Corporate Announcement of Thai Shimizu Company Limited

No. 1/2565

Re: Corporate Policy on Personal Data Protection

In recognition of the importance of lawful processing of the Personal Data in strict compliance with the relevant laws and regulations, the Board of Directors of Thai Shimizu Company Limited (the "**Company**") has approved and endorsed this Corporate Policy on Personal Data Protection (the "**Policy**") with an aim to establish the framework for a proper Personal Data processing to be implemented and institutionalized into all of the business operation of the Company that shall not be violating the relevant data subject's rights and shall comply with the Personal Data Protection Act B.E 2562 ("**PDPA**").

Clause 1 Policy Name and Effective Date

This announcement is named "Corporate Policy on Personal Data Protection" and shall become fully effective upon the announcement with the scope of application governing the personal data processing of all data subject that the Company is being engaged and is interacted by the Company, including customer, personnel, business partners, counterparties, service providers, any visitors entering the Company's premise, as well as the Company's shareholders and directors.

Clause 2 Definition and Principle of Personal Data Processing

2.1 The following key terms used on this Policy shall have the meaning as defined under the PDPA:

"**Personal Data**" means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased persons in particular

"**Sensitive Personal Data**" means any Personal Data that is sensitive and may cause any specific risk of unfair discrimination, including any Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Personal Data Protection Committee.

2.2 Key Principle of Personal Data Processing

The Company will process Personal Data with the lawful purpose and lawful basis of processing in strict compliance with PDPA, specifically the Company will ensure the processing of Personal Data only on the necessary basis, in particular, for the purpose to perform the duties between the Company and each data subject. The Company will also notify each data subject of purpose of data collection for acknowledgment and/or obtaining their consent in various forms as prescribed under PDPA as appropriate.

Clause 3 Manual and Guideline implementing this Policy

By virtue of this Policy, the Company may issue the detailed standard operating manual and guideline that would define in detail the procedures and guidelines to be implemented in order to assure the complete, accurate and comprehensive management of Personal Data protection in all aspects; provided that those manual and guideline shall have the same binding impact equivalent to this Policy.

Clause 4 Organization Structure for the Personal Data Protection Management and Monitoring

With the commitment to assure the governance, management and monitoring of the Personal Data protection being implemented in strict compliance with PDPA, the Company hereby establishes the following organization structure to serve such commitment:

4.1 The Company institutionalize the following 2 Lines of Defense organization structure in order to assure the full compliance in the management and monitoring of the Personal Data protection:

- 1st Line of Defense: Risk Owner refers to the chief or head of each internal department/business units of the Company being directly responsible for governing the Personal Data processing executed within their department/unit to assure the compliance and accuracy; and
- 2nd Line of Defense: Risk Control refers to the designated PDPA working teams to act as the focal point in monitoring and supervising the performance of Risk Owner and all the Personal Data processing executed by the Company. The Board of Directors will specifically and subsequently make the announcement on the structure, the powers and duties of such PDPA working teams in accordance with this Policy.

4.2 The Company commits to provide sufficient resources (in terms of system, manpower and financial aspects) to support the operation of each department/unit to ensure the compliance with this Policy.

Clause 5 Risk Assessment and Management for the Personal Data Processing

5.1 The Company hereby instructs that each department in the 1st Line of Defense undertakes the risk assessment of their Personal Data processing as one of the key elements in the Company's enterprise risk management regularly or every time there is any change in the Personal Data processing that has already been assessed. The 1st Line of Defense shall submit their risk assessment to the 2nd Line of Defense (the PDPA working teams) for verification, monitor and compilation into the Company's risk assessment on Personal Data processing.

5.2 Based on the risk assessment made, for any particular Personal Data processing activity being assessed of having high risk that may affect the fundamental rights and freedom of the data subject, particularly impairing the data subject's economic or society rights and benefits or resulting in the situation where the data subject would not be able to control their own personal data, the Company requires that each department/business unit shall prepare the Data Processing Impact Assessment and record it before the Company making final decision whether or not to proceed with such Personal Data processing activities.

5.3 The Data Processing Impact Assessment shall be executed and recorded in compliance with the following principles:

(1) the details of the relevant personal data processing activity shall be defined, clearly on the scope, objective and necessity for such activity;

(2) the consultation with the relevant stakeholders, including the data subject or the data processor, both internal and external, shall be undertaken;

(3) the assessment of the necessity and proportionality shall be recorded;

(4) risk assessment shall reflect the impact on the data subject's rights and freedom both on the likelihood and impact severity angles; and

(5) the assessment shall define the risk mitigation measures to be implemented.

Clause 6 Communication of the Policy

The Company gives high priority to the communication of this Policy and the implementing guideline to all the personnel of the Company by defining the communication policy to ensure the communication be made in all the communication channels on the regular basis and every time there is any material change in the Personal Data processing activities in the Company.

Clause 7 Management and Monitoring Mechanism

The Company establishes the management and monitoring mechanism for Personal Data protection under the following principles:

7.1 The Company designates that the 2nd Line of Defense (the PDPA working teams) to be the focal person having direct mandate and responsibility to regularly manage and monitor the performance of the whole Company to ensure compliance with the PDPA and the Policy by designing the regular monitoring plan. The PDPA working teams will report to the Board of Directors at least once a year or every time there is any material data breach within the Company that may affect the business or reputation of the Company.

7.2 In order to further assure the full compliance of the Personal Data processing undertaken by the Company in addition to the internal monitoring mechanism, if the Company may consider that it would be necessary to do so, the Company may appoint and engage the external auditor to conduct the Personal Data processing audit and submit the audit report to the Board of Directors from time to time as the Company may deem appropriate

7.3 In case of any non-compliance or Personal Data breach, the PDPA working teams shall be the focal unit being responsible for accepting all the breach notification and fact-finding. If there is any confirmed violation or breach committed by any personnel or employee of the Company, the PDPA working teams will report the Board of Directors to consider enforcing the appropriate disciplinary sanction on those personnel or employee pursuant to the disciplinary principles of the Company.

Clause 8 Record of Processing

The Company instruct that each department or business units as the 1st Line of Defense shall be responsible for preparing and updating the record of processing of all the Personal Data executed in their business operation regularly. The PDPA working teams shall monitor and guide the process of preparing the record of processing. This record of processing shall be used to determine the risk and define the legal basis for the Personal Data processing to be declared in the relevant privacy notice for each group of data subject.

Clause 9 Information Disclosure Policy

9.1 As the general rule, the Company has a clear direction that the Personal Data shall not be shared, sold, transferred or disclosed in any manner (collectively referred to as the "**Disclosure**") to any third party without the consent given by the relevant data subject, except in case that the Disclosure is required by laws or the contractual obligations that the Company may have with the relevant data subject; or such Disclosure is critical for the protection of the Company's legitimate interest; provided that that the Company shall disclose those Personal Data in strict compliance with Clause 9.2.

9.2 In case it is necessary to disclose the Personal Data to any third party as defined under Clause 9.1, the Company shall comply with the following protocols and measures:

- the disclosing department/unit shall assess the necessity for each specific Disclosure and shall assess the credential of the party to whom the Personal Data be disclosed to;
- each Disclosure shall be approved by the supervisor of each department/unit on the case-by-cases basis;
- each disclosing staff and department/unit shall assure that the Disclosure be made on the most secured communication channel as defined by the Company with the least risk on information security and shall avoid the disclosure via the personal communication channel that cannot be controlled;
- data processing agreement shall be executed between the Company and the receiving party where the terms and conditions on the rights and responsibility for the contracting parties shall be defined and the information security of the Personal Data disclosed shall be secured.

Clause 10 Data Retention Guideline

10.1 The Company define the Data Retention Guideline based on the necessity basis under the following framework and the Company shall notify the retention period for the Personal Data processing to the relevant group of data subject:

- in case any Personal Data shall be stored pursuant to the requirement of any laws, the retention period shall be set in consistent with the conditions set under such laws;
- in case any Personal Data shall be stored due to the necessity in reliance on the contractual relationship which the Company may have with the relevant data subject, the retention period shall be set for the period of time necessary for the Company to perform all of their contractual obligations or until the termination of the relevant agreement or relationship;

- in case any Personal Data shall be stored for the legitimate interest purposes, the retention period shall be set as sufficient to serve such specific purpose, for instance, retention period should be set for the prescription period in case any claim may be brought or for the period of time necessary for the Company's business purposes; provided that the key principles to be maintained is that the data subject rights shall not be impacted and the relevant data subject shall have the right to object to such Personal Data processing;
- in case any Personal Data is processed with the consent given, such Personal Data can only be processed with the consent given for the period of time until the consent is withdrawn which the data subject shall have the freedom to do so at any time;
- in case any Sensitive Personal Data is being processed, the Company shall take caution and implement the high standard management measures in processing Sensitive Personal Data and Sensitive Personal Data shall be destroyed immediately once there is no further necessity to process those data.

10.2 Once the retention period as determined pursuant to the principle defined has elapsed, the Company shall destroy or anonymize those Personal Data, both in the paper and electronic form, with the appropriate technic, in particular in case any Personal Data is stored in the devices (i.e. USB or computer), the Company shall use the best effort in properly destroying those Personal Data retained in those devices.

Clause 11 Information Security of the Personal Data

11.1 As the general rule, the Company has a clear direction that the Personal Data processing should be undertaken in electronic system where the access control and logging system can be put in place rather than the processing on paper. In case paper would need in the Personal Data processing, the Company makes a clear instruction: (i) on clear desk procedures to assure the information security contained on such paper; (ii) that any paper that contains Personal Data shall not be recycled or reused and shall be stored in locked cabinet(s) with the retention period labelled; and (iii) that any movement of the Personal Data recorded in paper shall be undertaken pursuant to the information security procedures defined.

11.2 The Company defines a clear framework for information security measures of the Personal Data to assure that there shall not be any unauthorized loss, access, use, amendment, revisions or disclosure of the Personal Data and, in particular:

- all Personal Data shall be stored in strict confidential and shall be classified as "Strictly Confidential" information;
- all Personal Data shall be assured of their integrity; and
- all Personal Data shall be assured of their availability.

11.3 The Company represents that the information security of the Personal Data shall be institutionalized into the organizational structure as well as the technical and physical measures under the key principles of role-based authorization matrix scheme.

11.4 The Company shall keep the logs for any access or modification of any Personal Data processing in all department/unit and aspects and designate that head of the department/business unit shall be responsible for monitoring the log of Personal Data being processed by the staff within their supervision on a regular basis; and the PDPA working teams shall monitor all the logs kept as necessary and appropriate.

11.5 All the Personal Data processing management and monitoring process shall be undertaken under the Maker-Checker framework and the efficiency of the management monitoring mechanism shall be reviewed on the regular basis.

11.6 In case Bring Your Own Device (BYOD) is permitted, the Company shall define a clear access control limitation for the use of such device to process any Personal Data in order to assure the information security under the key principle to limit the store of the Personal Data in BYOD to the minimum in order to avoid the potential data breach.

11.7 The Company defines a clear data recovery plan of the key Personal Data that shall run continuously in order to assure its availability and such data recovery plan shall be reviewed and tested at least once a year in order to assure that the comprehensive and accurate Personal Data is to be restored within the defined period of time.

11.8 The Company defines a clear monitoring and controlling mechanism to assure the information security of the Personal Data in case the third-party service provider is engaged, commencing from the selection process, documentation and agreement process and the access control monitoring process to assure the third-party service provider will only be entitled to access the Personal Data on the need-to-know basis and the third-party service provider shall maintain the same information security standard as the one defined by the Company. The department/business unit engaging such third-party service provider shall be responsible to monitor and control the full compliance of the respective service provider and in case of any default or non-compliance, the responsible department/unit shall consider imposing the sanction on the violating service provider immediately while assuring the business and service continuity of the Company.

Clause 12 Data Subject Rights

The Company acknowledges and respects the data subject rights over the Personal Data being processed by the Company and the Company commits to consider and respond to any data subject rights request in all circumstances within the reasonable timeline as prescribed under the applicable laws. The data subject rights include the following rights:

1. Right to request for access and a copy of Personal Data;
2. Right to request for data portability;
3. Right to object to the process of Personal Data being undertaken by the Company;
4. Right to request the Company to erase or destroy, or de-identify the Personal Data once the Personal Data is no longer necessary to be processed or when the data subject revokes his/her consent;

5. Right to request the Company to restrict the use of the Personal Data, in case the Personal Data shall be deleted, or such Personal Data is not necessary to be processed;
6. Right to withdraw consent that the data subject has given to the Company;
7. Right to request to rectify Personal Data;
8. Right to request the disclosure of the acquisition of Personal Data obtained without consent; and
9. Right to file a complaint in the event of violation of applicable laws.

Should each data subject has any questions or wish to rectify or erase the Personal Data or to exercise the aforementioned rights or contact the Company regarding the Personal Data issues or the Company's Personal Data Protection practices, please contact the Contact channel mentioned below.

If the data subject wishes to exercise any rights with regard to Items 1 to 9 set forth above, the data subject can submit a request to the Company via Contact channel mentioned below. Once the Company receives the data subject's request, the Company will examine the request in accordance with the conditions prescribed by law, complete the data subject's request, and notify the data subject of the result of the examination and completion of the request within 30 days from the date of receipt of all requests and supporting documents.

Please note that the Company shall retain its rights under the laws to reject the data subject's request in certain circumstances. If the Company decides to reject the data subject's request, the data subject will be notified of the reason for such rejection. The Company will try its best, also with considering technical capabilities, to answer the data subject's request on how the Company processes the Personal Data. However, if the data subject has unresolved concerns, the data subject can complain to the Company via the Contact channel mentioned below or proceed further to the authority officials as prescribed by the PDPA in case of the Company's infringement or non-compliance with the PDPA.

Clause 13 Management of the Personal Data Breach

13.1 The PDPA working teams shall be responsible for determining the policy and measures to be implemented in case of any potential Personal Data breach, in close coordination with the relevant department/business units. In case of any Personal Data breach, the PDPA working teams shall be the focal point who will receive the report and manage the breach at the first instance.

13.2 In case of any Personal Data breach, the PDPA working teams shall report such incidence firstly to the Board of Directors and prepare the report to be submitted to the Office of Personal Data Protection Committee within the framework of 72 hours upon the occurrence and to the affected data subjects at the earliest time possible.

13.3 After the successful resolution of the Personal Data breach, the PDPA working teams shall review and assess the root cause of such breach and prepare the report to the Boards of Directors for the future improvement of the measures to prevent future Personal Data breach.

Clause 14 **Review and Revisions of this Policy**

The Board of Directors shall review and improve this Policy by taking into consideration the report on the implementation of the plans and measures defined hereunder made by the PDPA working teams at least once a year or every time there is a material change in the Personal Data processing that the Company is undertaking in order to assure that the Policy will be up to date. The Company will notify the data subject of such change through the website at https://www.shimz-global.com/th/en/ and http://intranet.shimz.co.jp/global/bkk/.

Clause 15 **Contact Channel**

The data subject can contact the Company for any query or the exercise of any rights at:

Contact channel

Contact :	Thai Shimizu Co., Ltd. Unit 2301, 23rd Fl., Empire Tower, No.1, South Sathorn Road, Yannawa, Sathorn, Bangkok 10120, Thailand
Telephone number:	02-230-0333
Email:	th.pdpa@shimz.biz

Announced on May 25, 2022

Thai Shimizu Company Limited

廣瀬　学

Mr. Manabu Hirose
President