primo
SERVICE SOLUTIONS

Third Parties and Cross Border Data Transfer Policy

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 and Objectives

The purpose of this **Policy on Disclosure of Personal Data to Third Parties and Cross-Border Transfer of Personal Data** is as follows:

1. To establish the principles governing the disclosure of personal data to third parties (external organizations) and the transfer of personal data to foreign countries or international organizations.
2. To define the criteria and protective measures for the disclosure of personal data to third parties (external organizations) and the transfer of personal data to foreign countries or international organizations.

2. Scope

2.1 Geographical Scope

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

2.2 Scope of Application

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

3. Definitions

For the purposes of this Policy on Disclosure of Personal Data to Third Parties and Cross-Border Transfer of Personal Data, the following terms shall have the meanings set forth below.

Personal Data Protection Law	Refers to the Personal Data Protection Act B.E. 2562 (2019), as amended from time to time, including all applicable laws, regulations, rules, notifications, and related orders.
Processing of Personal Data	Refers to any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, including the collection, recording, organization, structuring, storage, alteration or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data.
Third-Party Data	Refers to information in any form, whether electronic or non-electronic, that is received from or held by the Company's business partners or other third parties.
Personal Data	Refers to any information relating to an individual that enables the identification of such individual, whether directly or indirectly, but excluding information relating specifically to deceased persons, as defined under Section 6 of the Personal Data Protection Act B.E. 2562 (2019). Examples include a person's name, surname,

	email address, photograph, fingerprint, national identification number, which can directly identify an individual, as well as location data or cookies, which may indirectly identify an individual.
Data Subject	Refers to an individual who can be identified, directly or indirectly, by personal data.
The Company	Refers to the group of companies under 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 & Residence Management Co., Ltd.
Third Parties	Refers to any natural person, juristic person, government office, government agency, or any other person, excluding the Data Subject, the Company, the Data Processor, and any person authorized by the Company or by the Data Processor to process personal data directly.
Data Controller	Refers to a person or legal entity having the authority to make decisions regarding the collection, use, or disclosure of personal data.
Data Processor	Refers to a person or legal entity that processes personal data on behalf of, or under the instructions of, the Data Controller.

4. Third-Party Personal Data Disclosure Policy

The Company may disclose personal data to external organizations in accordance with the following principles:

1. Where personal data is to be disclosed to vendors, business partners, subsidiaries, and/or external service providers, such disclosure may only be made if the relevant recipient has been identified in the Company's Data Inventory (Record of Processing Activities). Where the recipient is not specified in the Data Inventory, prior approval must be obtained from the Data Protection Officer (DPO) before any disclosure is made. The DPO shall assess the lawful basis for processing and ensure that the disclosure complies with the applicable Personal Data Protection Law.
2. Where personal data is transferred to a juristic person, the Company shall ensure that the recipient has implemented appropriate information security measures and maintains an adequate standard of personal data protection.
3. Where a government authority or other competent public authority requests access to personal data by citing applicable laws, regulations, or official orders with which the Company is legally required to comply, the responsible personnel may disclose such personal data only where there is, at a minimum, a legal provision, court order, official order, or formal written request issued under lawful authority. In all other circumstances, the Company may be subject to legal liability if it discloses personal data without a lawful basis. This restriction shall not apply where the disclosure is necessary for the Company to comply with its legal obligations, in which case the Company shall fulfill such obligations even in the absence of a formal request.

5. Cross-Border Personal Data Transfer Policy

To ensure that cross-border transfers of personal data comply with the Personal Data Protection Law, the Company shall ensure that any transfer of personal data to a destination country or international organization is carried out securely and in accordance with one of the following mechanisms:

1. Transfer to countries or international organizations providing an adequate level of personal data protection

The Company may transfer personal data to a destination country or international organization that provides an adequate level of personal data protection as recognized and certified by the Personal Data Protection Committee (PDPC).

2. Implementation of appropriate safeguards

Where applicable, the Company may rely on one or more of the following safeguards:

- Binding Corporate Rules (BCRs) approved by the Personal Data Protection Committee (PDPC);
- Standard Data Protection Clauses (SDPCs) or other approved standard contractual clauses;
- An approved Code of Conduct governing personal data protection.

3. Transfer under specific legal exceptions

Where the mechanisms described in Sections 1 and 2 cannot be applied, the Company may transfer personal data outside Thailand under any of the following circumstances:

- The transfer is required by law.
- The Data Subject has provided explicit consent after being informed that the destination country or international organization may not provide an adequate level of personal data protection.
- 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 necessary for the performance of a contract between the Data Controller and another natural 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 the performance of a task carried out in the public interest.

4. Where the destination country or international organization does not provide an adequate standard of personal data protection, and none of the mechanisms or exceptions above apply, the Company shall seek a determination or approval from the Personal Data Protection Committee (PDPC) before proceeding with the transfer.

6. Binding Corporate Rules (BCR)

The Company may transfer personal data within its group of companies or affiliated business entities for the purpose of conducting joint business operations, even where the destination country or international organization has not been recognized by the Personal Data Protection Committee (PDPC) as providing an adequate level of personal data protection. Such transfers may be carried out where they are made in accordance with the Company's **Binding Corporate Rules (BCR)** governing the transfer of personal data to data controllers or data processors located overseas within the same group of companies or affiliated business entities (the "Group Members"), provided that such BCR have been reviewed and approved by the PDPC.

The Binding Corporate Rules shall include, at a minimum, the following:

1. Be legally binding on, and enforceable against, all Group Members, including their employees and personnel.
2. Ensure enforceable rights for Data Subjects whose Personal Data are processed.
3. Include at least the following elements:

3.1 Details of the organizational structure and contact information of all Group Members.

3.2 The categories of Personal Data or sets of Personal Data to be transferred, including the types of Personal Data, the methods and purposes of processing, the categories of Data Subjects, and the destination countries or international organizations receiving the Personal Data.

3.3 The legally binding nature of the BCR, both internally and externally, among the Group Members.

3.4 The application of fundamental data protection principles, including:

- 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)
- Security Safeguards
- Requirements in Respect of Onward Transfers to Bodies Not Bound by the Binding Corporate Rules

3.5 The rights of Data Subjects in relation to the processing of Personal Data, including procedures for exercising such rights, the right to lodge complaints with the Personal Data Protection Committee, the right to bring legal proceedings before a competent court, and the rights to remedies and compensation arising from any violation of the BCR.

3.6 Acceptance of liability by the Data Controller or Data Processor established in Thailand where a breach of the BCR is committed by a Group Member located outside Thailand. Such liability may be limited or excluded only where it can be demonstrated that the overseas Group Member was not responsible for the event giving rise to the damage.

3.7 Notification of the contents of the BCR (particularly Clauses 3.4–3.6) to Data Subjects in addition to the privacy notices required under Sections 23 and 25 of the Personal Data Protection Act B.E. 2562 (2019).

3.8 The duties of the Data Protection Officer (DPO) appointed under Section 41 of the Personal Data Protection Act B.E. 2562 (2019), or any designated individual or legal entity responsible for monitoring compliance with the BCR, conducting training, and handling complaints.

3.9 Complaint handling procedures.

3.10 Internal compliance mechanisms to ensure adherence to the BCR, including at least:

- Data Protection Audits;
- Procedures to ensure corrective actions for protecting the rights of Data Subjects;
- Oversight by the designated DPO and the governing body of the Group Members; and
- Availability of audit results for inspection by the Personal Data Protection Committee.

3.11 Procedures for reporting and recording amendments to the BCR and notifying such amendments to the Personal Data Protection Committee.

3.12 Mechanisms for cooperation with the Personal Data Protection Committee to demonstrate compliance with the BCR, including making audit results available for review.

3.13 Procedures for notifying the Personal Data Protection Committee of any legal requirements applicable to Group Members in the destination country that may materially affect the safeguards provided under the BCR.

3.14 Appropriate personal data protection training for employees or personnel who regularly or continuously access Personal Data.

4. In addition to the BCR, the Company may adopt other appropriate safeguards recognized by the Personal Data Protection Committee to protect the rights of Data Subjects. These may include Standard Contractual Clauses, Codes of Conduct, or Certification Mechanisms, which permit the transfer of Personal Data to destination countries that do not provide an adequate level of data protection. The Company may adopt one or more of the following safeguards:

4.1 Standard Data Protection Clauses

The Company may implement Standard Contractual Clauses (SCCs) to ensure that Personal Data transferred internationally receives an appropriate level of protection. Such contractual

arrangements shall establish binding obligations governing cross-border transfers of Personal Data and enable Data Subjects to exercise their rights with respect to such transfers in accordance with applicable law.

4.2 Code of Conduct

The Company may transfer Personal Data where the recipient has agreed to comply with an approved Code of Conduct endorsed by the competent authority. Such Code of Conduct shall establish the obligations of overseas Data Controllers or Data Processors and include appropriate safeguards to protect the rights of Data Subjects whose Personal Data are processed and transferred internationally. The Code shall be directly enforceable with respect to Data Subjects. The Company is committed to conducting its business in accordance with the principles of good corporate governance, integrity, transparency, accountability, and responsibility toward all stakeholders, while ensuring compliance with applicable personal data protection laws.

4.3 Certification Mechanism

The Company may rely on a Certification Mechanism recognized by the Personal Data Protection Committee, together with legally binding and enforceable commitments made by overseas Data Controllers or Data Processors to implement appropriate safeguards for the protection of Data Subjects' rights. Such certification shall demonstrate that adequate safeguards are in place for the international transfer of Personal Data in accordance with internationally accepted standards.

_____

(Mr. Maroj Wananan)

Chairman of the Board of Directors

Primo Service Solutions Public Company Limited