:

1) If personal data is to be disclosed to business partners, business alliances, subsidiaries, and/or external service providers, such disclosure may only be carried out where the names of such business partners, business alliances, subsidiaries, and/or external service providers are specified in the Data Inventory. If they are not specified in the Data Inventory, approval must first be obtained from the Data Protection Officer prior to the disclosure of personal data. The Data Protection Officer shall consider the lawful basis for processing personal data and relevant conditions in compliance with personal data protection laws.
2) In cases involving the transfer of personal data to a juristic person, consideration must be given as to whether such transfer includes appropriate security measures and adequate standards for personal data protection.
3) In the event that a government agency or authority requests access to personal data by referring to any law, regulation, or order with which the Company is required to

comply, the responsible person may permit access to such personal data only where there is at least one of the following: a legal provision, order, or formal written notification issued under lawful authority. In cases other than these, the Company may be liable under the law for permitting access to or disclosing such data without a legal obligation, except where such disclosure is required for the Company's compliance with legal obligations, in which case the Company is legally required to act accordingly even without a request

5. Cross Border Data Transfer Policy

To ensure that personal data transfers comply with personal data protection laws, the transfer of personal data to destination countries or international organizations must be secure. The Company may consider the following options:

1) Transfer personal data to destination countries or international organizations that have adequate standards of personal data protection. The Company shall transfer personal data only to countries having personal data protection policies for such transfers that have been reviewed and certified by the Personal Data Protection Committee Office.
2) Establish agreements in one of the following forms:

- Binding Corporate Rules that have been reviewed and certified by the Personal Data Protection Committee Office.
- Agreements made in accordance with Standard Data Protection Clauses
- Code of Conduct

3) In cases where the options under Items 1 and 2 cannot be applied, personal data may still be transferred abroad under the following circumstances:

- The transfer is carried out in compliance with the law.
- Consent has been obtained from the data subject after informing the data subject of the inadequate standards of personal data protection in the destination country or receiving international organization.
- The transfer 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.
- The transfer is carried out pursuant to a contract between the personal data controller and another person or juristic person for the benefit of the data subject.

■ The transfer is necessary to prevent or suppress danger to the life, body, or health of the data subject or another person where the data subject is incapable of giving consent at that time.

■ The transfer is necessary for carrying out activities in relation to substantial public interest.

4) If the personal data protection measures of the destination country or receiving international organization are deemed inadequate, the matter shall first be submitted to the Personal Data Protection Committee Office for determination.

6. Binding Corporate Rules

The Company may transfer personal data within the same group of undertakings or affiliated business group for joint business operations, even where the destination country or international organization has not yet been declared by the Office of the Personal Data Protection Committee as having adequate standards of personal data protection, provided that such transfer of personal data complies with the policy on personal data protection for the transfer of personal data to personal data controllers or personal data processors located abroad and within the same group of undertakings or affiliated business group for joint business operations ("Group Members"), or Binding Corporate Rules ("BCR"), which have been reviewed and certified by the Office of the Personal Data Protection Committee. Such policy must contain at least the following details:

1) It shall be legally binding upon and enforceable against all Group Members, including employees and staff within the group of undertakings ("Group Members").
2) It shall guarantee enforceable rights of data subjects whose personal data are being processed.
3) The BCR shall contain at least the following elements:

3.1 Details of the structure and contact channels of the Group Members.

3.2 The personal data or categories of personal data to be disclosed, including details of the types of personal data, methods and purposes of processing personal data, categories of data subjects, and destination countries or international organizations receiving the personal data.

3.3 The legally binding effect of the BCR both within and outside the group of undertakings.

3.4 The application of general data protection principles, such as Purpose Limitation, Data Minimization, Limited Storage Periods, Data Quality, Data Protection by Design and by Default, Lawful Basis for Processing, Processing of Special Categories of Personal Data under Section 26 of the Personal Data Protection Act B.E. 2562 (2019), measures to ensure data security, and requirements in respect of onward transfers to bodies not bound by the Binding Corporate Rules.

3.5 BCR The rights of data subjects relating to the processing of personal data and the channels for exercising such rights, including the right to lodge complaints with the Office of the Personal Data Protection Committee and to initiate legal proceedings before a competent court, the right to remedies, and the right to compensation arising from violations of the BCR.

3.6 Acceptance of liability by the personal data controller or personal data processor that is a member of the corporate group and located in Thailand in the event of a BCR violation by a member of the corporate group located outside Thailand. The personal data controller or personal data processor shall not be liable in whole or in part if it can prove that the relevant corporate group member was not responsible for the event causing the damage.

3.7 Notification of the contents of the BCR (in particular Clauses 3.4 - 3.6) to data subjects in addition to the information required under Sections 23 and 25 of the Personal Data Protection Act B.E. 2562 (2019).

3.8 Duties of the Data Protection Officer (“DPO”) appointed under Section 41 of the Personal Data Protection Act B.E. 2562 (2019), or any person or juristic person assigned to monitor compliance with the BCR by members of the corporate group, including training and complaint handling.

3.9 Complaint handling procedures

3.10 Internal mechanisms within the corporate group for ensuring compliance with the BCR, which shall include at least the following elements: Data Protection Audits and methods for ensuring corrective actions to protect the rights of data subjects. The person assigned under Clause 3.8 (DPO) and the committee of the corporate group members shall be informed of the audit results, and the Office of the Personal Data Protection Committee shall be able to review such audit results.

3.11 Mechanisms for reporting and recording amendments to the contents of the BCR and reporting such amendments to the Office of the Personal Data Protection Committee.

3.12 Mechanisms for cooperating with the Office of the Personal Data Protection Committee in ensuring compliance with the BCR by members of the corporate group, such as making audit results available for inspection by the Office of the Personal Data Protection Committee.

3.13 BCR Mechanisms for reporting to the Office of the Personal Data Protection Committee any legal requirements applicable to members of the corporate group located in the destination country that may significantly affect the safeguards provided under the BCR.

3.14 จั Provision of appropriate personal data protection training to employees or persons who regularly or continuously access personal data.

4) In addition to the BCR, the Company may adopt other appropriate safeguards capable of protecting the rights of data subjects as may be prescribed by the Office of the Personal Data Protection Committee, including Standard Contractual Clauses, Codes of Conduct, or Certification Mechanisms. These serve as conditions enabling the Company to transfer personal data to destination countries even where such countries do not have adequate standards of personal data protection. The Company may adopt the approaches under Clauses 4.1 to 4.3 as follows:

4.1 Standard Data Protection Clauses

The Company adopts Standard Contractual Clauses to ensure that personal data is transferred appropriately for the provision of services, including maintaining standards and improving services in compliance with the law. Such clauses must specify contractual obligations regarding the transfer of personal data abroad, including cross-border data transfers, whereby data subjects are able to exercise their rights in relation to the transfer of personal data to foreign entities.

4.2 Code of Conduct

The Company shall transfer personal data only where the recipient has agreed to comply with a code of conduct approved by the competent authority. Such code of conduct, which specifies the obligations of foreign personal data controllers or personal data processors, must contain details of appropriate safeguards for protecting the rights of data subjects whose personal data is processed and transferred. Such code of conduct must also be directly enforceable by data subjects. The Company shall adopt a Code of Conduct based on the principles of good corporate governance, integrity, and ethics in business operations, with transparency, accountability, and

awareness of responsibilities toward all stakeholders, to ensure appropriate personal data protection in compliance with personal data protection laws.

4.3 Certification Mechanism

The Company shall apply certification mechanisms recognized by the Office of the Personal Data Protection Committee together with binding and enforceable commitments by foreign personal data controllers and personal data processors to implement appropriate safeguards regarding the rights of data subjects, to demonstrate that adequate protection exists for international transfers of personal data.

This Policy shall be effective from 26 July 2022 onwards.

_____

(Mr. Marote Vananan)

Chairman of the Board

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