AI Energy Public Company Limited

Personal Data Protection Policy

- English Translate Version -

บริษัท เอไอ เอนเนอร์จี จำกัด (มหาชน)

AI Energy Public Company Limited

- English Translate Version -

Personal Data Protection Policy

AI Energy Public Company Limited (“the Company”) and its subsidiaries ("the Company") support the rights of privacy and place importance on the protection of personal data related to or transacted with the Company. Therefore, the Company has formulated this Personal Data Protection Policy to explain how the Company handles your personal data, including collection, file, use, disclosure, and your rights. This policy is designed to inform you of the Company's personal data protection practices.

1. Scope of Policy

This Personal Data Protection Policy (the "Policy") aims to describe how the Company collects, uses, and discloses your personal data, as well as the rights you have concerning this personal data. The Policy applies to the Company, its employees, and individuals involved in processing personal data on behalf of or under the Company's authority.

2. Definitions

2.1 **"Personal Data"** refers to any information that can directly or indirectly identify a person, including data provided by the data controller or data owner to the Company to fulfill contractual conditions. Personal data is categorized into 2 types:

2.1.1 "General Personal Data" includes names, gender, date of birth, age, residential addresses, telephone numbers, fax numbers, email addresses, or any information with an individual's name or identifying marks, codes, or other means of identification, such as fingerprints, voice recordings, photographs, and data related to deceased individuals.

2.1.2 "Sensitive Personal Data" includes information concerning race, ethnicity, political opinions, beliefs in religion or philosophy, sexual behavior, criminal history, health data, health examination results, labor union membership, genetic data, biometric data, disabilities, or any other data that similarly affects the data subject's rights and freedoms.

2.2 **"Processing"** refers to any operation performed on personal data, including collecting, assembling, using, disclosing, modifying, deleting, or destroying personal data.

2.3 **"Data Subject"** means an ordinary person who is the owner of personal data that can identify that person, whether directly or indirectly."

2.4 **"Data Controller"** refers to an individual or legal entity with the authority to make decisions regarding the collection, aggregation, use, or disclosure of personal data.

2.5 **"Data Processor"** refers to an individual or legal entity that processes personal data based on the instructions or on behalf of the data controller.

2.6 **"The Company"** refers to AI Energy Public Company Limited and its subsidiaries, including individuals appointed by the Company.

3. Respect for Personal Rights

The Company respects and places importance on the rights of personal data and the protection of your personal data. The Company is aware that you desire the security of your personal data.

4. Roles, Duties, and Responsibilities

4.1 The Company's Board of Directors has the following roles, duties, and responsibilities:

4.1.1 Oversee the establishment of a personal data governance structure and internal controls within the Company to ensure compliance with laws and personal data protection policies.

4.1.2 Supervise and support the Company's efforts to effectively protect personal data and ensure compliance with laws.

4.2 The Audit Committee has the following roles, duties, and responsibilities:

4.2.1 Establish and oversee a personal data processing governance structure and internal controls within all departments related to the processing of personal data.

4.2.2 Assess the effectiveness of compliance with the Personal Data Protection Policy and report the assessment results to the Company's Board of Directors at least once a year. Also, control and ensure that various risks related to personal data are appropriately managed.

4.2.3 Define and review work standards and guidelines to ensure that operations comply with the law and personal data protection policies.

4.3 The Personal Data Protection Team, consisting of department managers and supervisors responsible for various personal data processing in the Company, is assigned roles, duties, and responsibilities as follows:

4.3.1 Regularly report the status of personal data protection to the Audit Committee and make recommendations for improving personal data protection to keep it up-to-date and in compliance with the law.

4.3.2 Provide guidance to employees on legal compliance and personal data protection policies.

4.4 Managements have duties and responsibilities in overseeing, supervising, and ensuring that their respective departments adhere to the Company's Personal Data Protection Policy. They also promote awareness among employees.

4.5 Company employees have the following roles, duties, and responsibilities:

4.5.1 Comply with the Company's Personal Data Protection Policy, standards, guidelines, procedures, and other documents related to personal data protection.

4.5.2 Report any abnormal incidents related to personal data protection and non-compliance with laws and the Company's Personal Data Protection Policy to superiors or through complaint channels.

5. Personal Data Processing Risk Assessment and Management

5.1 The Company requires a risk assessment of personal data processing to verify readiness and compliance with the law organization-wide, at least annually or whenever there are additional changes in personal data processing methods. Each department involved in the governance structure is responsible for assessing and managing risks in personal data processing within its own scope. As well as follow up and report the risk assessment to the Audit Committees and the Board of Directors.

5.2 In assessing the impact on personal data protection, the Company follows these principles:

5.2.1 Clear explanation of details of data processing, specifying the scope of the impact assessment and the necessity of the data processing.

5.2.2 Clear description of the necessity and proportionality of data processing.

5.2.3 Assessment of the likelihood and severity of impact on the data subject's rights and freedoms, considering 'likelihood' and 'severity of impact.'

5.2.4 Details of measures to mitigate risks specified. Records are kept, and assessment reports are prepared accordingly.

5.3 Monitoring of outcomes and compliance with personal data-related risk management procedures by the Risk Management Committee, along with quarterly reports to the Audit Committee and the Board of Directors.

6. Personal Data Collection Limitation

6.1 The Company will use lawful and fair methods to collect and retain your personal data. Data collection will be limited to what is necessary for the Company's operations and as required by law.

6.2 As the data controller, the Company will seek your consent before collecting your personal data, unless:

- It is necessary to achieve the purposes related to the preparation of personal history documents, with appropriate safeguards in place to protect your rights and freedoms.
- It is necessary to protect or prevent threats to life, physical health, or safety of individuals.
- It is necessary for the performance of a contract where you are a party, or for taking pre-contractual steps at your request.
- It is necessary for the legitimate interests pursued by the Company or by a third party, except where those interests are overridden by your fundamental rights and freedoms.
- It is necessary for your benefit, and obtaining your consent is impossible or would involve disproportionate effort.
- It is necessary for the purposes of carrying out the investigation by an investigating official or the adjudication of a case by a court.
- It is required by law, such as the Personal Data Protection Act (PDPA), Electronic Transactions Act, Telecommunications Business Act, Anti-Money Laundering Act, and various criminal and civil laws.

6.3 The Company may combine your personal data with personal data received from other sources, but only when necessary and with your consent, for the purpose of updating your personal data to ensure accuracy, completeness, and quality of the services provided.

6.4 The Company may ask for and file additional data from you to ensure that the data remains accurate, up-to-date, and complete.

7. Purposes of Personal Data Collection

The personal data collected from you by the Company, in its capacity as a personal data processor, will be used for the purposes of the Company's business operations and as instructed by or on behalf of the data controller only. For personal data collected directly from you, the Company will inform you of the purposes of collection, usage, or disclosure of your data to third parties, the retention period, your legal rights regarding your personal data, and the contact information for inquiries related to your personal data. The Company will maintain strict security measures to prevent unauthorized access or use of personal data unless otherwise specified for a new purpose and consent is obtained or as required by the Personal Data Protection Act or other relevant laws.

8. Disclosure of Personal Data / Limited Use of Personal Data

8.1 The Company, as the data controller, will use or disclose your personal data only with your consent and only for the purposes specified by the Company. The Company will ensure that its employees do not disclose, display, or otherwise make personal data available outside of the specified purposes or to external parties unless:

- It is necessary to achieve the purposes related to the preparation of personal history documents or letters of reference for the public interest or for research or statistical purposes, with appropriate safeguards in place to protect your rights and freedoms.
- It is necessary to protect or prevent threats to life, physical health, or safety of individuals.
- It is necessary for the performance of a contract where you are a party, or for taking pre-contractual steps at your request.
- It is necessary for the legitimate interests pursued by the Company or by a third party, except where those interests are overridden by your fundamental rights and freedoms.
- It is necessary for your benefit, and obtaining your consent is impossible or would involve disproportionate effort.

- It is necessary for the purposes of carrying out the investigation by an investigating official or the adjudication of a case by a court.
- It is required by law, such as the Personal Data Protection Act, Electronic Transactions Act, Telecommunications Business Act, Anti-Money Laundering Act, and various criminal and civil laws.

8.2 The Company may use the services of information service providers to carry out the storage of personal data, and these service providers must have adequate security measures in place and are prohibited from collecting, using, or disclosing personal data beyond what the Company specifies.

8.3 The Company may find it necessary to disclose your personal data to other entities within group of companies or outside of Thailand for the benefit of its operations and services to data subjects. In such cases, the Company will ensure that these entities maintain the confidentiality of the personal data and do not use it for purposes beyond the scope defined by the Company.

8.4 In some cases, the Company may allow individuals or other organizations to access or use your personal data as necessary and for the purposes of the Company. In this regard, the Company, as the data controller, must obtain your consent beforehand.

9. Measures and methods for safeguarding the security of personal data

The Company will implement appropriate security measures to safeguard the confidentiality of personal data and will develop information technology security management systems in accordance with legal standards. This includes promoting awareness of responsibility for data security among employees and external service providers to prevent loss, unauthorized access, destruction, use, alteration, or disclosure of personal data without legal rights or consent. If you suspect that your personal data may be disclosed to external parties, lost, or stolen, and unauthorized transactions have occurred, please inform the Company immediately.

10. Rights of data subjects

10.1 The right to access or request a copy of personal data related to yourself or to request disclosure of information obtained without your consent in cases where you did not provide consent for collection or storage.

10.2 The right to request the Company to correct or change your personal data to be accurate, complete, and up-to-date.

10.3 The right to request access to personal data about yourself from the Company in a readable or usable format, with tools or devices that operate automatically. This includes requesting the Company to send or transfer personal data to other data controllers.

10.4 The right to object to the collection, use, or disclosure, or to not allow the Company to process your personal data, unless the Company can prove that it collects, uses, or discloses personal data of service users with legal consent, or for compliance or the exercise of legal rights, or for legal claims, or for the performance of contractual obligations between you and the data controller, or by relying on other legal rights.

10.5 The right to request the deletion, destruction, or transformation of personal data into data that cannot identify the data subject, except in cases where the Company is required by law to retain such data.

10.6 The right to suspend the use or disclosure of personal data related to yourself.

10.7 The right to withdraw consent for the collection of personal data. Withdrawal of consent does not affect data processing that has already been carried out.

10.8 The right to file a complaint: In cases where the Company, including its employees or contractors, violates or does not comply with the Personal Data Protection Act B.E. 2562 or regulations issued under this Act, if the data subject files a request for rights under the provisions of the PDPA, the Company, upon receiving such a request, will proceed within the timeframe specified by law. Furthermore, the Company reserves the right to refuse or not take action on such requests as required by law. In cases where the data subject has restrictions and chooses to provide only specific personal data, it may result in the data subject not receiving full services from the Company, and the Company may not be able to work with the data subject or provide any services if the data subject does not consent to provide the necessary data.

Data subjects can submit requests for actions on the above rights along with a certified copy of their identification card with a signature at the Company's office or via email at hr@aienergy.co.th. Once the Company receives such requests, it will consider and notify the results of the assessment within 30 days or within a reasonable timeframe. However, these rights may be subject to limitations as specified by the law, and the Company will keep records of such requests along with personal data related to the requests as evidence, as indicated in the attached documents.

11. Oversight and Inspection

The Company has established monitoring and inspection of compliance with the Personal Data Processing Policy under the following principles:

11.1 The Data Protection Team is primarily responsible for monitoring and inspecting compliance with the policy and personal data processing measures, as well as ensuring the security of personal data as set by the Company. They report their findings and inspections to the Audit Committee and report to the board of directors at least once a year or in cases of significant breaches affecting the Company's business or reputation.

11.2 A risk assessment and monitoring plan concerning the Company's personal data processing is established, report of risk assessments to the board of directors at least once a year or whenever there are significant changes within the Company.

11.3 In cases of policy violations and breaches related to personal data processing discovered during inspections, the Data Protection Team is responsible for receiving and managing complaints, overseeing compliance, and investigating to determine the facts. If violations are confirmed, the Data Protection Team will propose appropriate disciplinary actions to the managing director, considering the severity of the breach and the position of the responsible party, in accordance with the disciplinary measures outlined in the Company's personnel management regulations.

12. Record of Processing Activities (ROPA) and Information Disclosure Policy

The Company establishes standards and procedures for managing personal data, classifying data as 'Strictly Confidential' under the Company's confidentiality principles. It manages data accordingly, following these principles:

12.1 Each department or unit responsible for processing personal data is assigned the duty of creating and regularly updating the Record of Processing Activities (ROPA). They also specify the processing requirements for personal data to ensure that employees within their department understand the importance of data subject rights and their responsibilities in safeguarding all data.

12.2 The Company stipulates that all personal data processing must be carried out through electronic systems that control access and log access more effectively than paper-based records. In cases where personal data is used in paper format, records of data use are maintained, and a Clean Desk Policy is

enforced, prohibiting the reuse of paper with personal data (recycled). The Company also defines the file period for such data, and when data is moved, it is done following data security procedures.

12.3 In cases where it is necessary to transfer or disclose personal data to external entities, the Company has established the following procedures:

12.3.1 A review of the necessity, including the risk of transferring personal data and the reliability of the recipients, is conducted beforehand.

12.3.2 Each transfer or disclosure must obtain approval from the relevant authority according to their power of authorization.

12.3.3 The departments processing the data are responsible for recording the activities of personal data processing and transferring or disclosing data outside the Company.

12.3.4 Employees disclosing or transferring data must follow the channels and methods provided by the Company to minimize security risks and avoid using private channels that cannot be controlled.

12.3.5 A contract or data processing agreement is signed between the Company and external parties to specify the conditions, rights, and responsibilities in processing personal data, ensuring the personal data's security.

13. Data Retention Period and Withdrawal of Consent

13.1 The Company will retain your personal data for as long as necessary, including the duration of the Company's relationship with you as a customer and may continue to retain it for the necessary period to comply with the law, legal obligations, the Company's purposes, or to establish, exercise, or defend legal claims or as ordered by the data controller, unless such an order contradicts the law or data protection regulations under this Royal Decree. In the case of sensitive personal data processed by the Company, such as criminal history or medical treatment records, the Company exercises caution in managing and processing the data to higher standards, especially concerning the duration of data destruction, ensuring that data is deleted or destroyed as soon as it is no longer necessary.

13.2 The Company will establish a system to periodically review and delete or destroy personal data when it exceeds the retention period set by the Company or as specified in procurement and service contract agreements or orders from the data controller, including data that is unrelated or unnecessary

for the purposes of data collection, data for which consent has been withdrawn, or data requested for deletion, unless it is retained for purposes specified by law.

13.3 When the retention period for personal data as defined by the Company has expired, the Company will delete or destroy the data or anonymize it, depending on the nature of the data. The Company establishes a cycle for document destruction, which is necessary annually. For paper-based data, the responsible department for the data is responsible for destroying the data through appropriate shredding equipment. Additionally, for electronic data, suitable technical methods are employed for destruction. If data has been recorded on any device or tool, such as USB or computers, the utmost effort is made to ensure complete destruction of all such data in accordance with the record of data processing activities that has been retained.

13.4 For document management processes, the Company establishes the following procedures:

13.4.1 The department responsible for data and documents must verify documents that have reached the retention period and perform movements, transfers, or destruction in accordance with the Company's retention policy.

13.4.2 When the destruction period is reached, the department must carry out the document shredding, along with filling out the 'Document Destruction Request Form' provided by the Quality Assurance department as evidence of the destruction.

13.4.3 In cases where the Company contracts external service providers for the destruction of personal data that is no longer necessary, the Company requires the establishment of a data processing agreement with these service providers to ensure the complete destruction of data using appropriate techniques, providing assurances of data integrity.

14. Personal Data Security

14.1 The Company establishes data security measures under the principle of preventing loss, unauthorized access, use, alteration, unauthorized modification, or disclosure of personal data within the framework of guarantees, as follows:

14.1.1 All data, especially sensitive personal data, is securely and confidentially retained, considering it as strictly confidential.

14.1.2 All data must be accurate, reliable, and based on information provided by data subjects, without unauthorized alterations.

14.1.3 Data must be readily available when needed.

14.2 The Company records the logs of access and changes to personal data in various sections. Supervisor of Human Resources are responsible for auditing employee log records for any changes to rights.

14.3 In cases the Company uses tools, equipment, or information assets for the storage and processing of personal data belonging to data subjects, regardless of the group, the Company creates a complete register for these assets and imposes restrictions or prohibitions on the use of information assets owned by each employee to ensure data security standards are maintained consistently across all devices and information assets.

14.4 The Company establishes a policy for backing up all important personal data to ensure continuous availability. Data is backed up, tested, and recovery processes are initiated at least once a year or according to the Information Technology department's procedures, ensuring that all processed personal data is accurate, complete, and readily available within the specified timeframe.

14.5 The Company defines processes to control and maintain the security of personal data processing, clearly outlining the responsibilities of external service providers. It establishes standards for selecting external service providers and contracts that define security standards for information systems accessible by external service providers. These standards limit access and usage to what is necessary and provide guarantees for maintaining data security standards identical to those of the Company. In case of any abnormalities or violations, immediate penalties are enforced against the service provider, ensuring no disruption to the Company's service continuity.

15. Personal Data Breach Management

15.1 The Company’s Personal Data Protection Team is responsible for establishing policies and measures to manage and handle incidents that may impact the security of personal data or result in personal data breaches. This team coordinates with relevant departments. The Human Resources department is responsible for reporting and managing such incidents, and other relevant departments participate in the incident management process.

15.2 In the event of a personal data breach, the Personal Data Protection Team is responsible for investigating any actions by data controllers, data processors, employees, or contractors of data controllers or data processors. They report such incidents to the Audit Committee and the Board of

Directors for acknowledge and send to PDPA government agency within 72 hours of becoming aware of the breach. Data subjects are also notified in case of an impact.

15.3 After the conclusion of a personal data breach, the Personal Data Protection Team is responsible for conducting a review and investigation to identify the root cause of the incident. They prepare a report for the board of directors and develop a plan for corrective and preventive actions to mitigate the risk of similar breaches in the future.

16. Review of Personal Data Protection Policy

The Company will consider reviewing and updating the Personal Data Protection Policy at least once a year or in the event of significant changes that affect the Company's business operations. This ensures that the policy remains current, relevant, and acceptable.

17. Publicizing the Personal Data Protection Policy

To inform, educate, raise awareness, and encourage compliance among employees within the Company, the Company communicates the Personal Data Protection Policy, measures, and reporting channels securely as follows:

17.1 The Company disseminates information to all employees through email and the Company's central drive, ensuring that all departments and personnel are aware of the policy and enforces compliance by the personnel mentioned above.

17.2 The Company provides training on the Personal Data Protection Policy to all new employees and conducts regular training for all employees to ensure that they understand the importance of personal data protection. This training also ensures that employees are aware of and comply with the Company's Personal Data Protection Policy. The Company aims to make sure that all employees who are relevant are well-trained and knowledgeable about personal data protection. Additionally, this training is aimed at making the practices accessible to external individuals or interested parties through the cCmpany's website at http://www.aienergy.co.th.

17.3 If any directors, managments, employees, or stakeholders have any questions regarding the Personal Data Protection Policy and measures, they can request additional information from:

17.3.1 Supervisor or Manager of their department

17.3.2 Human Resources department.

Contact Information:	Human Resources Department
	AI Energy Group Public Company Limited
Address:	55/2 Moo 8, Setakit 1 Road, Klong Maduea Subdistrict, Krathum Baen District, Samut Sakhon Province, 74110
Email:	hr@aienergy.co.th
Phone Number:	034-877-485-8

18. Handling of Personal Data Collected before the Effective Date of the Personal Data Protection Act B.E. 2562

For the personal data collected, gathered, used, and/or disclosed by the Company from you in any way due to your relationship with the Company as an employee, contractor, customer, business partner, business associate, shareholder, or member of the company's board of directors or in any other capacity before the effective date of the Personal Data Protection Act B.E. 2562, the Company hereby informs you that the Company will continue to collect, gather, use, and/or disclose your personal data for the same original purposes for which it was collected and used before the effective date of the said Act. The Company will not disclose your personal data to any other individuals, except as required by your written consent or as permitted by law. If the Company intends to collect, gather, use, or disclose your personal data for purposes beyond the original purposes for which it was collected before the effective date of the said Act, the Company will notify you and carry out such actions in accordance with the principles and procedures specified by the Personal Data Protection Act B.E. 2562.

You have the right to withdraw your consent for the Company to continue collecting, gathering, using, and disclosing your personal data for the same original purposes as stated above before the Personal Data Protection Act B.E. 2562 becomes effective, by contacting the Company through the contact channels provided.

19. Contact Information for the Company

If you have any additional questions about the Personal Data Protection Policy, please contact:

Contact Information:	Human Resources Department
	AI Energy Group Public Company Limited
Address:	55/2 Moo 8, Setakit 1 Road, Klong Maduea Subdistrict, Krathum Baen District, Samut Sakhon Province, 74110
Email:	hr@aienergy.co.th
Phone Number:	034-877-485-8

The Personal Data Protection Policy was approved by the board of directors meeting No. 1/2023 on February 17, 2023.

Effective date February 17, 2023

- translate version –

Miss Pimwan Thareratanavibool

Managing Director

- English Translate Version -

Annex

Personal Data Request Form

Data Subject Information

Name – Surname : ……

Address : ……

Email : …… Phone : ……

Type of Data Subject:

☐ Job Applicant / Trainee / Employee ☐ Business Partners and Business Associates ☐ Shareholders

☐ External Individuals Contacted ☐ Contracted Parties ☐ Others (Please specify)……

Intention for Managing Personal Data :

……

……

……

I wish to exercise the following rights regarding the above-mentioned personal data:

☐ Right to Consent ☐ Right to Withdraw Consent ☐ Right to Correct Data

☐ Right to Delete or Destroy Data ☐ Right to Suspend Data Usage ☐ Right to Send or Transfer Data

☐ Right to Access Data ☐ Right to Request Access and/or Copies of Data

I have read and understood the content of this request thoroughly. I confirm that the information provided to the Company is accurate and true. I understand that verification of authority and identity is essential for considering the rights you have requested. The Company may request additional information from me to verify the above for the purposes of ensuring accurate, complete, and lawful access, copying, or disclosure of data in the future.

Signature: .....

(……)

Date: ...../...../.....