CONTROLLED COPY

Document No: POL-ORD-0010
Revision No: 00
Effective Date: 22 February 2023
Classification: UNRESTRICTED

PERSONAL DATA PROTECTION POLICY

TABLE OF CONTENTS

1. Introduction

1.1. Purpose

Theta Edge Berhad ("**Theta**") and its subsidiaries (collectively the "**Company**") are committed to complying with the Personal Data Protection Act 2010 of Malaysia ("**PDPA**"). This Personal Data Protection Policy ("**Policy**") contains the requirements and standards listed out in PDPA. The Policy focuses on the processing of personal data in commercial transactions and zero tolerance on personal data breach.

The purpose of this policy is to protect the Company's interest due to infringement of PDPA which could amount to a fine up to RM500,000.00 and 3 years imprisonment or 4 times of the Company's turnover which may be applicable based on the discretion of the relevant authority.

1.2. Objective

The Policy's objective is to serve as a point of reference and is mandatory for the employees, departments and/or third party that are involved in dealing with personal data to comply with including any additional requirements listed in PDPA. When in doubt, the Business Unit is required to consult Organisation Resilience department for clarification.

1.3. Scope

This Policy shall comprise of the **Seven (7) Principles** stipulated in PDPA and guidelines as below:

1) General Principle;
2) Notice & Choice Principle;
3) Security Principle;
4) Disclosure Principle;
5) Retention Principle;
6) Data Integrity Principle; and
7) Access Principle.

1.3.1. General Principle

1.3.1.1. Personal data shall not be processed unless:

a) has obtain a single consent for specific transaction;
b) for a lawful purpose directly related to the commercial transaction between Data User and Data Subject;
c) necessary for, or directly related to the transaction; and
d) the data is adequate and not excessive for the transaction.

1.3.2. Notice & Choice Principle

1.3.2.1. The Personal Data notice is to be in writing and in dual language, national language and English provided by the Data User to a Data Subject in compliance with Section 7 of PDPA.

1.3.2.2. This principle prohibits a Data User from disclosing the personal data of a Data Subject:

a) for any other purpose than the transaction requirement; and
b) to any other parties which is not related to the transaction unless it acts as a Data Processor or agents that acts on behalf of the Data User.

However, disclosure of personal data is permitted where:

a) consent has been given by the Data Subject;
b) the disclosure is necessary to prevent or detect crime, or for the purpose of investigations;
c) the disclosure is required or authorized by law or order of the court;
d) the Data User had acted under the reasonable belief that they have a legal right to disclose the data to another person;
e) the Data User had acted under the reasonable belief that they would have received the consent of the data subject if the Data Subject had known of the disclosure and the circumstances of such disclosure; or
f) the disclosure was justified as being in the public interests in circumstances as determined by the Minister.

A list of authorized third-party disclosures must also be kept by the Data User, and such a list may be requested by the Commissioner or inspecting officer during an inspection.

1.3.3. Security Principle

1.3.3.1. The Company shall take the necessary measures to protect the personal data collected including the following:

a) safeguarding the data access to prevent any potential threat for personal data breach that would result to data loss, misuse, modification, or unauthorized or accidental access, disclosure, alteration, or destruction;
b) personal data is stored at a secured place or location predetermined by the Company;
c) any security measures incorporated into any IT equipment in which the personal data is stored;
d) the measures taken for ensuring the reliability, integrity, and competence of the personnel who is authorized to access the personal data;
e) Implement backup and recovery systems by using the latest antivirus software, implementing a scheduled malware monitoring, and scanning operating systems to prevent attacks on electronically stored data;
f) the transfer of personal data using removable media devices and cloud computing services is not allowed except with the written approval from the authorized personnel and proper recording of the activity is done periodically;
g) to enter into a contract with Data Processors who process personal data on behalf of the Data User;
h) conduct awareness programs for all relevant personnel;
i) In respect of physical processing, the transfer of personal data using conventional methods such as through post, by hand, fax, or others must be recorded; and
j) to ensure that all used paper, printed documents, or other documents which clearly shows personal data must be properly destroyed.

1.3.4. Disclosure Principle

No disclosure of personal data is allowed other than for the purpose of carrying out the transaction to any party other that has been authorized by the Company to process the personal data.

1.3.5. Retention Principle

1.3.5.1. The personal data **must not be retained longer than necessary** for the fulfilment of the transaction process and requires the Data User to destroy or permanently delete all personal data according to the requirement of the Document Control Policy.

1.3.5.2. However, the Company shall retain the personal data for a longer period following the regulatory and statutory requirement. For example:

1) Section 245 (3) Companies Act 2016: accounting records/employee personal file to be retained for 7 years;
2) Income Tax Act: employee pay history to be retained for 9 years; and
3) Any other respective Acts established in Malaysia.

1.3.6. Data Integrity Principle

Data User is required to take reasonable steps to ensure that the Data Subject's personal data is accurate, complete, not misleading and kept up-to-date for the purpose of the transaction.

1.3.7. Access Principle

1.3.7.1. The Data Subject may request for access to the personal data by following the methods below:

1) By accessing the portal; -
   www.sakupay.my

2) By emailing the form: -
   support@sakupay.my

3) By calling our call centre: -
   +603 6043 0000

1.4. Target Audience

This Policy applies to staff of Theta, customers and any third party that is involved in business dealing and commercial transaction that handles personal data.

1.5. Review and Improvement

This document should be reviewed yearly or whenever there is a change in PDPA 2010 or any laws in relation to Personal Data in the future.

1.6. Definitions

1.6.1.1. **Adequate**: Information taken is enough or sufficient for the purpose of collecting the data. To measure by looking at the nature and reason for collecting the data.

1.6.1.2. **Authorized personnel:** The person nominated and authorized by the Management Committee known as the Data Protection Officer ("DPO").

1.6.1.3. **Commercial transactions/Transaction**: Any transactions of a commercial nature, whether contractual or not which includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking, and insurance but does not include Credit Reporting agency under Credit Reporting Agencies Act 2010.

1.6.1.4. **Commissioner**: Commissioner in the Department of Data Protection under the Ministry of Communications and Multimedia.

1.6.1.5. **Data Controller/Data User**: a person who either jointly, alone or in common with other person who process the personal data or has

control over, or authorises the processing of any personal data, but does not include a data processor.

1.6.1.6. **Data processor**: other than an employee of the data user, who processes the personal data solely on behalf of the data user and does not process the personal data for any of their own purposes.

1.6.1.7. **Data subject**: An individual who is the subject of the personal data.

1.6.1.8. **Personal data**: Three conditions must be fulfilled for data to be considered as personal data under the PDPA 2010:

a) It is in respect of commercial transactions which are processed wholly or partly;
b) Information processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
c) Recorded with the intention that it should be wholly or partly processed by such equipment or be recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; and
d) Must relate directly or indirectly to a data subject who is identified or identifiable from the information or other information in the possession of the data user.

Personal data covers the usual types of personal information collected in a day-to-day transactions, for example, name, address, telephone number, email address, banking details, and photographs.

1.6.1.9. **Sensitive data**: Any personal data consisting of information as to the physical or mental health or condition of a data subject, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, sex life, sex orientation and race;

Health data will fall under sensitive personal data under 'physical or mental health'.

Biometric data will fall under sensitive personal data under 'physical condition of the data subject'.

1.6.1.10. **Third Party/Parties:** A relevant person in relation to a Data Subject, a Data Processor; or an authorized person in writing by the Data User to process the personal data under the direct control of the Data User

1.7. Roles and Responsibilities

The table indicates the role and responsibilities of the relevant function and stakeholders:

Employee	Under the Company's employment, permanent/non-permanent employees (of all grades) shall be responsible for following the Policy.
Individual Departments	Departments that deals with individual personal data will be responsible to comply with the PDPA requirement.
ORD	ORD and the appointed DPO shall be responsible for the upkeep of this Policy.

2. Records

Description of Records	Form Number	Responsibility
Human Capital PDPA form		Human Capital