



บริษัท เอเชียน มารีน เซอร์วิส จำกัด (มหาชน)

ASIAN MARINE SERVICES PUBLIC COMPANY LIMITED

Personal Data Management Policies and Guidelines

Asian Marine Services Public Company Limited

Asian Marine Services Public Company Limited conducts ship repair, shipbuilding, and engineering structural work. In the course of its business, the Company may need to collect, use, disclose, and transfer personal data to external personnel, which could directly or indirectly identify individuals. The Company prioritizes the right to privacy and the protection of personal data belonging to its Board of Directors, executives, shareholders, employees, customers, partners, contractors, job applicants, and all other parties with whom it conducts business. In order for the aforementioned personal data to be protected and prevented to incur the minimum risk of damage, the Company has therefore formulated these policies and guidelines, with the details as follows:

1. Definitions

Personal data refers to information relating to a person, which enables the identification of such person, directly or indirectly, but does not include information about a deceased person in particular.

Sensitive information refers to personal data that is particularly sensitive and at risk of being used for unfair discrimination. This includes data relating to race, ethnicity, political opinions, religious or philosophical beliefs, sexual orientation, criminal history, health data, disability, trade union information, genetic data, biometric data, or any other data that could adversely affect the data subject.

Data subject refers to an individual who can be identified from personal data, directly or indirectly. This includes the Company's directors, executives, shareholders, employees, job applicants, temporary staff, interns, customers, contractors, business partners, and visitors.

Data controller refers to a person or legal entity with the authority to make decisions regarding the collection, use, or disclosure of personal data.

Data processor refers to a person or legal entity who processes personal data on behalf of a data controller, including collecting, using, or disclosing it.

Data Protection Officer refers to a person or legal entity who controls or processes personal data, and is appointed to advise on and oversee operations to ensure the collection, use, and disclosure of personal data comply with government regulations, as well as to coordinate with the Office of the Personal Data Protection Committee established by the authorities.

2. Objectives

2.1. To establish operational guidelines in compliance with the Personal Data Protection Act B.E. 2562 (2019).

2.2 To establish consistent guidelines for the collection, use, disclosure, protection, retention, and destruction of personal data.

2.3 To ensure that the Company's directors, executives, shareholders, employees, customers, business partners, contractors, visitors, job applicants, temporary employees, and interns are confident that their personal data provided to the Company will be protected in accordance with the Personal Data Protection Act B.E. 2562 (2019).

3. Responsibilities

3.1 The Board of Directors

3.1.1 Establish policies and guidelines for personal data protection.

3.1.2 Promote and support the proper implementation of these policies and guidelines.

3.2 Executives

3.2.1. Establish measures and operating methods concerning personal data within the Company to comply with applicable laws, policies, and these guidelines.

3.2.2. Designate departments or individuals responsible for implementing these policies and guidelines.

(1) Establish relevant guidelines or operational manuals.

(2) Supervise, control, monitor, and inspect operations to ensure they are carried out in accordance with relevant policies and operational manuals.

3.3 Responsible Department/Person/ Data Protection Officer

3.3.1 Inform data subjects to acknowledge the objectives of collecting, using, and disclosing their personal data before or at the time of collecting the personal data, as well as the various rights of the data subject.

3.3.2. Process requests from data subjects to exercise their rights, such as correcting, changing, and/or deleting or destroying personal data as requested by the data subject, and maintain a complete record and evidence of these actions.

3.3.3 Store, maintain, and prevent the use or disclosure of personal data, in accordance with the objectives that the Company has informed the Data Subject or for which the Data Subject has given consent.

4. Scope of Enforcement

4.1 These policies and guidelines shall be enforced on all employees of the Company and its subsidiaries.

4.2 This Personal Data Protection Policies cover all data processing activities, from the collection, use, and disclosure of data to its destruction and the exercise of rights of the data subject.

4.3 Protection of the personal data of all data subjects, as defined in Section 1.

5. Operating principles as follows:

5.1 Collection, Use, and Disclosure of Personal Data

For the collection, use, and disclosure of personal data, the Company must obtain explicit consent from data subjects, including sensitive data. In case of visitors to the Company's website, such persons shall be deemed to have already given consent to collect and use personal data. The Company will collect, use, and disclose personal data only to the extent necessary for its operations and in accordance with the objectives outlined in its policies, which is in compliance with the rules prescribed by the Personal Data Protection law, such as:

1. To comply with the contract or request of the data subject.
2. To comply with laws which the Company must comply with.
3. For the legitimate interests of the Company.
4. For the public benefit
5. To prevent harm to the life, body, or health of the data subject.
6. To assist in resolving legal disputes, disciplinary processes, or grievances.
7. To take any other actions related to achieving the objectives of the CCTV system.
8. In accordance with the consent of the data subject.

The Company may collect sensitive personal data for the following objectives:

1. Biometric data, such as facial recognition data, fingerprint recognition data, and iris recognition data, as well as voice identity data, is used to verify the identity of the data subject and support the identity verification process required by anti-money laundering laws.
2. The motion data recorded by CCTV cameras is intended to prevent and mitigate harm to life, body, health, and safety of employees, interns, customers, contractors, and visitors. The Company provides notice of the

image recording and allows data subjects the opportunity to “not consent” or “request the Company to delete data” later through the consent withdrawal process or the exercise of various rights.

In cases of legal exceptions, or general information under contract standards such as submitting data to the Revenue Department or handling sensitive information not subject to consent requirements, like health data used for disease prevention, the collection, use, and disclosure of personal data do not require the data subject’s consent.

The Company will collect, use, and disclose personal data for benefits directly related to the objectives of the collection and use. The Company must inform data subjects before or at the time of collection about the details of the collection, as follows:

1. Objectives of the collection
2. Collected personal data
3. Potential impacts of not providing personal information
4. Persons or agencies to whom the collected personal data of the data subject may be disclosed.

Rights of the Data Subject

1. Right to be informed
2. Right to request access to personal data
3. Right to request access to and transfer personal data
4. Right to object to the collection, use, or disclosure of personal data.
5. Right to request the deletion or destruction of personal data.
6. Right to withdraw consent
7. Right to request a halt to data use
8. Right to rectification or change of data to be correct, complete, and up to date.

The collection of personal data will be used only for the notified objectives. Any change to or addition of objectives must obtain prior consent from the data subject, except as prescribed by law.

The Company has the duty to notify the objectives, the sending or transferring of data to external personnel (if any), and the rights to the data subject prior to or at the time of collecting personal data.

Collecting personal data from sources other than directly from the data subject **is prohibited.**

5.2. Personal Data Protection, Retention, and Retention Period Measures

5.2.1 The Company employs appropriate measures to maintain the accuracy, currency, and reliability of personal data, protecting it from destruction, alteration, and unauthorized access.

5.2.2. The Company implements appropriate personal data security measures to ensure that personal data shall be protected and safeguarded as required by law. These measures include preventing loss, leakage, unauthorized access, unlawful processing or transfer, and accidental loss.

5.2.3 The Company will retain personal data only as necessary for the objectives for which it was collected, used, and disclosed as notified to the data subject, until the data subject's relationship with the Company ends or as required by law.

5.2.4 The Company must review these measures as needed or when technology evolves, to maintain appropriate security efficiency.

5.2.5 Documents for which no transactions are executed, such as rejected job applications, price quotations, and proposals that did not result in a sale or business deal, will be retained for no more than 2 years.

5.2.6. Documents used in working or conducting business, such as the data of employed employees, will be retained during employment and for at least 5 years after the termination of employment. The data of customers and business partners conducting business together shall be retained throughout the period of business, and for no less than 10 years after the termination of business.

5.3. Channels for Exercising Rights of the Data Subject

5.3.1 Provide channels for receiving requests to exercise the rights of data subjects, through the channels designated by the Company.

5.3.2. Maintain records of requests to exercise rights by data subjects, including the grounds for refusal in cases where requests are not fulfilled, as evidence required by law.

5.4. Deletion or Destruction of Personal Data

5.4.1. Personal data that exceeds the period specified by the Company for retention, or cases where the Company does not have rights or cannot claim a lawful basis in processing the personal data of the data owner, the Company will proceed to destroy that personal data.

5.4.2. Personal data is no longer necessary to store for the stated purpose.

5.4.3. The data subject withdraws consent for the collection, use, or disclosure of personal data, and the Company no longer has the legal authority to collect, use, or disclose that personal data.

6. Complaints and Notification of Personal Data Breaches

The Company provides processes and channels for reporting personal data breaches. The Data Protection Officer will assess and collect personal data and notify the Personal Data Protection Committee within 72 hours of becoming aware of the incident. If the breach impacts the rights and freedoms of data subjects, they will be notified of the cause of the breach and available remedies without delay.

7. Training

7.1. To ensure all employees are adequately informed, the Company will take appropriate actions to make employees are informed of and aware of personal data protection.

7.2 Employees responsible for processing personal data must be trained and build understanding regarding personal data protection.

8. Policy Review

The Company will review its policies as appropriate to ensure compliance with applicable laws, regulations, rules, practices and changing circumstances.

9. Cookies and the Use of Cookies

Visiting the Company's website may involve placing cookies on visitors' devices and automatically collecting data. Some cookies are necessary for the website to function correctly, while others are used to facilitate the website visitors. Further details are available in the Company's cookie policies.

10. Contact Channels

Asian Marine Services Public Company Limited, 128 Moo 3, Laem Fha Pha Subdistrict, Phra Samut Chedi District, Samut Prakan 10290, Telephone: 02 8152060, Website: www.asimar.com, Email: dpo@asimar.com