-Translation-

Privacy Policy

For Employees, Workers, Interns, and Job Applicants

Eastern Water Resources Development and Management Public Company Limited and its subsidiaries place great importance on protecting the personal data of employees, workers, interns, and job applicants (collectively referred to as **"you"**). This policy ensures that your personal data is protected and handled in accordance with the Personal Data Protection Act. It provides details on the collection, use, disclosure, and rights related to your personal data, as well as contact channels for the company. The privacy policy is outlined as follows:

This policy is not part of the employment contract. The company and/or its subsidiaries may update it in accordance with applicable laws, such as implementing new systems or processing methods related to the use of personal data.

1. Definitions

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

"Group Company" means The 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)

" Employees" refers to permanent employees, probationary employees, contract employees, or temporary employees.

" Workers" refers to employees, interns, personnel of the company's partners, and/or subsidiaries working in the East Water building or operational areas of the company and subsidiaries.

"Personal Data" means information about an individual that can identify that person, directly or indirectly, but does not include information about deceased person.

"Sensitive Personal Data" means 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.

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) To be used in the consideration of hiring employees to work for the Company and/or its subsidiaries, which includes the application process through online job application channels via the Company's and/or its subsidiaries' websites, direct job applications to the Company and/or its subsidiaries, or through recruitment service providers. This also covers the interview process, the selection and assessment process, the employment contract offer process, and other human resources management procedures related to recruitment and selection. Furthermore, it includes internal processes of the Company and/or its subsidiaries such as performance evaluation, compensation, and benefits administration.	• To comply with contractual relationships. • For legitimate interests.
2) To consider the transfer of employees to become employees of the Company and/or its subsidiaries, in cases where personnel are transferred within the group of companies in accordance with the internal policies, regulations, or requirements of the Company and/or its subsidiaries. Your personal data may be used for coordination, performing duties, or conducting transactions with clients, partners, government agencies, state enterprises, public organizations, independent organizations established by law, or other external entities or individuals, in your capacity as a representative of the Company and/or its subsidiaries. This also includes the execution of contracts, amendments or addendums to agreements, granting or receiving power of attorney, providing explanations, supplying information or statements to external parties, or participating in training, seminars, and academic discussions.	
3) To consider internship applications from students based on the list provided by universities, colleges, or educational institutions,	• To comply with contractual relationships.

Objective	Lawful Basis
including the interview process, the selection and evaluation process, the process of offering an internship agreement to you, and other human resource management procedures related to the consideration and selection of interns for the Company and/or its subsidiaries.	• For legitimate interests.
4) To verify and confirm your identity as an employee of the Company and/or its subsidiaries.	For legitimate interests.
5) To carry out activities in accordance with the agreement during your internship with the Company and/or its subsidiaries, such as compensation payments (if any), recording internship attendance, site visits or job shadowing, granting access to information systems and databases necessary for the internship, as well as the execution of any related agreements.	To comply with contractual relationships.
6) To comply with the various policies of the Company and/or its subsidiaries, and to use the information for corporate governance, work monitoring, and ensuring compliance with the Company's and/or its subsidiaries policies.	For legitimate interests.
7) To carry out business planning, reporting, and forecasting; risk management; audit supervision, including internal audits by the internal audit department and internal organizational management. This also includes using the information for internal operations related to financial disbursements by the accounting and finance departments of the Company and/or its subsidiaries. Additionally, it serves as information for verifying qualifications or suitability for work under contracts or agreements with the Company and/or its subsidiaries. Furthermore, it includes investigations and inquiries into internal complaints, fraud prevention, or other legal proceedings, as well as handling and managing complaints and allegations related to the operations of the Company and/or its subsidiaries or related parties, to ensure transparency and fairness for all parties involved.	For legitimate interests.

Objective	Lawful Basis
8) To improve the work or services of the Company and/or its subsidiaries.	For legitimate interests.
9) To be used as information for applying to access the Company's and/or its subsidiaries' internal intranet system, electronic systems access, or to grant access rights to use the internet or various electronic systems.	For legitimate interests.
10) To investigate and inquire into internal complaints, prevent fraud, or carry out other legal proceedings, as well as reviewing and managing complaints and allegations related to the operations of the Company and/or its subsidiaries or related parties, to ensure transparency and fairness for all parties involved.	For legitimate interests.
11) To establish legal claims, granting and receiving powers of attorney, exercising or defending legal claims, conducting litigation, and enforcing legal actions. This also includes compliance with laws, court orders, letters, or directives from authorities, independent organizations, or officials with legal authority, such as complying with summons, seizure warrants, court orders, police officers, prosecutors, or government agencies. Additionally, it includes reporting or disclosing information to shareholders, government agencies, or independent organizations such as the Securities and Exchange Commission, the Revenue Department, the Department of Land, the Department of Business Development, the National Anti-Corruption Commission, and others. All these actions are to ensure compliance with applicable laws.	• For legitimate interests. • To comply with legal obligations.
12) To maintain security within the buildings and/or operational areas of the Company and/or its subsidiaries, such as tracking individuals, securing the East water building 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 to prevent potential crimes and fraud.	For legitimate interests.

Objective	Lawful Basis
13) To collecting and using your personal data, including your full name, position, department, and photographs, video footage, and/or audio related to the operations and activities of the Company and/or its subsidiaries, for publicity and promotional purposes through various channels such as the Company's and/or its subsidiaries' social media platforms (e.g., Facebook, Line, YouTube) as well as printed media.	For legitimate interests.
14) To serve as a database of stakeholders of the Company and/or its subsidiaries, as well as for managing relationships or coordinating communications related to the Company and/or its subsidiaries. Additionally, for conducting surveys and collecting feedback to analyze and improve the operations of the Company and/or its subsidiaries.	Legal basis of consent
15) To comply with laws related to public health benefits, such as the prevention of health risks from dangerous communicable diseases or epidemics that may enter or spread within the Kingdom.	To comply with legal obligations.
16) To managing hygiene and safety.	To prevent or mitigate harm to life, body, or health of individuals.

The above purposes are important objectives for managing employment relationships and complying with applicable laws. Furthermore, the Company and/or its subsidiaries may process data of employees, interns, job applicants, and personnel for additional purposes **("Additional Purposes")** based on legitimate interests or with your consent, in accordance with the applicable personal data protection laws currently in force and/or as amended (if any).

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, copies of national ID card, passport copy, disability ID card copy, date of birth, gender, age, nationality, religion, signature, photograph, taxpayer

identification number, professional license number, driver's license information, electronic system username, and so on.

(2) Contact Data such as current address, registered address and work address, phone number, email address, Line ID, emergency contact details, and copy of house registration, etc.

(3) Financial Data such as bank account numbers, etc.

(4) Work-related Data such as job position, job details, work location, employer's name, division, department, role/responsibilities, assigned tasks and projects, manager's name, employment status, contract type, average working hours, business travel information, etc.

(5) Information regarding your compensation and benefits, such as salary, bonuses, other compensation, insurance and/or benefits, employee welfare, tax details, time records and leave days along with reasons for leave, and information related to social security and financial assistance, such as social security, leave of absence, bank account number, etc.

(6) Work performance and competency data, such as work history, educational background, copies of academic transcripts, copies of certificates or diplomas, employment certificates and verifications, skills, training records, training certificates, professional licenses, driver's license, competency and conduct assessments, company test results, annual performance reviews and evaluations, disciplinary actions including penalties and complaints by officials, employee surveys, interview assessments for recruitment, as well as information obtained during job interviews, training certificates, training records, etc.

(7) Images recorded by closed-circuit television (CCTV).

(8) Other necessary information for background checks, suitability assessments, or risk evaluations prior to decision-making for transactions, including legal proceedings or enforcement, such as marital status, asset information, etc.

(9) Opinions, suggestions, and complaints.

(10) History of participation in activities or projects with the Company and/or its subsidiaries.

(11) Screening information according to epidemic prevention measures.

(12) Information regarding the use of various electronic systems of the Company and/or its subsidiaries, including information about the use of applications and website browsing data such as browsing history, IP address, etc.

(13) Other personal data necessary for providing conveniences, such as food or beverages consumed, etc.

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. Categories of Data Recipients.

The Company and/or its subsidiaries may grant access to the personal data of employees, personnel, interns, and job applicants including sensitive data to various departments and individuals, based on the necessity of access and only to the extent required for fulfilling contractual obligations or exercising legitimate rights. This may include supervisors, the Human Resources Department, labor committees, audit committees, and other regulatory or supervisory units.

As part of necessary business operations, the Company and/or its subsidiaries may disclose or transfer employee data or sensitive data to external parties. You may request that the Company or the Data Protection Officer, using the contact information provided below, disclose the current list of data processors and third parties. The Company and/or its subsidiaries may share employee data and sensitive data with the following entities:

5.1 Within the Corporate Group.

(a) The Company and/or its subsidiaries may transmit or transfer your personal data to other companies within the corporate group.

(b) The Company and/or its subsidiaries will not use or disclose personal data of data subjects in any manner without the data subject's consent, unless the personal data is legally permitted to be collected without consent as stipulated by law, or there is a legal provision allowing such action.

(c) The Company and/or its subsidiaries will ensure that personnel of the Company do not use or disclose the personal data of data subjects for any purpose beyond the stated purposes of the Company and/or its subsidiaries, unless:

- Consent has been obtained from the data subject, or
- It is 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 authorize external individuals or entities to access or use the personal data of the data subject, such disclosure will be limited to what is necessary and only for the purposes and within the authority of the Company and/or its subsidiaries. The external individuals or entities must have adequate personal data protection standards. In any case, the Company and/or its subsidiaries must always obtain consent from the data subject beforehand.

5.2 Third Parties.

(a) The Company and/or its subsidiaries may transmit or transfer your personal data, contact details, and work-related information to partners, suppliers, customers, or end-customers, both current and future.

(b) The Company and/or its subsidiaries may transmit or transfer your information to acquiring businesses or acquired entities, and related advisors, if the business you are employed with is sold, transferred, or merged with another entity (or in similar transactions), either before such transactions (e.g., during a due diligence process) or after the transaction has been completed, in accordance with the rights permitted under applicable laws and jurisdictions where such entities are located.

(c) The Company and/or its subsidiaries may transmit or transfer data related to salary, benefits, and equity compensation to external independent consultants (e.g., auditors), insurers, tax authorities, government agencies, benefits providers, and other third parties.

5.3 Data Processors.

(a) The Company and/or its subsidiaries may transfer or disclose your personal data to third parties who act as data processors, to process such data under appropriate instructions. These data processors are contractually obligated to comply with proper procedures and organizational security measures to protect personal data and to process personal data only as instructed.

(b) Access to your personal data is strictly limited to individuals who have a need to know the information to perform their job duties. The Company and/or its subsidiaries may disclose your personal data as required or permitted by applicable law to government agencies, courts, or other legally authorized entities.

6. Collection of Personal Data.

6.1 The Company and/or its subsidiaries shall not collect personal data unless the data subject has given prior or concurrent consent at the time of collection, except where permitted by law. In requesting consent from the data subject, the Company must obtain such consent explicitly in writing or via electronic means, unless otherwise specified by applicable laws.

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 in order to comply with laws or contracts, or that it may be necessary to provide personal data to enter 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 person 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 were 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 as necessary for the efficient performance of duties and to achieve the purposes for which the data was collected, in accordance with the applicable local laws, for strictly necessary periods.

For the personal data of job applicants, the Company and/or its subsidiaries shall retain the personal data of applicants who are not selected for employment for a period of 1 year.

Employment relationships involve ongoing duties over a long period. When the Company and/or its subsidiaries no longer require your personal data for the performance of contractual obligations or legal duties, the Company and/or its subsidiaries shall delete such data from the system and record the deletion. Alternatively, the Company and/or its subsidiaries may pseudonymize or anonymize the personal data so that it can no longer identify you, unless the Company and/or its subsidiaries are

required to retain your data, including personal data, to comply with legal obligations or regulations that the Company and/or its subsidiaries must follow, such as labor laws, social security laws, and other relevant laws.

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