

-Translation-

Privacy Policy

For partners, tenants, visitors, Eastwater building service users, and operational area users.

Eastern Water Resources Development and Management Public Company Limited and its subsidiaries place great importance on the protection of personal data of our business partners, tenants, visitors, users of the Eastwater Building, and users of the Company's operational areas (collectively referred to as "**you**"). This policy ensures that your personal data is protected and handled in accordance with personal data protection laws. It also provides details on the collection, use, disclosure of your personal data rights, and contact channels. The details are as follows:

1. Definitions

"The Company" means Eastern Water Resources Development and Management Public Company Limited.

"Group Company" means Eastern Water Resources Development and Management Public Company Limited and its subsidiaries.

"Subsidiary" means a company that has one of the following characteristics:

1. A company that the company has control over.
2. A company that is under the control of the company as mentioned in (1) in succession, starting from being under the control of the company as mentioned in (1)

"Partner" refers to a natural person, such as a consultant or a sole proprietor, or a natural person acting as a representative of a legal entity conducting business with the Company as a partner, including employees of such partners.

"Tenant" refers to a natural person who has entered into a lease agreement with the Company for the Eastwater building, including natural persons who are representatives of legal entities acting as tenants, as well as employees of such tenants.

"Visitor" refers to a natural person who visits or contacts individuals or legal entities located within the Eastwater building.

"Service User" refers to a natural person who uses any type of service within the Eastwater building, the Company's operational areas, or the operational areas of its subsidiaries.

“**Eastwater Building**” refers to the premises within the Eastwater building located in Bangkok, including the surrounding areas that are owned by the Company.

“**Operational Area**” refers to business operation areas, including factory premises used in the operations of the Company Group.

“**Personal Data**” refers to any information relating to an individual that enables the identification of such individual, either directly or indirectly, but excludes information of deceased persons specifically.

“**Sensitive Personal Data**” refers to personal data related to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, genetic data, biometric data such as facial recognition, fingerprint scanning, etc., or any other data that affects the personal data owner in a similar manner as prescribed by law.

“**Data Controller**” means a person or legal entity with the authority to make decisions regarding the collection, use, or disclosure of personal data.

“**Personal Data Processor**” means a person or legal entity that collects, uses, or discloses personal data according to the instructions or on behalf of the data controller. Such a person or legal entity is not the data controller.

2. Purposes of Collecting, Using, or Disclosing Personal Data

The Company and/or its subsidiaries have the following purposes and lawful bases for collecting, using, or disclosing personal data:

Objective	Lawful Basis
1) For purposes such as vendor registration, procurement, financial transactions, safety training for partners and/or their employees, and organizing partner meetings or related activities.	Performance of Contractual Relationship and Processing of Requests with Partners
2) For managing rental spaces for tenants, coordinating matters related to lease agreements, and organizing tenant meetings and related activities.	Performance of Contractual Relationship and Processing of Requests with Partners
3) To enable the Company and its subsidiaries, or other external parties such as government agencies or courts, to share information on a group-wide basis, particularly regarding information technology security, network systems, or future merger and acquisition activities.	Legitimate Interest
4) For the purpose of maintaining security within the building and/or operational areas of the Company and/or its subsidiaries, such as	Legitimate Interest

Objective	Lawful Basis
tracking, securing the Eastwater building premises, and operational areas of the Company and/or its subsidiaries in case of emergencies, recording still images and/or video footage via closed-circuit television (CCTV), and preventing potential crimes and fraud.	
5) For advertising and public relations through the Company's and/or its subsidiaries' social media platforms such as Facebook, Line, YouTube, as well as printed media.	Legitimate Interest
6) For performance evaluation, market analysis and research, marketing strategy development, as well as for business planning, reporting, and forecasting purposes.	Legitimate Interest
7) For collecting feedback, analysis, research, and development of products and services, including activities of the Company and/or its subsidiaries to better suit your needs, as well as for improving communication and public relations.	Legitimate Interest
8) For risk management, governance, and internal audits conducted by the Internal Audit Office, as well as for internal organizational management, such as fraud detection and prevention.	Legitimate Interest
9) For contacting to request additional information, recording the outcomes of such actions, and carrying out internal processes of the Company and/or its subsidiaries.	Legitimate Interest
10) For selecting participants for activities, responding to inquiries through online channels, announcing activity results, awarding prizes to participants according to conditions set by the Company and/or its subsidiaries, as well as maintaining a database of activity participants' records with the Company and/or its subsidiaries.	Legitimate Interest
11) For improving the work quality and efficiency of the Company and/or its subsidiaries, such as creating databases, analyzing, and developing the Company's and/or its subsidiaries' operational	Legitimate Interest

Objective	Lawful Basis
processes, in order to ensure compliance with the Company's policies.	
12) For compliance with laws, investigations, and legal proceedings according to applicable laws and regulations, and for reporting or disclosing information to government agencies or other organizations under legal authority, court orders, or regulatory bodies with legal jurisdiction, including for asserting legal claims, exercising rights, or mounting legal defenses.	To comply with legal obligations
13) For managing hygiene and safety.	To prevent or mitigate harm to life, body, or health of individuals.
14) To serve as a stakeholder database of the Company and/or its subsidiaries, as well as for managing relationships or coordinating matters related to the Company and/or its subsidiaries, including conducting satisfaction surveys and collecting feedback for the purpose of analyzing and improving the operations of the Company and/or its subsidiaries.	Legal Basis of Consent

3. **The personal data that the Company and/or its subsidiaries receive from you, or from individuals authorized by you, or from external agencies such as government agencies, regulatory agencies, or public sources, will be collected, used, and disclosed by the Company and/or its subsidiaries as follows.**

- (1) Identity Data such as full name, national identification number, passport number, date of birth, gender, age, nationality, signature, photograph, professional license number, driver's license information, electronic system username, etc.
- (2) Contact Data **such** as address, house registration copy, telephone number, fax number, email, geolocation, emergency contact person, social media account (e.g., LINE ID), secretary information, etc.
- (3) Financial Data, such as bank account number, etc.

- (4) Communication Data with the Company and/or its subsidiaries, such as information about the date, time, and location of contact, recordings of images and/or audio during communications with the Company and/or its subsidiaries, etc.
- (5) Information about the company or organization where the individual works, such as the employer company or affiliated department, workplace location, job position, etc.
- (6) Information about educational background, work history, training, expertise, and various achievements, etc.
- (7) Information about personal preferences and interests.
- (8) Recordings captured by CCTV cameras.
- (9) Information regarding participation in meetings between the Company and/or its subsidiaries, including attendance at training sessions, seminars, activities, or other programs organized by the Company and/or its subsidiaries, which may include still images, video recordings, and/or audio recordings during such meetings, trainings, seminars, or activities.
- (10) Other necessary information for background checks, suitability assessments, or risk evaluations before entering transactions, including for litigation or enforcement purposes, such as marital status, asset information, etc.
- (11) Opinions, suggestions, and complaints.
- (12) History of participation in activities or projects with the Company and/or its subsidiaries.
- (13) Information for screening under epidemic prevention measures.
- (14) Information regarding the use of various electronic systems of the Company and/or its subsidiaries, including data related to the use of applications and website browsing information, such as website visit history, IP address, etc.
- (15) Other personal information necessary for convenience, such as dietary preferences or beverages consumed.

4. Sensitive Personal Data.

The company and/or its subsidiaries do not intend to collect, gather, or use information regarding religion, blood type, nationality, or race that appears on your ID card and/or passport for any specific purpose. If you have provided a copy of your ID card and/or passport to the company and/or its subsidiaries, please conceal such information. If you do not conceal the aforementioned information, it is considered that you have authorized the company and/or its subsidiaries to conceal such information.

The documents with the concealed information will be considered valid and legally enforceable in all respects. However, if the company and/or its subsidiaries are unable to conceal the information due to certain technical limitations, the company and/or its subsidiaries will collect and use such information solely as part of your identity verification documents.

In cases where the company and/or its subsidiaries need to collect your sensitive personal data, the company and/or its subsidiaries will seek your explicit consent on a case-by-case basis, unless otherwise required by law.

The company and/or its subsidiaries may process the following sensitive personal data:

- (1) Religious information.
- (2) Health and/or disability information.
- (3) Nationality and racial information.

5. Types of Data Recipients.

Access to your personal data is strictly limited to individuals who have a legitimate need to know the information, solely to perform their job responsibilities and data processing roles as specified below.

The Company and/or its subsidiaries may share your personal data within the corporate group for internal management and marketing purposes only to the extent necessary, with the details as follows.

- (a) The Company and/or its subsidiaries may transfer or disclose your personal data to other companies within the corporate group.
- (b) The Company and/or its subsidiaries shall not use or disclose your personal data in any manner without your consent, unless the personal data can be collected without consent as permitted by applicable law, or in cases where the law authorizes such actions.
- (c) The Company and/or its subsidiaries shall ensure that their employees do not use or disclose your personal data for any purposes beyond the intended purposes of the Company and/or its subsidiaries, except when :
 - Consent has been obtained from the data subject; or
 - Such actions are permitted by law.
- (d) Personal data will be collected for use or disclosure between the Company and/or its subsidiaries. In cases where the Company and/or its subsidiaries permit external persons or agencies to access or use the data subject's personal data, the Company and/or its subsidiaries will act only as necessary and in accordance with the objectives and authority of the Company and/or its subsidiaries. The external persons or agencies must have sufficient standards for personal data protection. In all cases, the Company and/or its subsidiaries must always obtain the consent of the data subject beforehand.

The Company and/or its subsidiaries may appoint service providers acting as data processors to provide IT services and assistance in managing other tasks, such as IT hosting providers and IT maintenance services. These service providers will act as data processors and are subject to the same instructions, with the service providers having access to your personal data only to the extent necessary for providing the services.

The Company and/or its subsidiaries may disclose your personal data as required or permitted by applicable laws to government agencies, courts, external advisors, and similar third parties.

The current list of personal data processors and external parties to whom the company has shared your data will be provided upon request to the company and/or its subsidiaries and the data protection officer, according to the contact details provided below.

6. Collection of Personal Data.

6.1 The Company and/or its subsidiaries shall not collect personal data without obtaining prior or concurrent consent from the data subject, except in cases where such collection is permitted by law. The request for consent from the data subject must be made explicitly, either in writing or by electronic means, unless otherwise prescribed by law.

In cases where sensitive personal data is to be collected, the Company and/or its subsidiaries must always obtain explicit consent from the data subject beforehand, unless the collection is allowed under applicable law.

6.2 Before or at the time of collecting personal data, the Company and/or its subsidiaries shall inform the data subject of the following details, unless the data subject is already aware of such details:

- (1) The purpose of collecting personal data.
- (2) Notification that the data subject may be required to provide personal data to comply with laws or contracts, or that it may be necessary to provide personal data to enter into a contract, including the possible consequences of not providing such personal data.
- (3) The personal data to be collected and the retention period. If the retention period cannot be clearly defined, an estimated retention period based on standard data collection practices shall be provided.
- (4) The types of persons or external agencies to whom the collected personal data may be disclosed.
- (5) Information about the entity collecting the personal data, including contact details and methods of communication. In cases where there is a data protection officer or

representative, their contact information and methods of communication must also be provided.

(6) The rights that the data subject is entitled to receive.

6.3 The Company and/or its subsidiaries shall not collect personal data from sources other than the data subject directly, except in cases where permitted by law.

6.4 The Company and/or its subsidiaries shall record the following information to allow the data subject to be verified, and such records may be kept in written form or in an electronic system:

- (1) The personal data collected.
- (2) The purpose of collecting each type of data.
- (3) Information about the entity within the Company and/or its subsidiaries responsible for storing the personal data.
- (4) The retention period of the personal data.
- (5) The rights and methods for accessing personal data, including conditions related to individuals authorized to access the personal data and the conditions for such access.
- (6) The use or disclosure of personal data that is exempted by law from the requirement of consent.
- (7) Reports of refusals to access, disclose, or obtain personal data, or objections from data subjects as required by law, along with the reasons for such refusals.
- (8) Descriptions of the security measures that the Company and/or its subsidiaries are obligated to implement.

7 Your Rights as a Data Subject.

(1) Right to Access.

You have the right to access and obtain a copy of your personal data that is under the responsibility of the company and/or its subsidiaries. You also have the right to request the disclosure of the acquisition of such personal data that you did not consent to the company and/or its subsidiaries. However, this right is not absolute, and the rights and benefits of others may limit your right to access your data. The company and/or its subsidiaries may charge a reasonable fee for processing and managing such requests.

(2) Data Portability Right.

You have the right to request, send, or transfer your personal data provided to the company and/or its subsidiaries to another data controller or to yourself, as required by law.

(3) Right to Object.

You have the right to object to the collection, use, processing, or disclosure of your personal data if you find it incorrect, inappropriate, or unfair.

(4) Erasure Right.

You have the right to request the company and/or its subsidiaries to delete or destroy your personal data or make it anonymous if there is no authority to collect it or if it is no longer necessary.

(5) Right to withdraw consent.

You have the right to withdraw the consent given to the company and/or its subsidiaries at any time while your personal data is still with the company and/or its subsidiaries, unless the withdrawal of consent is restricted by law or contract that benefits you. The withdrawal of consent will not affect the processing of personal data that you have already consented to legally.

(6) Right to restrict processing.

You have the right to request restriction of the use of your personal data because it is under review or no longer necessary.

(7) Rectification Right.

You have the right to request the company and/or its subsidiaries to correct your personal data to be up-to-date, accurate, complete, and not misleading.

(8) Right to Lodge a Complaint.

You have the right to lodge a complaint with the authorized officer under the Personal Data Protection Act B.E. 2562 if the company and/or its subsidiaries do not comply with the law. In case you submit a request to exercise your rights under the Personal Data Protection Act B.E. 2562, the company and/or its subsidiaries will proceed within the time specified by law. The company and/or its subsidiaries reserve the right to deny or not comply with such requests if required by law.

8 Security of Personal Data.

The company and/or its subsidiaries have appropriate measures in place to ensure the security of their information technology systems. These measures are designed to prevent loss of unauthorized access, use, alteration, modification, or disclosure of personal data. These measures are outlined in the information technology security policy of the group of companies.

9 Retention Period.

Your personal data shall be retained by the Company and/or its subsidiaries and/or the Company's and/or subsidiaries' service providers only for as long as necessary to effectively perform

their duties and to achieve the purposes for which the data was collected, in accordance with applicable local laws. Personal data of contractors and tenants shall be retained for a period of 10 years from the date the contract between the contractor or tenant and the Company terminates. Personal data of visitors and service users shall be retained for a period of 3 years from the date the personal data was collected.

The Company and/or its subsidiaries shall delete such data from their systems and record the deletion accordingly. Alternatively, the data may be pseudonymized or anonymized so that the personal data can no longer identify you, unless the Company and/or its subsidiaries are required to retain such data, including personal data, to comply with legal obligations or regulations, such as statutory data retention periods.

10 Changes to the Privacy Policy.

The company and/or its subsidiaries may update or amend this privacy policy to comply with relevant practices and legal requirements. If there are changes to the privacy policy, the company and/or its subsidiaries will notify you by publishing the changes on the company's and/or its subsidiaries' website. This privacy policy was last reviewed on October 16, 2024.

11 Contact Channels.

If the data subject wishes to contact the company and/or its subsidiaries regarding this privacy policy or their rights, they can contact **the Personal Data Protection Officer** team at:

Eastern Water Resources Development and Management Public Company Limited

East Water Building, 23rd-26th Floor, 1 Soi Vibhavadi Rangsit 5, Vibhavadi Rangsit Road,
Chomphon Subdistrict, Chatuchak District, Bangkok 10900.

Phone: 02-272-1600 ext. 2522 or 2577 Fax: 02-272-1601-3

Email: EW_Compliance@eastwater.com

Announced on 24 October 2024.

-Signed-

.....
President & CEO