I. Objective of the Data Privacy Policy

As part of its social responsibility and adherence to Republic Act 10173, otherwise known as the Data Privacy Act of 2012, its implementing rules and regulations as well as in compliance with international data protection laws, Döhle Seafront Crewing (Manila) Inc. has adopted this Data Privacy Policy to ensure adequate level of data protection and to safeguard personal information collected, processed, and managed in line with its business of supplying qualified seafarers internationally.

This Data Protection Policy provides the primary framework, conditions for data collection, its processing, management, cross-border transmission, and disposal.

II. Scope of the Data Privacy Policy

This Data Protection Policy applies to all processed personal data contemplated under the Data Privacy Act by: a) Döhle Seafront Crewing (Manila) Inc.; b) its branches; and, c) 3rd Party service providers whom Döhle Seafront Crewing (Manila) Inc. has outsourcing agreements to process data in line with its nature of business as a crewing and manning agency.

III. Definition of Terms:

- **Data Privacy Act (DPA)** – Republic Act 10173 otherwise known as the Data Privacy Act of 2012, including its Implementing Rules and Regulations, and other circulars or issuances in relation thereto;
- **Data Subjects** – Individuals whose personal, sensitive personal, or privilege information is processed;
- **Consent (of the Data Subject)** – any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;
- **Company** – Döhle Seafront Crewing (Manila) Inc.;
- **Processing** – Any operations or set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;
- **Data Sharing** - the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes

outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

- **Personal Information** – Any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify and individual;
- **Privileged Information** – refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication;
- **Sensitive Personal Information -** refers to Personal Data:

    - About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    - About an individual's health, education, genetic or sexual life, or to any proceeding for and offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
    - Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
    - Specifically established by an executive order or an act of Congress to be kept classified.

- **Security Incident -** is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;
- **Personal Data Breach** –breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
- **Personal Information Controller (PIC) -** refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

    - A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
    - A natural person who processes personal data in connection with his or her personal, family, or household affairs;

    There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

- **Personal Information Processors (PIP)** - refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

IV. Principles of Processing Personal Data

1. **Transparency** - The Company shall ensure the data subjects are duly informed of how personal information is being handled. As a general rule, personal data shall be collected directly from the individual himself.

   When data is collected, the data subject shall be made aware or informed of the company of the following:

   i. The identity of the Personal Information Controller;
   ii. The purpose of the data being collected;
   iii. Personal Information Controllers or categories of third parties to whom the data subject's data will be transmitted and processed;
   iv. The risks and safeguards involved; and,
   v. His or her rights as a data subject.

2. **Legitimate Purpose** - The processing or acquisition of personal information shall be compatible with a declared and specified purpose in processing or acquiring the same, which must not be contrary to law, morals, or public policy. When collecting and processing personal data, the Company shall ensure that individual rights of data subjects are protected according to law and fair play.

   Collection must be for a declared, specified, and legitimate purpose:

   i. Consent of data subject is absolutely required prior the collection and processing of his or her personal data.
   ii. Consent shall be time bound in relation to the declared, specified and legitimate purpose explained by the Company to the data subject.
   iii. Regardless of purpose or legitimacy of data acquired, except under special circumstances, the personal data of data subject cannot be further processed if he or she withdraws consent previously given.

3. **Proportionality** - The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. As such, personal data can be processed only for the purpose/s that was/were defined before the data was collected. In case of subsequent changes in the purpose/s, the Company shall duly inform the data subjects concerned of the said changes and secure their consent for the same.

4. **Data Management** – The Company shall ensure that processing of personal data is necessary and limited to its intended purpose. Wherever possible, the use of statistical and anonymized data will be preferred to ensure personal data is not conveyed when such will result in achieving the same required purpose or objective.

Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods. Further processing (or intention to do so) must likewise be communicated to the data subject in order to acquire his or her valid consent.

5. **Disposal of Personal Data** – Subject to exceptions, after the legitimate purpose of the data has been completed or when processing relevant to the purpose has been terminated, the Company shall ensure the personal data collected is timely deleted. The Company shall ensure to evaluate captured personal data to determine if the same has served its purpose and thus can be deleted.

   The Company shall ensure that personal data shall be deleted in a secure manner to prevent further processing, unauthorized access, or disclosure to any party or the public that would prejudice the interest of the data subject.

   Personal data shall not be collected or retained in perpetuity in contemplation of a possible future use yet to be determined; except in cases where the Company can anonymize personal data used, without any trace to its specific data subject. In this regard, the Company must absolutely ensure complete anonymization and security of such data processes.

6. **Data Accuracy and Timeliness** – The Company shall ensure that personal data collected and kept on file is up to date, correct and complete. Inaccurate, incomplete data shall be timely corrected, deleted, supplemented or updated.

7. **Security and Confidentiality** – The Company shall maintain the highest level of confidentiality and security over the personal data collected. Suitable organizational and technical security above or on par with industry standards must be provided to prevent or immediately recover from data breaches.

V. Collection, Processing, Retention of Personal Data

Döhle Seafront Crewing (Manila) Inc., as a licensed manning agency organized under Philippine Law with its function as a crewing arm of the Döhle Group and other principal partners engaging in the recruitment and placement of seafarers globally shall collect, process, and retain personal data to achieve on the following legal purposes:

1. Customer/Partner Personal Data

i. Contractual relations – Personal data of the relevant prospective clients, customers and partners shall be processed by the Company to establish, execute and terminate contracts and agreements.

ii. Consent to data processing – Consent shall likewise be required. Declaration of consent shall be in writing, whether by hand or electronically. Any verbal

or telephonically conveyed consent shall be documented and attested to by the party whose consent is given.

iii. Legal request – Processing of a data subject's data for a party other than the data subject him/herself shall be allowed when in compliance with a lawful order of a legal authority.

iv. Privileged and sensitive data processing is only allowed if the law requires or when the data subject has provided his or her express consent. Privileged and sensitive data can likewise be processed when necessary for exercising or defending legal claims.

v. Use of internet or data when personal data is being collected – The Company shall ensure that personal data processed and collected with the use of websites and apps that the data subjects are informed through a privacy statement including cookies information.

2. Employee Personal Data (Sea and Shore)

i. Employment data processing – personal data maybe collected in order to recruit, carry out and terminate employment relations. During the recruitment phase, when an applicant is rejected, his or her data may be kept for purposes of a recruitment data bank, with the consent of the applicant.

ii. Data processing for employment shall always relate to the purpose of the employment agreement.

3. Sharing of Personal Data to 3rd Party

Data processing through a PIP is allowed provided that the following requirements are complied with:

i. The data sharing between the PIC and the PIP is covered by a **data sharing agreement**;

ii. The PIP has the competence and qualification to ensure personal data captured though its engagement with Döhle Seafront is kept secured, and adequate protective measures has been in placed by the PIP in the protection of personal data.

iii. Contractual obligations of the PIP in data protection are upheld.

iv. Prior to the data processing contract being initiated, the PIP has demonstrated to the PIC's satisfaction that the PIP is capable and qualified to process personal data which must be documented.

v. Regular inspections are conducted by the PIC to 3rd Party entities to validate compliance with privacy laws.

VI. Rights of the data subjects

1. **Right to be informed.**
   i. The data subject has a right to be informed whether personal data pertaining to him/her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
   ii. The data subject shall be notified and furnished with information indicated hereunder before the entry of his/her personal data into the processing system of Döhle Seafront, or at the next practical opportunity.
      a. Description of personal data to be entered into the system;
      b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
      c. Basis of processing, when processing is not based on the consent of the data subject;
      d. Scope and method of personal data processing;
      e. The recipient or classes of recipients to whom the personal data are or may be disclosed;
      f. Methods utilized for automation access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about logic involved, as well as the significance and envisage consequences of such processing for the data subject;
      g. The identity and contact details of the personal data controller or its representative;
      h. The period for which the information will be stored; and
      i. The existence of their rights as data subjects, including the right to access, correction, and object to processing, as well as the right to lodge a complaint.

2. **Right to object.** The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

   When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

i. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
ii. The information is being collected and processed as a result of a legal obligation.

3. **Right to Access.** The data subject has the right to reasonable access, upon demand or request, to the following:
    i. Contents of his or her personal data that were processed;
    ii. Sources from which personal data were obtained;
    iii. Names and addresses of recipients of the personal data;
    iv. Manner by which such data were processed;
    v. Reasons for the disclosure of the personal data to recipients, if any;
    vi. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
    vii. Date when his or her personal data concerning the data subject were last accessed and modified; and
    viii. The designation, name or identity, and address of the personal information controller.

4. **Right to rectification.** The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, that recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

5. **Right to Erasure or Blocking.** The data subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal data from the personal information controller's filling system.

    i. This right may be exercised upon discovery and substantial proof of any of the following:
        a. The personal data is incomplete, outdated, false, or unlawfully obtained;

b. The personal data is being used for purposes not authorized by the data subject;
c. The personal data is no longer necessary for the purposes for which they were collected;
d. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
e. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
f. The processing is unlawful;
g. The personal information controller or personal information processor violated the rights of the data subject;

ii. The personal information controller or personal information processor violated the rights of the data subject.

6. **Right to damages.** The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

7. **Transmissibility of Rights of the Data Subject.** The lawful heirs and assigns of the data subject may invoke the rights of the data subject, to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding numbers.

8. **Right to Data Portability.** Where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of the data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

VII. Confidentiality

All employees and agents acting on behalf of the Company, including sub-contractors shall keep all personal data obtained through the course of employment in confidentiality. Any unauthorized collection, processing, retention undertaken during the time of employment or contract is prohibited and the Company reserves the right to pursue all legal remedies for violation of the personal data confidentiality.

The Company has adopted a “information segregation” principle where employees, agents, sub-contractors shall only have access to personal information only as appropriate for the scope of work and the execution of the purpose it is intended. The Company shall in reasonable periodicity review the access rights of individuals mentioned herein and shall correct, mitigate to ensure compliance thereto.

All employees, agents and sub-contractors are prohibited to use personal data for private or commercial purpose, sharing to third persons unauthorized, or to make it available in any other way which is not for its intended purpose.

VIII. Security Measures and Breach Reporting

The Company, through its employees, agents and sub-contractors involved in the processing of personal data is mandated to safeguard personal data from unauthorized access and processing or disclosure, including accidental loss, destruction and modification for both soft and hard files of personal data.

Where new methods or systems are in place for personal data collection, processing, retention, using electronic means or IT platforms, the Company shall ensure appropriate safeguards to IT security is in place, and such circumstance is ascertained by the company IT manager.

In the event that there is a breach, un-authorized access or processing personal data or signs thereof, the Company employees, its agents, sub-contractors are obligated to report the same within 24 hours of its discovery to the company DPO from the time of his or her knowledge of the breach or potential breach to personal data of data subjects.

All personal data security incidents shall be verified and recorded and accordingly reported within the regulatory timeline or sooner as imposed by applicable laws.

IX. Outsourcing and sub-contracting

When new data sharing agreements has been entered by the Company as allowed in applicable laws e.g. outsourcing, etc., the contract or agreement shall include express stipulations requiring the external party the following:

i. Processing of personal data shall only be upon documented instruction of the Company, including transfers of personal data to another country or organization unless required by law;
ii. Confidentiality obligation is imposed upon the persons and employees authorized by the external agent/entity and subcontractor to process the personal data;
iii. Develop and implement appropriate security measures;
iv. Comply with the Data Privacy/Protection laws locally and under international standards;
v. Not to engage another processor (sub-contracting) without prior instruction from the Company: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
vi. Assist the Company, by appropriate technical and organizational measures and to the extent possible, fulfill the obligations to respond to request by data subjects relative to the exercise of their rights;
vii. Assist the Company in ensuring compliance with the Act, these Rules, other relevant laws, taking into account the nature of processing and the information available to the personal information processor.
viii. At the choice of the Company, delete or return all personal data to the latter after the end of the provision of services relating to the processing, provided that this includes deleting existing copies unless retention is justified and allowed by law.
ix. Make available to the Company, all information necessary to demonstrate compliance with the obligations laid down by law, and to allow for and contribute to audits, including inspections, conducted by the Company or another auditor mandated by the latter.
x. Immediately inform the Company if, in its opinion, an instruction violates applicable privacy laws.

X. Data Protection Officer

The Data Protection Officer (DPO) shall be responsible for ensuring the Company's compliance with applicable laws and regulations on data privacy/protection. The DPO shall regularly check via verification audits, risk assessments and reviews as well as other generally accepted modes of verification that appropriate control measures are in place.

The DPO, being internally independent shall perform the following functions:

i. Monitoring the Company's compliance model for data privacy and protection with applicable local and international laws.

ii. Act as liaison between the Company and other regulatory institutions, and is in charge of the applicable registration, notification, and reportorial requirements mandated by laws on data privacy/protection based on local and international laws as applicable.
iii. Develop, establish, and review procedures and policies for the exercise by data subjects of their rights in data privacy.
iv. Act as primary contact for data subjects to coordinate and consult with all concerns relating to their personal data.
v. Formulate capacity building, orientation and training programs for employees, agents or representatives of the company regarding personal data privacy and security.
vi. Prepare and file reports as mandated by applicable laws on data privacy and protection.

XI. Effectivity

The provisions of this Policy are effective this 1st day of January, 2018, until validly revoked or amended by this Company.