Personal Data Protection Policy
DAOL (THAILAND)

Objective

DAOL (THAILAND) PUBLIC COMPANY LIMITED, DAOL SECURITIES (THAILAND) PUBLIC COMPANY LIMITED, DAOL INVESTMENT MANAGEMENT COMPANY LIMITED, DAOL REIT MANAGEMENT (THAILAND) COMPANY LIMITED, DAOL LEND (THAILAND) COMPANY LIMITED, and any funds and trusts managed or established by DAOL (THAILAND) (hereinafter the policy called "**DAOL (THAILAND)**"). DAOL (THAILAND) is acknowledged of and prioritizes the personal data rights of customers, shareholders, directors, employees, and other DAOL (THAILAND) stakeholders. In order to ensure that personal rights are safeguarded in accordance with the laws governing the protection of personal data. Furthermore, the Board of Directors of each company within the DAOL (THAILAND) has given their approval for the enforcement of this policy. The objective is to establish transparent and appropriate standards, mechanisms, oversight, and administration for the protection of personal data.

1. Scope

The Personal Data Protection Policy applies to the companies within DAOL (THAILAND), the employees of DAOL (THAILAND), and individuals involved in the processing of personal data on behalf of the companies within DAOL (THAILAND), as outlined in the policy.

2. Definition

2.1 **Personal Data Processing** refers to any activity involving personal data, including but not limited to collecting, compiling, recording, organizing, structuring, updating, editing, storing, grouping, retrieving, using, disclosing by forwarding, publishing, or any action that makes the personal data available, combining, blocking, deleting, or destroying the data as well.

2.2 **Personal Data** refers to any information that can identify an individual, either directly or indirectly. However, according to the Personal Data Protection Act B.E. 2562 does not cover data related to deceased individuals. Examples of personal data include first and last names, email addresses, telephone numbers, and IP addresses.

2.3 **Sensitive personal data** refers to personal information that is considered sensitive and has the potential to be used for discriminatory purposes, as defined by the Personal Data Protection Act (B.E. 2562). Sensitive personal data refers to any information that could potentially affect the rights and freedoms of individuals whose personal data is involved. This includes details related to race, ethnicity, political opinions, religion, philosophy, sexual preference, criminal record, health information, disabilities, labor union membership, genetic or biological data, or any other personal data as specified by the personal data protection committee.

2.4 **Personal Data Subject** means a natural person whose personal data can identify that person, whether directly or indirectly.

2.5 **Personal Data Controller** means a natural person or juristic person who has the authority to make decisions regarding the collection, use, or disclosure of personal data.

2.6 **Personal Data Processor** means a natural person or juristic person who engages in the collection, use, or disclosure of personal data in accordance with the instructions or on behalf of the personal data controller. However, the natural person or juristic person who carries out such action is not the personal data controller.

3. Supervision of Personal Data Protection

3.1 DAOL (THAILAND) has implemented a personal data governance framework, to identify suitable approaches and measures for legal compliance, as outlines below:

(1) Establish a legally compliant organizational structure that clearly outlines the roles and responsibilities of the relevant agencies and operators involved. In order to establish a system for governing, controlling, and ensuring accountability, enforcement, and monitoring of measures to protect personal data, in accordance with the personal data protection policy of DAOL (THAILAND) and applicable laws.

(2) The Board of Directors is responsible for fulfilling the following roles, duties, and responsibilities:

(2.1) Ensure compliance with the law and this policy by overseeing the personal data governance structure and internal control of DAOL (THAILAND).

(2.2) Ensure effective supervision and monitoring of DAOL (THAILAND) to safeguard personal data and maintain compliance with applicable legal requirements.

(3) The Audit Committee has the duty to oversee and examine adherence to personal data protection laws, policies, and guidelines set forth by the Personal Data Protection Committee and the Data Protection Officer. Additionally, the internal audit aims to provide invaluable information for the development, enhancement, and adherence to personal data protection laws within DAOL (THAILAND).

(4) DAOL (THAILAND) has formed the Personal Data Protection Committee to oversee adherence to the Personal Data Protection Policy of DAOL (THAILAND) in accordance with the personal data protection law, as well as any amendments, policies, and/or regulations pertaining to personal data protection of DAOL (THAILAND). The committee's responsibilities and obligations are outlined in the Personal Data Protection Committee Charter.

(5) In accordance with the law and the Personal Data Protection Policy of DAOL (THAILAND), a personal data protection officer (“DPO”) will be appointed for DAOL (THAILAND). The DPO will have specific roles and responsibilities, which include the following duties:

(5.1) Regularly provide updates on the status of personal data protection measures to the Personal Data Protection Committee and provide suggestions for enhancing the personal data protection practices of DAOL (THAILAND) in accordance with legal requirements.

(5.2) Provide recommendations to the employees of DAOL (THAILAND) regarding legal compliance and the Personal Data Protection Policy.

(5.3) Inspect the operations of DAOL (THAILAND) to be in accordance with the law and the Personal Data Protection Policy.

In this regard, DAOL (THAILAND) has implemented measures to ensure an independent execution of the duties of the Personal Data Protection Officer. Furthermore, the DPO is safeguarded under the regulations of the Personal Data Protection Law, ensuring that they cannot be dismissed or terminated solely on the grounds of their compliance with the Personal Data Protection Law.

(6) The employees of DAOL (THAILAND) have roles, and responsibilities as follows:

(6.1) Ensuring compliance with the personal data protection policy of DAOL (THAILAND), as well as relevant guidelines, procedures, and other associated documents pertaining to the protection of personal data.

(6.2) Promptly informing their supervisors about any unusual events concerning personal data protection and any instances of non-compliance with the law and the personal data protection policy of DAOL (THAILAND).

3.2 DAOL (THAILAND) will be responsible for the development of policies, guidelines, procedures, and other necessary documents pertaining to the protection of personal data. In order to adhere to the legal requirements and the Personal Data Protection Policy of DAOL (THAILAND).

3.3 DAOL (THAILAND) intends to implement a policy management procedure to ensure ongoing adherence to the personal data protection policy of DAOL (THAILAND).

3.4 Employees of DAOL (THAILAND) will receive regular training or awareness from DAOL (THAILAND). To raise awareness among DAOL (THAILAND) employees of the value of protecting personal data and to make sure that all pertinent DAOL (THAILAND) employees have received training, are knowledgeable about and comprehend personal data protection, and are abiding by the company's personal data protection policy.

4. Personal Data Processing

4.1 DAOL (THAILAND) will process personal data in its capacity as a processor as well as a data controller. Processing must adhere to legality, equity, transparency, and consideration for the accuracy of personal data. Thus, in accordance with the purposes of processing, relevant laws, and business proposals of DAOL (THAILAND), DAOL (THAILAND) will determine the scope of processing personal data and the period of data storage. Furthermore, DAOL (THAILAND) will guarantee the appropriate security, confidentiality, and integrity of personal data.

4.2 DAOL (THAILAND) will have a clear procedure in place to guarantee that the personal data subject is notified of the purpose of collection, the specifics of data processing (privacy notices), and the request for consent is obtained in compliance with the law. This procedure will also include measures for supervision and inspection.

4.3 DAOL (THAILAND) is committed to implementing appropriate procedures and controls to effectively manage personal data throughout all stages. In order to adhere to the legal requirements and personal data protection policy of DAOL (THAILAND).

4.4 DAOL (THAILAND) is committed to establishing and upholding Records of Processing (RoP) to document different transactions and activities associated with the processing of personal data. In order to adhere to legal requirements. DAOL (THAILAND) will make necessary updates to the personal data processing record in the event of any changes to relevant items or activities.

4.5 DAOL (THAILAND) will establish a process to ensure the verification of personal data's accuracy. Including the provision of a system for rectifying personal data. Ensuring the implementation of appropriate technical and managerial measures to uphold the security of the collection. Ensure that personal data is used and disclosed in a manner that is suitable for the associated risks in each specific situation. In order to prevent unauthorized or unlawful loss, access, use, alteration, modification, or disclosure of personal information. Furthermore, DAOL (THAILAND) will conduct a review of technical and administrative measures when deemed necessary or in the event of technological advancements. In order to ensure the preservation of security in the process of collection, DAOL (THAILAND) will ensure that personal data is used and disclosed in accordance with applicable laws and regulations.

4.6 In the event that DAOL (THAILAND) submits, transfers, or permits others to use personal data, it will enter into agreements with the recipients or users of such personal data to establish rights and obligations in compliance with the law and DAOL (THAILAND)'s personal data protection policy.

4.7 In the event that DAOL (THAILAND) decides to submit or transfer personal data overseas, DAOL (THAILAND) will ensure compliance with all relevant legal obligations.

4.8 DAOL (THAILAND) will securely dispose of personal data once the designated period has elapsed. In compliance with the legal and business regulations of DAOL (THAILAND), it is required by law, such as anti-money laundering laws, to retain customer receipt documents for a period of 10 years starting from the termination of the customer relationship. This requirement also applies to periods not explicitly specified by law, DAOL (THAILAND) will establish the duration of storage as deemed necessary and suitable for the business proposes of DAOL (THAILAND).

4.9 DAOL (THAILAND) will conduct risk assessments and implement appropriate measures to mitigate risks and minimize the potential impacts associated with the processing of personal data.

5. The Rights of Personal Data Subject

DAOL (THAILAND) has implemented protocols to ensure compliance with legal requirements regarding the protection of personal data. These protocols include measures, channels, and methods for facilitating the exercise of individuals' rights, as well as procedures for denying such requests in accordance with applicable laws and regulations. In compliance with applicable laws and regulations, as well as any court

orders, or to prevent harm to the rights and freedoms of individuals who may be impacted. Recording and assessing responses to requests for the exercise of personal data rights.

6. Personal Data Security

6.1 DAOL (THAILAND) will implement appropriate safeguards to ensure the protection and security of personal information. This includes implementing measures to prevent the disclosure of personal data and unauthorized access to personal data.

6.2 DAOL (THAILAND) will provide the management of unforeseen circumstances concerning personal data, including the implementation of a Privacy Incident Management Policy and guidelines for addressing such incidents through an Incident Response Program, with the aim of effectively identifying and handling them. in a prompt and timely manner, with regards to any unusual events concerning personal data.

6.3 In the event of data leakage, which including the personal data is lost, accessed, used, changed, modified, or disclosed without proper permission or in violation of the law, DAOL (THAILAND) mandates the implementation of the following measures:

(1) In the event of a personal data breach, DAOL (THAILAND) will promptly notify the Office of the Personal Data Protection Committee within 72 hours of becoming aware of the incident. DAOL (THAILAND) has been granted an exception to the requirement of reporting incidents to the Office of the Personal Data Protection Committee. This exception applies only in situations where the violation does not pose a risk of impacting rights and individual freedom.

(2) As the data controller, DAOL (THAILAND) will promptly inform the data subject about their personal data incident. When DAOL (THAILAND) assesses data leakage as a significant threat to the rights and freedoms of individuals' personal data.

7. Personal Data Protection Supervision

7.1 DAOL (THAILAND) is committed to implementing a comprehensive follow-up procedure in the event of any changes in the law. DAOL (THAILAND) will continuously enhance our personal data protection measures to ensure the personal data protection measures are in compliance with the latest legal requirements.

7.2 DAOL (THAILAND) is committed to conducting regular reviews and enhancements of policies, guidelines, procedures, and other relevant documents pertaining to the protection of personal data. It is advisable to review and update the document at least once a year to ensure compliance with current laws and circumstances.

8. Penalty

Non-compliance with the Personal Data Protection Policy of DAOL (THAILAND) may lead to disciplinary measures. Including being subject to legal consequences as prescribed by the law.

9. Announcement and Review

No.	Subject	Writer	Approved By	The Date of Approval
1	Newly Developed	Data Protection Officer	The Board of Director	13 May 2020
2	Completely revision	Data Protection Officer	The Board of Director Meeting of DAOL LEND (THAILAND) COMPANY LIMITED No. 5/2023	6 November 2023
			The Board of Director Meeting of DAOL SECURITIES (THAILAND) PUBLIC COMPANY LIMITED No. 6/2023	7 November 2023
			The Board of Director Meeting of DAOL INVESTMENT MANAGEMENT COMPANY LIMITED No. 6/2023	8 November 2023
			The Board of Director Meeting of DAOL REIT MANAGEMENT (THAILAND) COMPANY LIMITED No. 7/2023	8 November 2023
			The Board of Director Meeting of DAOL (THAILAND) PUBLIC COMPANY LIMITED No. 7/2023	8 November 2023
3	There has been an amendment to the group companies and partner companies, namely DAOL DIGITAL PARTNER COMPANY LIMITED and WE Insurance Broker Co., Ltd., which have been removed from the DAOL (THAILAND).	Data Protection Officer	The Board of Director Meeting of DAOL LEND (THAILAND) COMPANY LIMITED No. 3/2024	4 November 2024
			The Board of Director Meeting of DAOL SECURITIES (THAILAND) PUBLIC COMPANY LIMITED No. 6/2024	5 November 2024
			The Board of Director Meeting of DAOL INVESTMENT MANAGEMENT	6 November 2024

No.	Subject	Writer	Approved By	The Date of Approval
			COMPANY LIMITED No. 6/2024	
			The Board of Director Meeting of DAOL REIT MANAGEMENT (THAILAND) COMPANY LIMITED No. 5/2024	6 November 2024
			The Board of Director Meeting of DAOL (THAILAND) PUBLIC COMPANY LIMITED No. 5/2024	6 November 2024

The Personal Data Protection Policy of DAOL (THAILAND)
will be in effect starting from 8 November 2024