Personal Data Protection Policy

TTW Public Company Limited and its subsidiaries (the "Companies") are committed to protecting and respecting of your Personal Data and privacy under the Thai Personal Data Protection Act B.E. 2562, as possibly amended in the future, as well as other applicable laws and rules in Thailand (collectively "the PDPA"). The Companies conduct the Personal Data Protection Policy (the "Policy") and intend to protect your personal information that the Companies collect, use, or disclose during the course of business activities. The Companies have the obligations as indicated in any laws regarding the protection of Personal Data, privacy, data security, and personal rights.

Scope of this Policy

This Policy has the objectives for the collection, use, or disclosure of Personal Data; the types of Personal Data that the Companies may collect, use, or disclose; the intention to use of such Personal Data, the third parties the Companies may disclose, the collection and retention of Personal Data, how you can access or request changes to your Personal Data that is held by the Companies, and how you can complain if you think that the Companies have violated the applicable law on Personal Data protection.

Definitions

"**Company**" means TTW Public Company Limited.

"**Subsidiaries**" mean the firms that TTW Public Company Limited holds the shares and has the rights to control all management.

"**Companies**" or "We" (our/ ours) mean TTW Public Company Limited and its subsidiaries.

"**Personal Data**" means any information that relates, whether directly or indirectly, to an identified or identifiable person, or which can be used to distinguish or trace an individual's identity, whether by reference to such information alone, or when combined with other identifying information, but this excludes the data of dead persons.

"**Sensitive Personal Data**" means any information as specified in the Thai Personal Data Protection Act, as well as other applicable laws and rules, such as information about race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal backgrounds, health

information, disability, labor union information, genetic data, biometric data, or any other information that similarly affects the data subject.

"Processing" means the collection, use, or disclosure of Personal Data.

"Personal Data Controller" means any individual or legal entity authorized to make decisions concerning the collection, use, or disclosure of Personal Data.

"Personal Data Processor" means any individual or legal entity that processes the collection, use, or disclosure of Personal Data, in accordance with instructions, or on behalf of the Controller. Any person who performs the Processing is not considered a Controller.

1. Type of Personal Data that the Companies collect

The type of Personal Data that the Companies may collect depends on the nature of the activities and the means which are used to collect the Personal Data, which may include the following information:

1.1 Employees and Job Applicants

- Personally identifiable information, such as name, surname, address or contact details, gender, age, nationality, marital status, date of birth, and passport/ID Card number; identification information about your property, such as your car license number and bank account details, information about persons under your care, your travel information, such as your visa application, travel itinerary, and flight information, Sensitive Personal Data, such as your religious belief, health-related data, criminal record, convictions or proceedings (or alleged offenses), or any other information of a similar nature, and biometric data, such as face scans and fingerprints.
- Educational background and work experience, such as your school/university certificates, academic records, academic or language test results, certificates, and reference letters.
- Basic information about your work, such as your work contact details, employee identification number, position, job description, line of supervision, working hours, and the terms and conditions of your employment agreement.
- Information about your employment, such as your resume, military service, information obtained during job interviews, and references.

- Information relating to your benefits and remuneration, such as information about the payment of your salary and other benefits, your social security information, information about retirement and pensions, your provident fund information, tax information, information about third party beneficiaries.
- Information about your work efficacy, including work performance evaluation, the Companies' opinion about your work performance, feedback, information about work rules or complaints, annual leave/sick leave/absence records, health-related data, information about physical checkups, and workplace and safety information, including information about inspection and risk assessments.
- Equality and diversity information (only if you give consent), and audio/ visual information about you, if audio/ visual records are kept for any activities or disciplinary action purposes, or as evidence in an investigation.

1.2 Other Third Parties

- Personally identifiable information, such as your name and surname, ID card number, passport number, telephone number, email address, applications, postal address or other contact details, your birth date, nationality, occupation, photograph, biometric data, audio recordings and other information that required for risk assessment, including the personal data of your representative or authorized representative or your proxy.
- Audio/ visual information about you, if audio/ visual records are kept for any activities or security purpose.
- Health-related data and criminal records of any representatives who provide services to us, and information about the sale or provision of services by you.
- Payment information, such as your bank account number, bank account details, billing information, credit or debit card information, such as your credit or debit card number, and the name of the cardholder (if any).
- In cases where you use any of our websites or mobile applications, technical information, the Companies will collect the Personal Data such as the IP address and Cookies, and, in the case of mobile applications, the Companies will collect the Personal Data of your location and your mobile device.

1.3 Stakeholders

- Personally identifiable information, such as your name and surname, ID card number, passport number, telephone number, email address, applications, postal address or other contact details, your birth date, nationality, occupation, photograph, biometric data, audio recordings and visa application and travel itinerary.
- Audio/ visual information about you, if audio/ visual records are kept for any activities or security purpose.
- Financial status, such as your income, the source country of your income, your other sources of income, your sources of investment funds, the value of your personal property, your accounts, identification information about your property, such as your car license number, details relating to your bank accounts, bonds, certificates of deposit, bills of exchange, debentures, listed securities, and investment units, and your salary certificate.
- Educational background and work experience, such as your highest education level achieved, the institutions (and their countries) from which you obtained your education, the field(s) of your education, the year of your graduation, certificates, your finance-related educational background, your career, details about your work, the name of your company and the type of business, your position and department, the nature of your work, your responsibilities, the name of your secretary and his/her telephone number, or applications, your length of service to date, and your work experience.
- Legal offense record, such as records of anti-money laundering offenses, information about transaction suspension, involvement in any anti-money laundering scheme, or transaction rejections by any financial institution (if any), information about bankruptcy, information about any related legal entities, any information for the KYC process, information about risky businesses under anti-money laundering law, any criminal record from the government agencies / supervisory bodies.
- Information for investment assessment.
- Information about sales and purchase transaction and other transactions.
- Information about persons relating to any Stakeholder, such as his/her spouse, children, emergency contacts, his/her guarantor; persons who give consent on behalf of legal

representatives, guardians, and/or estate administrators; parents and/or legal representatives, grantors of powers at all levels, beneficiaries, and guarantors.

Any provision of your Personal Data is vulnerable. You may choose not to give any information that is requested by the Companies. However, the lack of such information may result in the Company's inability to provide you with certain products or services.

Some of the Personal Data collected by the Companies may be considered "Sensitive Personal Data." The Companies intend to collect Sensitive Personal Data only upon your consent, except the cases that the Companies collect such data under compliance of any applicable laws such as temperature, travel timeline and syndrome for the health-related purposes in case of outbreak of diseases in accordance with the Communicable Disease Act B.E. 2558 or relevant laws.

In cases your documents contain the Sensitive Personal Data and the Companies find it unnecessary to collect e.g. religious data in your ID card where you are free to cover such data before sending it to the Companies or the Companies will cover it.

2. The channel that the Companies collect the Personal Data

The Companies will collect your Personal Data through many possible channels such as your documents, Companies' website, application in devices or other channels.

Generally, the Companies collect your Personal Data directly from you, such as job application forms or any documents provided before becoming our personnel, director, or executive, forms or systems for registration as our service provider or vendor, our channels for receipt of information or our website, oral methods, such as by phone or through video/virtual conferences, emails or other communication channels, and through mobile applications which are made available by the Company or any related company.

In the event that the Companies collect your Personal Data from others rather than the sources you give, the Companies will notify you and ask your permission within 30 days from the collecting date except the exemption by the laws.

The Companies do not intent to collect the Personal Data of incapable persons. Therefore, if you are incapable, the Companies will need the prior consent from your rightful representative or guardian before collecting such data.

3. The objectives to process the Personal Data

The Companies collect your Personal Data for the following objectives:

3.1 Employees and Job Applicants

- For business administration and management, and the Company's operations.
- For human resource management, such as to assist employees with onboarding program, set plans, and perform acts regarding employment and training, promotion, job rotation and relocation of employees, and manpower allocation, etc.
- For employee identity verification or identification when accessing digital technology systems, and to examine usage of digital technology systems by employees, according to our IT policy.
- For other benefits regarding our business operations, such as to offer products to customers or business partners, communicate, improve products or services, organize training, perform statistical or marketing analysis, manage IT systems, conduct testing and development, maintain security systems and measures.
- To comply with any legal procedures, laws, rules, or court orders, or policies set out by a government supervisory authority, law enforcement authority, government agency, dispute resolution agency, or any supervisory authority.
- To carry out data storage and processing to be in order and in compliance with any applicable laws, rules, and regulations, including our working rules and applicable laws.
- To carry out the statistical survey or survey forms requested by the governmental bodies.
- To investigate complaints and issues concerning inappropriate behavior, as part of disciplinary process.
- For internal and external communications of the Companies.
- To keep records of employees, insurance, medical history, and insurance plans.
- For reference and background checks in order to avoid any possible conflicts of interest, for compliance with the regulations of local or foreign administrative authorities, and to examine the terms and conditions of employment.
- To facilitate investigations by competent officers, provide assistance in respect to law enforcement on behalf of the Companies for government agencies or any other supervisory

agencies, perform reporting obligations, perform any requirements under law, or as approved by government agencies or any other supervisory agencies.

- To process payments, collect charges or payments, fulfil accounting objectives, perform accounting management, perform auditing, and pursue debt payments in case that employees owe the Companies.
- To examine, prevent, or perform any acts in connection with violation of law and risk mitigation, in case of threatened fraud, money laundering, illegal acts, or threats to the lives, health, or safety of other persons.
- To ensure the Companies' safety.
- To conduct organizational restructuring or any other transactions that are part of business activities, or business acquisition or sale proposals resulting in your Personal Data being transferred or disclosed.
- To comply with rules, to conduct business audit (both internal and external).

3.2 Other Third Parties

- To communicate with you, to get to know you, verify your identity, verify any information provided by you to the Companies.
- To offer, sell, provide, manage, operate, proceed with, and otherwise handle products and services for you, including for procurement, communicate with you in order to respond to your purchase orders, deliver products based on your purchase orders and provide services to you.
- To comply with a contract, enter into the contract with you, proceed with management procedures, fulfil and effect your requests or any transactions contemplated herein, or any other documents that you may send to the Companies from time to time, analyze risks, collect any outstanding payments from you, amend or terminate the contract, pursue debt payments, execute our contractual rights against you.
- In case you are customers or representatives: to render the services to you, install, repair the products, advise in relation to products and services, support or assist in the service or product management.

- To communicate with you, including communications about product management or other information about our products, or any accounts that the Companies have with you, provision of technical support for any of our websites and applications, or communications about any changes relating to this policy.
- To process collections or payments, issue invoices, collect charges or payments, fulfil accounting objectives, perform accounting management, and perform auditing.
- To examine, prevent, or perform any acts in connection with violation of law and risk mitigation, in case of threatened fraud, money laundering, or threatened illegal acts, or threats to the lives, health, or safety of other persons.
- To provide information about other products or services which may be of interest to distributors, suppliers, or representatives, who may inform the Companies to deny to obtain such information at any time.
- To ensure the Companies' safety.
- To assist the Companies in our business operations, such as to serve advertisements, public relation materials, sales promotions, and other communications, improve our products or services, organize training, hold marketing activities, perform statistical or marketing analysis, conduct consumer surveys, manage IT systems, conduct testing and development, maintain security systems and measures.
- To conduct organizational restructuring or any other transactions that are part of business activities, or business acquisition or sale proposals resulting in your Personal Data being transferred or disclosed.
- To comply with rules, to conduct business audit (both internal and external).
- To comply with the Companies' policy.
- To comply with any applicable laws, rules, agreements, or policies set out by a government supervisory authority, law enforcement authority, government agency, dispute resolution agency, or any supervisory authority.
- To provide assistance in respect to law enforcement, or investigations by or on behalf of the Companies, or by police officers or government agencies, or by any other supervisory

agencies, perform reporting obligations, perform any requirements under law, or as approved by government agencies or any other supervisory agencies.

3.3 Stakeholders

- For business administration and management, and the Companies' operations.
- For verification or identification of shareholders and independent directors, including their related persons, such as their spouses, children, emergency contacts, guarantors, or persons who give consent on behalf of legal representatives, guardians, and/or estate administrators; parents and/or legal representatives, proxies, and beneficiaries.
- For other benefits regarding our business operations and administration, such as to make meeting agendas for shareholders' meetings, board of directors' meetings, or other internal meetings, as well as the minute of meeting, public relation and other activities.
- To sale and purchase transactions or other transactions by stakeholders, including risk assessments for investments, according to applicable laws and regulations.
- To comply with any legal procedures such as holding the shareholders' meeting, sending the invitation letters, dividend payment, or comply with any applicable laws, rules, agreements, court order, policies set out by a government supervisory authority, law enforcement authority, government agency, dispute resolution agency, or any supervisory authority.
- To carry out data storage and processing to be in order and in compliance with any applicable laws, rules, and regulations, including our working rules and applicable laws.
- To comply with any requirements with respect to payment of wages, compensation, benefits, remuneration plans, offers, rewards, and compensation account.
- For performance appraisal, internal reporting, data analysis, and performance of contractual obligations.
- For internal communications, notification of internal and external appointments, whether through telephone, text, email, post, electronic media, such as applications with communications features, or any communication channels.
- To process payments, collect charges or payments, fulfil accounting objectives, perform accounting management, perform auditing, and pursue debt payments, in case stakeholders owe the Companies.

- To facilitate investigations by competent officers, provide assistance in respect to law enforcement on behalf of the Companies for government agencies or any other supervisory agencies, perform reporting obligations, perform any requirements under law, or as approved by government agencies or any other supervisory agencies.
- For anti-money laundering crime checks (e.g. transaction suspension, involvement in anti-money laundering schemes, or transaction rejections by financial institutions), examination of information about bankruptcy, information about any related legal entities, information for the KYC process, information about occupations or businesses considered risky under anti-money laundering laws, and information about offenses received from supervisory bodies; to examine, prevent, or perform any acts in connection with violation of law and risk mitigation, in case of threatened fraud, money laundering, or threatened illegal acts, or threats to the lives, health, or safety of other persons.
- To ensure the Companies' safety.
- To conduct organizational restructuring or any other transactions that are part of business activities, or business acquisition or sale proposals resulting in your Personal Data being transferred or disclosed.
- To comply with rules, to conduct business audit (both internal and external).

In the event that the Companies reveal your Personal Data for other purposes apart from aforementioned in this policy, the Companies will notify you for such objectives or ask your permission before proceeding it.

4. Disclosure or transferring your Personal Data

The Companies may disclose your Personal Data to any persons or organizations in connection with business operations or management, including the government agency or officials. The Companies will disclose your Personal Data only for the original purpose for which data was collected, or for related objectives, except for security purposes, or for compliance with the laws.

The Companies may disclose or share your Personal Data to any of the following parties:

- The affiliates and subsidiaries.
- Shareholders, including their executives, either they are natural persons or legal entities, companies in the same group as the shareholders'.

- Organizers, advertisers, the press, and sponsors of events or exhibitions.
- Hotels or other event site service providers, or their representatives relating to events or exhibitions.
- Contractors, service providers, suppliers, and other agents, who act on behalf of the Companies or who are retained by the Companies, such as event-related service providers, banking or financial service providers, hosting service providers, cloud application or network providers, event registration service providers, domestic and overseas tourism service providers, security service providers, auditing service providers, legal service providers, insurance service providers, marketing survey service providers, email management service providers, postal service providers, representatives and agents that sell or promote products and services, auction service providers.
- Thailand Securities Depository Co., Ltd.,
- Banks, or financial institutions as the case may be.
- Any persons that you agree to provide your Personal Data.
- Persons engaged in the sale of our business, in whole or in part, a merger, or acquisition.
- Any persons or government agencies, as required by the law, court orders, or orders of any authorities.
- Supervisory bodies, government agencies, private organizations, or state-owned enterprises with the duty to supervise our business operations, when they require the Companies to disclose Personal Data.

The Companies may hire third parties to fulfil any of the above objectives, either in whole or in part, or for the development or maintenance of our system. In such cases, the Companies will control and put in place measures to ensure that such third parties will store and use Personal Data strictly in accordance with this policy, any data security requirements and conditions, and the personal data protection law.

5. Data retention

To secure the Personal Data, the Companies have implemented the following measures:

- The right to access, and/or process Personal Data including the identity verification, authorized persons, Personal Data processing must be strictly complied with our policy.

- The Companies have established a safe encoding method to prevent loss or unauthorized or unlawful access, destruction, use, alteration, or disclosure of Personal Data.
- Personal Data may be transferred, including transfer for storage on a database, to an external organization or any country only if the personal data protection measures implemented by such organization, or the country, are of equal or higher standards than the measures in this policy.
- In case that the Companies engage a third party to store the Personal Data of employees, such as the time recording application or document storage companies, the Companies will require those firms to keep the information confidential, and prohibit use to only the purposes determined by the Companies.

The Companies will collect, use, disclose, and retain your Personal Data throughout the sale and purchase of our products. Upon the end of the relationship between the Companies and you, the Companies will retain your data, including Personal Data, only as necessary for the fulfilment of the above objectives, not exceeding 10 years from our last contact, or from the end of the relationship between the Companies and you, except where it is necessary for the Companies to retain your Personal Data for more than 10 years, to the extent that it is permitted by law. When it expires, the Companies will destroy your Personal Data or make it unidentified.

6. The Companies' website

The Companies may collect your Personal Data through our website as described below:

- When you apply for job vacancy, the Companies will require the necessary information such as your history, contact, education record, working experience, and other necessary information.
- Your device, IP address, connection information, location, browser, log file, referring website, customer behavior, access time, keywords and your search.
- The Companies use the Cookies to record the data and present it to match with your requirements, in which, the Companies will use Cookies, which are tools that recognize your device and record certain information during your visit to the Companies' website. This is to better respond to you when you use certain parts of the website. The information collected and analyzed by the Companies for future improvement includes information about your

computer and connections, your browsing history, and etc. You may change your browser settings so that your browser does not detect the Cookies or delete it, or disable it.

- The Companies may use the information technology from the supplier to store the Personal Data, in which, the Companies will select the proper supplier to comply with the policy.

Other websites: this policy is applied for only the Companies. In case you link to other websites through our web pages, the Companies are not responsible for their practice concerning data and privacy. You have to review and consider the Personal Data Protection policy of such websites.

CCTV: the Companies use a CCTV system to record images of persons and vehicles around our premises, for public safety and for prevention and detection of crimes. The CCTV cameras provide 24-hour footage of the entrance, lobby, balconies, outdoor parking areas, areas along the fence, and other accessible areas. The information is recorded for one month, and is then overwritten. Camera locations were chosen to avoid footage which is not related to the purpose of inspection and monitoring.

Live feeds from the CCTV system can be examined, only in necessary circumstances, by an authorized person. The Companies believe that live feeds and visual recordings are seen only by authorized employees, who are directly responsible for access to such information. The Companies respect your privacy and do not have CCTV cameras in locations where privacy can be expected, such as toilets.

7. Consent

To assess the Personal Data, the Companies will notify you the relevant details and obtain the prior consent from you before your data collection. However, if the laws allow the Companies to assess your Personal Data without prior consent, whenever you access our website or give your Personal Data to the Companies, it will imply that you consent the Companies to collect, reveal, transfer your data according to the objectives. In the event that you would like to revoke your consent or any rights in connection with your Personal Data (see Topic no.8: Rights of personal data owner), you shall notify the Companies as per the guideline.

If you provide Personal Data of another person, you must obtain prior consent from that person. In such event, you represent and warrant that you have obtained consent from that person, or you are entitled to provide Personal Data of such person to the Companies. When you provide Personal Data of such person to the Companies, it shall be deemed that you represent that such person acknowledges and gives consent under this privacy policy.

If the Companies require any additional consent, the Companies or any of third party service providers, will obtain your consent for the collection and use of your Personal Data at the time of collection.

To give your Personal Data is voluntary, you may choose not to give your data to the Companies. Anyhow, in the event that the Companies must collect your data according to the laws or for the purposes of entering into contracts, if you deny to give such data, the Companies may not be able to provide you the services or enter into such contracts with you.

8. Rights of personal data owner

You have the right to access your data, obtain the copies of your data, withdraw your consent, or request to edit or delete or destroy your Personal Data that is in our possession or control, or request that such data be anonymized or transfer your data to other data controller.

To exercise the said rights, the Companies may refuse your request or limit it according to the laws. In case you find the Companies not comply with the Thai Personal Data Protection Act. B.E. 2562, you can petition to the Office of the Personal Data Protection Commission.

You can exercise your right through our form by www.ttwplc.com or telephone no. 0-2019-9490-3 or email: ttw_pdpa@ttwplc.com or contact: Human Resources and Administration Department in the event that the data owner is the Companies' employee.

9. Contact of Data Protection Officer

Assistant Managing Director, Office of Managing Director

TTW Public Company Limited

30/130 Moo 12, Buddhamonthon sai 5 road,

Raikhing, Sampran, Nakhon Pathom

Tel: 02-0199490-3 (1103)

10. Change in the Personal Data Protection Policy

The Companies will review this policy from time to time in order to abide by the laws and its guideline. Anyway, the Companies reserve the right to change this policy without prior notice to you.

Announced as of 10 August 2022

(Ms. Walainut Trivisvavet)

Managing Director