



S Hotels and Resorts Public Company Limited

Personal Data Protection Policy

Confidential

Version 1.0, May 2020

Table of Contents

1.	Introduction	3
2.	Objective	3
3.	Definition.....	3
4.	Roles and Responsibilities	5
5.	Scope of the Policy.....	5
6.	Content of the Policy	5
6.1.	Collection, Use, or Disclosure of Personal Data	5
6.2.	Cross Boarder Transfer of Personal Data	6
6.3.	Data Subject Rights.....	7
6.4.	Storage, Retention Period, and Disposal of Personal Data.....	7
6.5.	Data Breach Incident/Data Subject Rights Request Management	7
6.6.	Data Protection Impact Assessment: DPIA.....	8
7.	Policy Review and Management.....	8
8.	Violation of the Policy	8

1. Introduction

S Hotels and Resorts Public Company Limited (“SHR”) has created this personal data protection policy (“Policy”) to set the appropriate standard of personal data protection, in alignment with The Personal Data Protection Act B.E. 2562 (2019) of Thailand (“Thai PDPA”) and The General Data Protection Regulation (EU) 2016/679 (“GDPR”).

2. Objective

- To be used as a policy for any business operations related to personal data; including collection, use, or disclosure of personal data, data subject rights, storage and disposal of personal data, and data breach incident management.
- To determine the scope, authority, and responsibilities of Data Protection Officer (DPO) Steering Group, in accordance with Thai PDPA and GDPR.

3. Definition

Any text or word states in this Policy is to have the following meaning; unless such statements can be shown or explained otherwise.

Words	Meanings
Person	Natural person
Personal Data	<p>Any information relating to a Person, which enables the identification of such Person, whether directly or indirectly.</p> <p>Personal Data:</p> <ul style="list-style-type: none"> • Identity Data: data about natural person which can be used to identify specific individual, whether by a direct or an indirect mean such as name, surname, date/ month/ year of birth, gender, national ID number, passport number, driver's license number, passport number, marital status, and etc. • Contact Data: data such as email address and phone number. • Sensitive Data: data such as ethnicity, race, political opinions, culture, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, and biometric data. • Financial and Transaction Data: data such as bank account number, credit and debit card number, monthly income, payment information, and etc. • Technical and Usage data: data such as IP address, login information, website browsing information, cookie ID, device types and settings, platforms, and other technologies used to access SHR website. • Profile Data: data such as username and password, purchase history, interests, likes, and information from survey responses.

	<ul style="list-style-type: none"> • Marketing and Communication data: data such as data subjects' preferences in receiving marketing materials from SHR and from third party. This also include contact information data subjects have SHR, such as tape record when contact is made via contact center or from other social media channels. • Employment and Education Data: data such as employee ID number, employment history (including job titles, work history, and training records), education background, recruitment information (such as CV and cover letter), images, salary and etc. <p>Personal data excludes:</p> <ul style="list-style-type: none"> • Deceased person data • Business contact information such as juristic person's phone number and juristic person's address • Anonymized data which cannot be used to identify a specific individual
Personal Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Controller	Data controller means a person or a juristic person which having the power and duties to make decisions regarding the collection, use, or disclosure of the personal data.
Data Processor	Personal data processor means a person or a juristic person who operates in relation to the collection, use, or disclosure of the personal data pursuant to the orders given by or on behalf of a data controller, whereby such person or juristic person is not the data controller.
Data Subject	Data subject refers to any individual person who can be identified, directly or indirectly, via a personal data; including employees, customers, business partners, vendors and suppliers, visitors, and any other persons.
Third Party	Person, juristic person and/or other party that SHR discloses, receives, or transfers personal data to. For example, outsourcing service providers, consulting and law firms, vendors, telemarketing companies, co-brand partners, correspondent banks, recruitment agencies.
Office of the Personal Data Protection Committee	Government agencies responsible and overseeing the personal data protection.
Data Protection Officer /DPO Working Team: DPO	Data Protection Officer (DPO) or DPO working team of the Company.
Data Protection Officer (DPO) Steering Group	Personal Data Protection Committee carry out direction and guidance for decision making on the protection of personal data.

4. Roles and Responsibilities

SHR has established a regulatory framework for business operations in accordance with this policy as follows:

Department/Personnel Performing Tasks	Roles and Responsibilities
Data Protection Officer (DPO) Steering Group	Provide guidance and direction in making decisions regarding personal data protection. For example, giving advices and processes to resolve and manage arising issues in relevant business field to personal data protection, receiving compliant form data subjects, processing special request from data subjects regarding their rights, and etc.
Data Protection Officer /DPO Working Team: DPO	Support SHR and its hotels and resorts personal data processing activities including; <ul style="list-style-type: none"> • Provide advisory and training services regarding personal data protection for SHR employees. • Review and monitor regulations' compliance. • Act as a coordinator to cooperate with regulatory agencies regarding personal data protection. • Review and revise the processes and documents relating to personal data protection. • Carry out duty in handling complaints. • Propose a policy review.

5. Scope of the Policy

This policy applies to executives and all employees from SHR departments where there is a collection, use, and disclosure of personal data controlled and processed by SHR, to ensure compliance with Thai PDPA and GDPR; this also applies to SHR properties (hotels and resorts), entities, and associate companies unless there is a policy which specified otherwise.

6. Content of the Policy

For compliance with regulations and requirement of Thai PDPA and GDP, SHR sets out Policy with details as states below.

6.1. Collection, Use, or Disclosure of Personal Data

6.1.1. SHR shall collect, use, or disclose personal data only as necessary and relevant to the clearly states purposes. Nonetheless, the collection and disclose of personal data done on behalf of the Company, the data have to be correct and complete and is not processed in a way that is inconsistent with stated purposes.

6.1.2. SHR can proceed to collect, use, and disclose personal data in scenarios as addresses below;

- To comply with the contract or purposes agreed between SHR and data subjects.
- To carry out SHR legal obligation or to exercise legal rights.
- To provide SHR with legitimate interest. For example, to handle internal management including disclosure of information within the same business group, in order to improve operation and service standard or to provide appropriate security and prevent unlawful activities.
- To perform SHR duty in carrying out a task in the public interest or in the exercise of official authority
- When SHR obtain consent form data subject; unless in the scenario where there is an exemption of consent request made under Thai PDPA, GDPR, or other relevant laws.

6.1.3. SHR will take any appropriate action to request for data subject's consent and/or inform them regarding privacy notice which address all SHR purposes relating to collection, use, or disclosure of personal data. For purposes not specified in the privacy notice, SHR must obtain consent from data subject prior to carrying out such processing activity in all cases (except when there is exemption according to Thai PDPA and GDPR or other relevant laws.) Nonetheless, consent request shall not be a condition to receive the Companies' services or products.

6.1.4. In the event that the data subject is a minor, SHR will proceed under the Thai PDPA and GDPR conditions and requirements for obtaining a minor's consent.

6.1.5. Prior to the disclosure of personal data to third parties, SHR shall arrange for the Data Processing Agreement (DPA) to be made with the processor who process personal data on behalf of SHR; in order to determine the scope and duty of personal data processing and assign responsibilities in personal data protection as states within this policy. This is to ensure that the processor comply with the agreement in the incident that any violations or data breach incident arise.

6.1.6. In the event that SHR receives personal data from other sources, such as from third parties, SHR will proceed in accordance with Thai PDPA and GDPR.

6.1.7. In the event where SHR receives request from third party to confirm that SHR has obtained consent from data subjects to collect, use, or disclose personal data to the third party, the business unit that receive such request must notify SHR legal team and the DPO; in order to ensure that the scope of the collection, use, or disclose of personal data is consistent with the requirements of this policy. If the request resurface on the property level, the General Manager shall be notified and escalate the communication to SHR DPO.

6.2. Cross Boarder Transfer of Personal Data

SHR shall not transfer personal data outside Thailand unless the personal data is protected with the same or higher standard of protection under this Policy, and/or;

- The data subject has consented to the transfer of personal data and the individual is notified regarding insufficient privacy protection regulation and measures of the destination country;
- The transfer is necessary for the performance of contract between SHR and the data subject or it is a requirement to fulfil individual's request prior to entering into a contract with the Company;
- The transfer is necessary for the performance of contract between SHR and a third party which is for the benefit of data subjects;
- Personal data is sent through a server which locates in a foreign country; however, the action must be done in accordance with the contract between the company and a persons or juristic persons for the benefit of the data subjects;
- The transfer is for legal compliance;
- The transfer is for preventing or suppressing a danger to life, body, or health of the data subject

or other people when the data subject is unable to give consent at that time;

- The transfer is necessary for the performance of a task carried out in the public interest;
- The transfer has to be made to SHR's business group or properties (hotels and resorts), entities, and associate companies in foreign country; in order to carry out business operation or conduct joint venture business. The transfer of personal data will be in accordance with the personal data protection policy regarding Binding Corporate Rules (BCR); such policy must be inspected and certified by the Office of the Personal Data Protection Committee.

In the event that SHR has necessity to send or disclose customers' personal data internationally, SHR shall create personal data protection agreement or contract with the contracting partner in that country.

6.3. Data Subject Rights

SHR encourages data subject who wish to request SHR to proceed with the exercise of data subject as clearly specified Thai PDPA and GDPR. Nonetheless, SHR has addressed details of data subject rights in the "Privacy Notice."

6.4. Storage, Retention Period, and Disposal of Personal Data

6.4.1. SHR shall retain personal data for as long as necessary to achieve the purposes of collection, use, and disclosure of personal data and for legal compliance. In the event that business relationship between SHR and data subject is over or the storage of such data is no longer required for legal compliance or business objectives, SHR will consider to properly store or dispose of personal data in accordance to the Retention and Disposal/Deletion Procedure.

6.4.2. SHR will ensure appropriate security measures for personal data; as well as a measure to protect customer confidentiality.

6.4.3. All of SHR employees have roles and responsibilities to ensure that the documents which contain personal data has appropriate storage and disposal measure, in accordance with the Retention and Disposal/Deletion Procedure.

6.5. Data Breach Incident/Data Subject Rights Request Management

6.5.1. Data subjects and any person who discover violation of personal data protection or data breach incidence can report and file a complaint via a channel addressed below

E-mail: contactus@shotelsresorts.com

6.5.2. All allegations shall be kept as confidential and submitted to the DPO to record the complaints and document any data breach incident.

6.5.3. If the incident affects the rights and freedom of an individual or may affect SHR reputation and lead to financial damage, the DPO shall proceeds as follows;

- Report the incident to the Personal Data Protection Committee, to assess possible risk and make decision regarding the violation on the necessity to notify the Office of the Personal Data Protection Commission and data subject.
- If it is found necessary, the DPO must report to the Office of the Personal Data Protection Commission within 72 hours of the incident.

6.5.4. If the violation has a high risk in affecting rights and freedom of data subjects, SHR shall to notify the data subject, as well as providing risk mitigation plans without delay.

6.6. Data Protection Impact Assessment: DPIA

SHR shall carry out risk assessment upon the processing activity that may result in a risk toward rights and freedom of an individual and provide appropriate security measure for the risk level, in order to comply with Thai PDPA and GDPR.

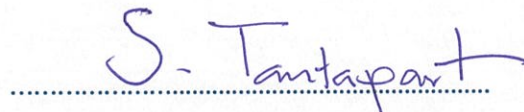
7. Policy Review and Management

SHR shall review and revise the Policy at least once every 1 year or when any significant change arises.

8. Violation of the Policy

Noncompliance with the Policy without SHR exemption is considered as a violation which can result in various disciplinary actions such as warning, imposing penalty, work suspension, termination of employment contract, and possibly face legal action.

Announced on 15 May 2020



(Mr. Sompong Tantapart)

Chairman of the Board of Directors

S Hotels and Resorts Public Company Limited