CH OFFSHORE LTD

CORPORATE OPERATING PROCEDURES

Personal Data Protection Policy

Revision	Date	Remarks	Document and Revision number	Prepared	Approved
1	15 May 2023	Approved for Use	CHO-SOP-CORP-002	LC	Board

This is a Controlled Document
All queries, suggestions, interpretation, clarification or change request shall be addressed at the first instance to the Corporate Manager or if unavailable, his delegate.

Table of Contents

1.0 PURPOSE

1.1 CH Offshore Ltd. and its subsidiaries (collectively known as “CHO Group” or “Group”) recognise both the rights of individuals to protect their Personal Data (defined herein) and the needs of the Group to collect, use or disclose Personal Data for legitimate business and legal purposes only. We are committed to protecting your Personal Data and aim to treat your Personal Data with confidentiality and care.

1.2 The objective of this Personal Data Protection Policy (“PDPP” or “Policy”) is to set out the systems, policies and processes on data protection and the legal conditions that must be satisfied in relation to the collecting, handling, processing, storage, transportation and destruction of personal information in compliance with the requirements of the Personal Data Protection Act 2012 (“PDPA”).

1.3 This Policy also seeks to develop a process to receive and respond to complaints that may arise with respect to Personal Data.

1.4 The Group today operates in an increasingly connected and competitive digital economy where individuals’ online and real-world activities generate a burgeoning amount of data. As the business environment evolves, the Group understood the importance to shift from a compliance-based approach to an accountability-based approach in managing Personal Data. This acknowledgement and change have helped the Group strengthen trust with the public, enhance business competitiveness and provided greater assurance to our customers, all of which are essential factors for the Group to thrive in the digital economy.

2.0 SCOPE

2.1 This Policy applies to all departments, business units and subsidiaries within the Group as well as individual employees and board members of the Group and any third-party service provider who agrees to abide by this Policy by way of contract.

2.2 This Policy applies to all Personal Data collected on paper, on a computer or other storage media by the Group.

2.3 This Policy does not form part of any employee’s contract of employment and may be amended from time to time. Any breach of this Policy will be taken seriously and may result in disciplinary action up to and including dismissal of any of our employees. If an employee considers that the Policy has not been followed in respect of Personal Data about themselves or others, they should raise the matter with their manager as soon as possible.

2.4 The Group may designate one or more individuals to be responsible for ensuring that the Group complies with the Personal Data Protection Act. The Group will make available to the Public the Business Contact Information (defined herein) of the Designated Protection Officer (“DPO”). The designation of a DPO does not relieve the Group of its obligations under the PDPA.

2.5 This Policy does not apply to an individual acting in a personal or domestic capacity.

3.0 POLICY STATEMENT

3.1 During the course of the Group’s business activities, we may collect, store, use or disclose Personal Data of employees, crew, directors, customers, suppliers, vendors, clients, shareholders and other stakeholders and we recognise the need to treat such personal information in an appropriate and lawful manner. We are committed to complying with our legal obligations in this regard in respect of

all Personal Data we handle. We will only collect Personal Data that is relevant to our business and legal purposes and/or employment relationship with our employees, crew and other stakeholders.

4.0 DEFINITIONS

4.1 "Personal Data" refers to data about a non-corporate individual who can be identified from that data or from that data and other information that the Group has or is likely to have access to. Personal Data can be factual (such as name, address or date of birth) or it can be an opinion (such as a performance appraisal). Personal Data can be in the form of any electronic and non-electronic media.

4.2 Personal Data includes, but is not limited to the following:

a) Personal details
Name, gender, nationality, race, marital status, date of birth, place of birth and details of any criminal record.

b) Identification information / documents
Copies of NRIC, passport, visa and work pass

c) Contact details
Telephone number, mobile number, email address, home address

d) Photograph or Video images
Photographs (including Passport Size photographs) and video images taken at Company's events.

e) Voice Recording

f) Thumbprint

g) Next-of-kin details
Name, relationship with employee/seafarer, telephone number, email address and home address.

h) Medical information / Medical declaration
Copies of medical fitness and details of any disability (for insurance / internal & external claims purposes)

i) Academic certificates / Certificate of competency / Testimonial
Copies of academic certificates, certificate of competency and testimonial

j) Flag State documents
Flag state endorsement and seaman books

k) Training certificates
Copies of STCW and any other training certificates required for the position employed

l) Bank information
Bank account details (for salary crediting purposes)

m) Previous employment information

Previous employer(s), previous work experience and previous remuneration information (including bonuses, benefits and perks)

n) Immediate Family's Particulars (Dependent, Spouse)
Name, NRIC/passport, date of birth, nationality, relationship to employee, occupation, copies of childbirth certificate, marriage certificate, death certificate, adoption certificate, medical records/medical declaration, etc., for leave entitlement and medical insurance coverage

o) Referees' contact details
Referees' telephone number, mobile number and email address

4.3 This Policy does not apply to:

a) Business Contact Information.
b) Personal Data in relation to a deceased individual who has been dead for more than 10 years.
c) Publicly available information which cannot be associated with an individual or which has been anonymised.

4.4 "Data Protection Officer ("DPO")" refers to the person appointed by the Group to ensure compliance of the PDPA.

4.5 "Data Users" include employees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following the Group's Policy at all times.

4.6 The main Data Users within the Group include, but are not limited to:

a) HR/Admin department
b) Corporate department
c) HSE department
d) Crewing department
e) Senior Management
f) Corporate Secretary

4.7 "Data Intermediary" refers to an individual or organisation that processes Personal Data on behalf of another organisation but does not include an employee of that other organisation for example our insurance broker. The Group must ensure that contracts entered into with Data Intermediaries include references to their Personal Data Protection Policy and sets out clearly the purposes of the contract, the roles and responsibilities of each party obligations of the Data Intermediaries when processing Personal Data and the retention / cessation requirements of Personal Data.

Data Intermediaries would include, but are not limited to:

a) Travel agent for booking of flights and arranging of visas
b) Hotel accommodation booking for business travel
c) Embassies and High Commissions for visa application
d) Port agents for arrangement of immigration formalities and transportation to/from airport
e) Charterers and shipowners for operational purposes such as arrangement of work permit in the countries where the vessel operates, approving marine crew for offshore projects and for coordinating logistics
f) Government departments or authorities for compliance purposes/regulatory obligations (e.g., CPF, IRAS, MOM, ICA, MSF, Flag States, Labuan FSA, SSM/CCM, etc.)
g) Banks for salary crediting
h) Banks authorised signatories/Banks for providing business internet banking user rights

i) External Company Secretary
j) Insurance broker/Insurance Company for insurance coverage
k) Training centres for providing of training courses

4.8 "Processing" is the carrying out of any operation or set of operations in relations to the Personal Data, such as:

- Recording
- Holding
- Organisation
- Adaptation or alteration
- Retrieval
- Combination
- Transmission
- Disclosing
- Erasure; or
- Destruction

4.9 "Business Contact Information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual not provided by the individual solely for his personal purposes.

5.0 INCREASED FINANCIAL PENALTY

5.1 An increased financial penalty for contraventions of the PDPA will apply. The quantum of the penalties will be 10% of the Gross annual turnover in Singapore or S$1 million, whichever is higher. This came into effect on 1 February 2021.

6.0 OFFENCES FOR MISHANDLING PERSONAL DATA ON BEHALF OF AN ORGANISATION OR PUBLIC AGENCY

6.1 Effective 1 February 2021, a new offence to hold individuals accountable for mishandling Personal Data on behalf of an organisation or public agency came into play. The offences include one or more of the following:

- Any unauthorised disclosure that is carried out knowingly or recklessly
- Any unauthorised use of Personal Data knowingly or recklessly and results in a wrongful gain or a wrongful loss to any person
- Any unauthorised re-identification of anonymized information

6.2 On conviction, the individual is liable to a fine not exceeding S$5,000.00 or to imprisonment for a term not exceeding 2 years or both.

7.0 DATA PROTECTION OBLIGATIONS

7.1 Anyone processing Personal Data must adhere to the following ten (10) obligations:

a) Consent Obligation

b) Purpose Limitation Obligation
c) Notification Obligation
d) Access & Correction Obligation
e) Accuracy Obligation
f) Protection Obligation
g) Retention Obligation
h) Transfer Limitation Obligation
i) Openness Obligation
j) Data Portability Obligation (this will take effect when the Regulations are issued - end 2021)

8.0 CONSENT OBLIGATION

8.1 The Consent Obligation prohibits organisations from collecting, using or disclosing an individual's Personal Data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his Personal Data. Exceptions to obtaining consent can occur only if such exception is authorised under the PDPA or any other written law.

8.2 The nature and type of data the Group collects, and the source of such data varies depending on the nature of the relationship the Group has with the data subject. The use of Personal Data includes, but is not limited to:

a) Recruitment and selection
- To evaluate applications for employment and make decisions in relation to selection of employees/seafarers
- Pre-employment screening, including, but not limited to reference checks and criminal record checks
- For recruitment and provision of contracts of employment

b) Management of employees'/seafarers' relationship with CHO Group, for safety and security reasons and to support charterers' manpower (where applicable)
- For ongoing employment and performance appraisal purposes
- To provide and administer remuneration, benefits and incentive schemes
- To comply with regulatory and legal requirements
- To manage grievances, allegations (e.g., whistleblowing, harassment), complaints, investigations and disciplinary processes, and making related management decisions

c) Management of Company related publications / CCTV footage
- To manage and maintain the CHO website and CHO Annual Report
- To manage and maintain CCTV footage for health & safety and security purposes

d) Management of shareholder lists
- To manage general meetings
- To pay dividends
- To send out documents including the CHO Annual Report

Including for all other purposes incidental and associated with the above.

8.3 The Data Inventory Map (Appendix 1A & 1B) shows the types of Personal Data collected, who collects the data, how and why the data is collected, when consent is obtained, when the data subject is notified of the purpose, who the data users are, to whom the Personal Data is disclosed to and their respective retention period. The Data Inventory Map will be reviewed annually and updated as and when required.

8.4 Third parties from whom the Group collects Personal Data should be able to provide consent for the collection, use and disclosure of Personal Data on behalf of the individual or demonstrate that the third-party source had obtained consent for the disclosure of the Personal Data. Examples of such third parties would be crew manning agencies or HR agencies.

8.5 Consent can be obtained in a number of different ways, namely:

a) Verbal Consent

In accordance with best practice, the Group should obtain consent in writing or recorded in a manner that is accessible for future reference.

b) Written

Written consent can be provided by the individual signing a consent form or signing a broader document within which consent for provision of Personal Data is identified.

c) Deemed consent

- By conduct

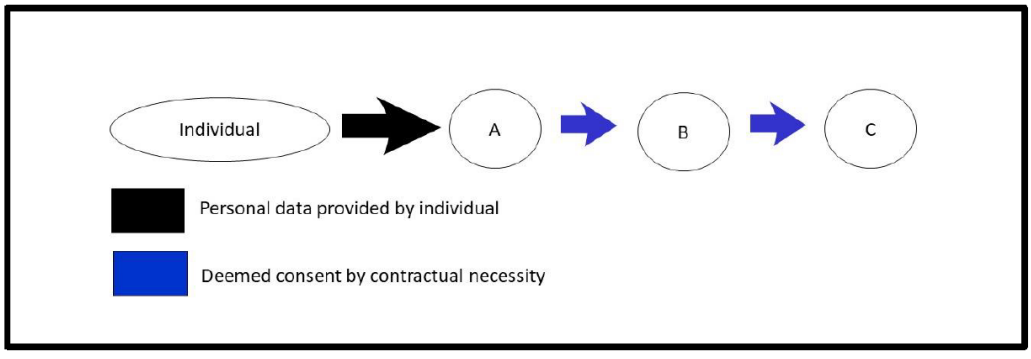
(i) When an individual voluntarily provides Personal Data to the Group for a particular purpose, it is reasonable to assume that the individual has provided deemed consent for the use of the Personal Data for that particular purpose.

(ii) When an individual voluntarily takes certain actions that allow the Personal Data to be collected, without providing the data himself. Consent is deemed to be given to the extent that the individual intended to provide his data and took the action required for the data to be collected by the Group

- By contractual necessity

(i) Consent is deemed where an individual provides his Personal Data to the Group for the purpose of a transaction, and it is reasonably necessary for the Group to disclose the Personal Data to another organisation ("B") for the necessary conclusion or performance of the transaction between the individual and the Group. Deemed consent by contractual necessity extends to disclosure by B to another downstream organisation ("C") where the disclosure (and collection) is reasonably necessary to fulfil the contract between the individual and the Group. To be clear, deemed consent by contractual necessity allows further use or disclosure of Personal Data by C and other organisations downstream (refer to Diagram 1 below) where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and the Group.

Diagram 1:



- By notification

(i) Consent is deemed where an individual consented to the collection, use or disclosure of Personal Data for a purpose that he had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his Personal Data. Deemed consent by notification is useful where the Group wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the Personal Data for, and it is unable to rely on any of the exceptions to consent (e.g. business improvement, research) for the intended secondary use. This is subject to the Group assessing and determining that the following conditions are met, taking into considerations the types of Personal Data involved and the method of collection, use or disclosed:

(a) Conduct an assessment to eliminate or mitigate adverse effects
(b) The Group must take reasonable steps to ensure that notification provided to individuals is adequate
(c) The Group must provide a reasonable opt-out period

(ii) After the opt-out period has lapsed and the individual no longer wishes to consent to the purpose, the individual can withdraw his consent for the collection, use or disclosure of Personal Data

(iii) Under the Personal Data Protection Regulations 2021, the Group must retain a copy of its assessment throughout the period that the Group collects, uses or discloses Personal Data based on deemed consent by notification.

8.6 Exceptions to consent

a) Legitimate interest

- When necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual
- Where data is processed for the purposes of detecting or preventing illegal activities(e.g., fraud or money laundering)
- Preventing threats to physical safety and security
- Ensuring IT and network security, or preventing the misuse of services
- Publicly available data
- Necessary for evaluation purposes
- Recovery or payment of debt owed

"investigation", "proceeding" and "publicly available" are defined in the PDPA.

To rely on this general exception, the Group will need to assess the adverse effect and ensure the legitimate interest outweigh any adverse effect. The Group, in relying on the legitimate interests exception to collect, use or disclose Personal Data must make it known to individuals that they are relying on this exception to collect, use and disclose Personal Data without consent.

b) Business Improvement

This exception applies to the Group under the following circumstances:

- Carry out operational efficiency and service improvement
- Develop or enhance products/services
- Know more about the Group's customers

c) Revised Research Exception

This exception applies to institutes carrying out scientific research and development, or arts and social science research, or to market research aimed at understanding potential customer segments.

This exception DOES NOT apply to the Group.

8.7 If ad-hoc requests for the disclosure of Personal Data are made to the Company which are not covered by the scenarios as per the Data Inventory Map, specific consent should be sought from the individual in writing prior to the disclosure of the Personal Data. Examples of such requests include:

a) Bank reference checks (when employees apply for bank loans)
b) Employment references (when employees apply for positions in other companies)

8.8 Consent Withdrawal Process

8.8.1 The Group is aware that individuals have the right to withhold their Personal Data and may withdraw their consent to the collection and processing of Personal Data.

8.8.2 Individuals who wish to withdraw consent to the use of their Personal Data may do so at any time by submitting their withdrawal request to the DPO through email or post (contact details can be found in Clause 0).

8.8.3 If the Personal Data is used for multiple purposes, the individuals can withdraw consent for a specific purpose without concurrently withdrawing consent for the other purposes.

8.8.4 In situations where stakeholders had consented to the use of their Personal Data (including photographs) in Group promotional material (e.g. brochures) and Group Annual reports, and such consent is subsequently withdrawn, the Group will not be required to recall copies of such material and will be permitted to distribute such material that has already been printed. The Group will also be permitted to continue to use and publish (on company website) soft copies of such material.

8.8.5 Upon receiving withdrawal notice,:

a. The DPO must inform the individual of the likely consequences of withdrawing their consent which could include the discontinuation of provision of services or termination of employment or business relationships;

b. If the individual still wishes to proceed with the withdrawal of consent, the DPO must inform the individual that the withdrawal of consent will take at least ten (10) business days from the day the Group receives the withdrawal notice, to become effective;

c. The Group must cease collecting, using or disclosing the Personal Data, as the case may be, unless the collection, use or disclosure of the Personal Data without consent is required or authorised under the PDPA or any other written law; and

d. The DPO must inform all Data Intermediaries about the withdrawal of consent and ensure that they cease collecting, using or disclosing the Personal Data.

8.9 The Group must not prohibit withdrawal of consent, although this does not affect any legal consequences arising from such withdrawal.

8.10 The withdrawal of consent for the collection, use or disclosure of Personal Data does not require the Group to delete or destroy the individual's Personal Data. The Personal Data can still be retained in accordance with the Retention Limitation Obligation.

9.0 PURPOSE LIMITATION OBLIGATION

9.1 The Group may only collect, use or disclose Personal Data about an individual for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, for which the individual was notified.

9.2 The Group should not collect, use or disclose Personal Data when the purposes for which the Personal Data was collected is no longer valid and should not collect excess Personal Data than what is required for the specific purposes.

9.3 If Personal Data is required for new purposes, fresh notification and consent must be obtained.

9.4 The Group must ensure that forms designed to collect Personal Data only collect such Personal Data as necessary for the specific purpose. Such review should be carried out by the relevant head of department and DPO.

10.0 NOTIFICATION OBLIGATION

10.1 The Group must notify the individuals of the purpose(s) for which it intends to collect, use or disclose the individuals' Personal Data on or before such collection, use or disclosure of the Personal Data. For example, this could be:

- Before / When individuals are entering into a contract (e.g., employment agreement)
- Before individuals enter the Group's premises through signages (e.g., of the presence of CCTV) or by the security officer

10.2 Upon request, the individual must be informed of the contact details of the DPO whom they can contact regarding the collection, used and disclosure of the Personal Data.

10.3 Forms such as job application forms, post hire forms, visitors' log book used to collect Personal Data provide appropriate level of details to enable individuals to understand various purposes for which and how the Personal Data collected will be used.

10.4 All employees of the Group, including seafarers, should be directed to this Policy upon joining the Group and should acknowledge via a declaration form (Refer to Appendix 2) that they have read and understood the Policy. Such declaration is required on an annual basis. Links to the Group's Policy (online version) are also provided to individuals at the point of collection of Personal Data.

10.5 If events involving external parties are held by the Group, and photographs or videos of the event may be used in marketing material e.g., Annual Report, brochures, Group website, a notice will be placed at the reception or entrance of such event to inform the participants and guests of this purpose. Participants will be deemed to provide consent when they participate in the event however, they will be able to withdraw consent in accordance with Clause 8.8.4.

10.6 The Notification Obligation does not apply when:

a) The individual is deemed to have given consent (as per PDPA); or

b) The Group is collecting, using or disclosing Personal Data without consent of the individual in accordance with the circumstances specified in the PDPA (e.g., necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual)

11.0 ACCESS AND CORRECTION OBLIGATION

11.1 The Group must, upon request, (i) provide an individual with his or her Personal Data in the possession or under the control of the Group and information about the ways in which the Personal Data may have been used or disclosed during the past year subject to any relevant exception in the PDPA; and (ii) correct an error omission in an individual's Personal Data that is in the possession of or under the control of the Group.

11.2 To facilitate the Group in meeting its Access and Correction Obligation, the following Appendices and data sources have been put in place / identified:

a) A tabulation of the types of Personal Data collected and identify the custodian of the Personal Data. (Refer to Appendix 1A & 1B – Data Inventory Map for Employees and Seafarers)

b) A register of third parties or Data Intermediaries to whom Personal Data may have been disclosed. The Group may provide Appendix 3A and 3B as an alternative to providing the specific set of Data Intermediaries to whom the Personal Data has been disclosed. (Refer to Appendix 3A and 3B – Third Parties/Data Intermediaries Disclosure List for Corporate Office and Crewing Department).

c) Identify Personal Data that can be retrieved and amended by the employees directly via Times Software and ensure that employees are informed of the system availability.

d) Keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected. Proper documentation may help the Group in the event of a dispute or an application to the PDPC for a review.

11.3 Any individual requesting access to Personal Data may submit an access request to the DPO in accordance with Clause 0.

11.4 If the requestor is making an access request on behalf of another individual, the DPO should ensure the requestor is legally authorised to act on behalf of the individual.

11.5 The individual does not need to provide a reason for making an access request.

11.6 The Group is only required to provide Personal Data that the individual has requested for and is entitled to have access to under the PDPA and only if it is feasible for the Group to do so. Information which is no longer within the Group's possession or under its control upon receiving the access request will not be provided. Access requests will only be granted if the burden or expense of providing access is not unreasonable, frivolous or vexatious.

11.7 If the individual making the access request asks for a copy of his Personal Data in documentary form, the Group will charge a fee equivalent to the cost of retrieval. A written estimate of the fee must be provided to the individual. If such Personal Data cannot be practically provided to the individual in documentary form (e.g., CCTV footage which cannot be extracted), then the Group will provide the individual with a reasonable opportunity to examine the requested data in person.

11.8 Within 30 days, the DPO will reply to the individual with a written estimate of the fee to fulfil the access request, the requested information or the time by which the Group will be able to respond to the request.

If any exception or prohibition under PDPA applies such that the Group may reject the access request, the DPO should inform the individual of the relevant reason(s) so that he/she understands the reason(s) behind the rejection. Examples of exceptions include legal professional privilege information and opinion data kept solely for evaluative purpose. Examples of prohibitions include situations whereby provision of Personal Data may cause immediate or grave harm to the individual's or another person's safety or physical or mental health or reveals Personal Data about another individual.

11.9 An individual may submit a request to correct an error or omission in the individual's Personal Data that is in the possession or under the control of the Group to the DPO in accordance with Clauses 11.0 and 00.

11.10 Upon receipt of a correction request, the Group is required to consider whether the correction should be made. If the correction should be made, the DPO should ensure that the corrections are made within 10 working days and send the corrected Personal Data to every company to which the Personal Data was disclosed within a year before the correction request was made, unless that other company does not require the corrected Personal Data for any legal or business purpose.

11.11 The PDPA provides exceptions under which the Group is not required to correct Personal Data despite receiving such a correction request. Examples of exceptions include opinion data kept solely for evaluative purposes or any examination conducted by an education institution prior to the release of examination results.

12.0 ACCURACY OBLIGATION

12.1 This obligation is to ensure that where Personal Data may be used to make a decision that affects the individual, that the Personal Data is accurate and complete, however the Group is not required to check the accuracy and completeness of the individual's Personal Data each and every time it makes a decision about the individual.

12.2 Although the Personal Data provided by an individual is assumed to be accurate, the Group must make reasonable effort to:

a) Accurately record Personal Data which it collects
b) Collect all relevant parts of the Personal Data (so that it is complete)
c) Take appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness; and
d) Consider whether it is necessary to update the information.

12.3 Third parties including Data Intermediaries who provide Personal Data to the Group will be asked to verify the accuracy and completeness of the Personal Data provided by them.

13.0 PROTECTION OBLIGATION

13.1 The Group is obligated to protect Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

13.2 The following outlines the security measures that the Group has in place:

a) Administrative measures
- Requiring employees to be bound by confidentiality obligations in their employment agreements.
- Conducting regular training sessions for staff to impart good practices in handling Personal Data and strengthen awareness of threats to security of Personal Data.
- Ensuring that only the appropriate amount of Personal Data is held.

b) Physical measures
- Storing confidential documents in locked file cabinets.
- Restricting employee access to confidential documents on a need-to-know basis.
- Using privacy filters to minimise unauthorised personnel from viewing Personal Data on computers and laptops.
- Proper disposal of confidential documents which are no longer needed, through shredding or similar means.
- Visitors arriving at Security post are signed in and issued with a visitor pass so that visitors are easily recognised to ensure they are unable to gain access to Personal Data of our employees as well as other visiting guests.

c) Technical measures
- Ensuring computer networks are secured through password protection and firewalls.
- Activating self-locking mechanism for the computer screen if the computer is left unattended for a certain period of time (e.g., 5 minutes)
- Adopting appropriate access controls (e.g., to appropriately assign access rights)
- Updating computer security and IT equipment regulatory.
- Ensuring that IT service providers are able to provide the requisite standard of IT security.

13.3 The Group must ensure Data Intermediaries engaged have processes in place to ensure that Personal Data in their possession or under their control is protected by having reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

14.0 RETENTION OBLIGATION

14.1 The Group is required to cease to retain documents containing Personal Data or anonymise the data as soon as it is reasonable to assume that the purpose for which that Personal Data was collected is no longer being served by the retention of the Personal Data and the retention is no longer necessary for legal, tax and business purposes.

14.2 The retention periods for various categories of Personal Data pertaining to the corporate office are as follows. The list below may not be exhaustive and/or complete: -

No.	Data	Purpose	Minimum Retention Period
Singapore Corporate Office			
1	Job application forms & CVs (For unsuccessful applicants)	Current & future recruitment purpose	1 year
2	Employment Record: a. Employee record b. Salary record	For managing employment relationship and for the processing and payment of payroll including CPF contributions, submission of individual tax to IRAS, employees' benefit management	- For current employees: Latest 2 years as per Employment Act - For Ex-employees: Last 2 years, to be kept for 1 year after the employee leaves

			employment as per Employment Act. - Extended to 7 years or longer as per Clause 14.4
3	Other employment records such as academic and training cert, transcript, emergency contact, family details, thumbprint, family data & contact details, performance evaluation	For managing employment relationship including employees' benefit management	- To be kept for 1 year after the employee leaves employment - Extended to 7 years or longer as per Clause 14.5
4	Employment records that support the salary computation such as salary increment, bonus letter, etc.	Support data used for payroll processing purpose, accounting recording purpose and managing employment relationship	- For current employees: Latest 2 years as per Employment Act - For Ex-employees: Last 2 years, to be kept for 1 year after the employee leaves employment as per Employment Act. - Extended to 7 years or longer as per Clause 14.5
5	Employment records that support childcare leave claims such as dependent's personal details used for the claims submission. If details are not used for claims purposes, they will follow other employment records' retention period.	For submission of claims purpose	- For current employees: Latest 2 years as per Employment Act - For Ex-employees: Last 2 years, to be kept for 1 year after the employee leaves employment as per Employment Act - Extended to 7 years or longer as per Clause 14.5
6	Photographs, Videography of employees, clients, suppliers or other stakeholders	For annual reports, Company's website and other Company's publications	See clause 8.8.4 and 10.5
7	Closed-Circuit Television Cameras (CCTV)	For security purpose	- 6 years as CCTV is used for safety, security and investigation
8	Staff claims or other payroll summary data for accounting and tax purposes	Accounting & Tax purpose	- 5 years as required by Companies' Act - Extended to 7 years or longer as per Clause 14.4
9	Record of CPF Payment (Form CPF 90)	Accounting & Tax purpose	- 5 years as required by Companies' Act - Extended to 7 years or longer as per Clause 14.5
10	Medical claims & Insurance records	Insurance, Accounting & Tax purpose	- 5 years as required by Companies' Act - Extended to 7 years or longer as per Clause 14.514.4
11	Childcare leave claims record (from the relevant ministries)	Accounting & Tax purpose	- 5 years as required by Companies' Act - Extended to 7 years or longer as per Clause 14.5

14.3 The Group has short term employment contracts with seafarers who are often called back for assignments after their contracts end. As such, the Group retains the Personal Data of seafarers even after the day they leave employment for ease of recalling them back for assignments. The Group has determined the retention period of various categories of Personal Data pertaining to seafarers as follows. The list below may not be exhaustive and/or complete: -

No.	Data	Purpose	Minimum Retention Period
Seafarers' Personal Data			
1	Personal Data of seafarer candidates for employment	For future job considerations	- 5 year - Extended to 7 years or longer as per Clause 14.5
Seafarer employed on board of vessels by the Group			
2	Personal details (Surname, name, rank, nationality, date of birth & place of birth)	Current & future recruitment purpose	- 5 year - Extended to 7 years or longer as per Clause 14.5
3	Identification information/document (Seaman book, ID, Passport, etc.)	Application of permit, arranging for custom clearance, transportation, accommodation	- 5 year - Extended to 7 years or longer as per Clause 14.4
4	Contact details of seafarer (telephone numbers, email address and home address, etc.)	To facilitate employment relationship management and communication	- 5 year - Extended to 7 years or longer as per Clause 14.5
5	Passport size photograph, photographs printed in annual report and uploaded on Company's website	For employment relationship, for Company's website and other Company's publications	5 year. Also see clause 8.8.4 and 10.5

6	Next-of-kin details	To facilitate employment relationship management (including salary crediting where applicable) and communication	- 5 year - Extended to 7 years or longer as per Clause 14.44.5
7	Medical information (copies of medical fitness, drug and alcohol test and yellow fever vaccination certificates)	For job qualification assessment. This is necessary for the entry into performance of the seafarer's employment contract and for compliance with applicable laws and regulations to which the Group is subject to (Flag state, ISM, ISPS, MLC, STCW, etc.)	- 5 year - Extended to 7 years or longer as per Clause 14.5
8	Certificates of competency		
9	Flag state documents (Flag state endorsements and Seaman books)		
10	Visas		
11	Training certificates (STCW and other training certificates)		
12	Services with other companies (durations, name of ship, flag, GRT, type of ships, engine specifications and name of Company)	For job qualification assessment	- 5 year - Extended to 7 years or longer as per Clause 14.5
13	Evaluation reports (information on seafarers' performance on board the vessels)	For future job considerations and facilitate employment relationship management	- 5 year - Extended to 7 years or longer as per Clause 14.514.4
14	Wage and payroll data (social insurance number, wages, payroll reports, allotments requests, deduction, etc.)	For managing employment relationship and for the processing and payment of payroll including social contributions, submission of individual tax to relevant authorities, employees' benefit management.	- 5 year - Extended to 7 years or longer as per Clause 14.44.5
15	Injury and sickness report	For job qualification assessment	- 5 year - Extended to 7 years or longer as per Clause 14.5
16	Services with the Company (sign-on and sign-off dates, name of Company's ships, sign-on and sign-off ports)	For managing employment relationship and for the processing and payment of payroll including social contributions, submission of individual tax to relevant authorities, employees' benefit management	- 5 year - Extended to 7 years or longer as per Clause 14.5

14.4 Some documents need to be retained longer than the requirements established per the retention table above for legal purposes. Under the Limitation Act (cap 163), actions founded on a contract must be brought within 6 years from the date on which the cause of action accrued. Hence, the Group can retain records relating to its contracts for 7 years from the date of termination of the contract and possibly for a longer period if an investigation or legal proceedings should commence within that period. This extended retention period will apply to both employees and seafarers alike.

14.5 Other documents such as certificates of competency, training certificates, wage & payroll data, medical claims & insurance records and records of CPF Payment (CPF Form 90), etc. can also be retained longer than the requirements established per the retention table above for legal and/or accounting & tax purposes. In a similar manner, the Group shall retain such records for 7 years from the date of termination of an employment relationship with the employees/seafarers, and possibly for a longer period of time if an investigation or legal proceedings should commence within that period.

14.6 The Group should review the Personal Data it holds annually to determine if that Personal Data is still needed. Personal Data must not be kept by the Group "just in case" it may be needed for other purposes that have not been notified to the individual concerned. Upon determination that the Personal Data is no longer required, the Group will make reasonable efforts to cease to retain the Personal Data by:

a) Destroying the Personal Data in an appropriate manner such as:
- Shedding of confidential paper document containing Personal Data
- Degaussing all hard disks when they are no longer in use
- Using of re-writeable media like hard disks, USB memory sticks, etc., as such mediums allow for nearly unlimited overwriting of data, so that Personal Data may be disposed from them without the need to dispose of the medium itself.

b) Returning to the individual concerned.
c) Anonymising the Personal Data such that the remaining data does not identify any particular individual.
d) Deleting soft copies from the server to the extent possible without requiring formatting the server.

14.7 The Group must ensure that Data Intermediaries cease to retain documents containing Personal Data, or remove the means by which the Personal Data can be associated with particular individuals as soon as it is reasonable to assume that the purpose for which the Personal Data was collected is no longer being served by retaining the data; and retention is no longer necessary for legal or business purposes.

15.0 TRANSFER LIMITATION OBLIGATION

15.1 The Group is restricted to only transfer Personal Data to a country or territory outside of Singapore when it is taken to have satisfied the requirements in those countries/territories are in compliance with the standard of protection that is at least comparable to the PDPA.

15.2 The Group will take appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations that provide a standard of protection that is minimally comparable to the PDPA.

16.0 OPENNESS OBLIGATION

16.1 The Group has appointed a DPO to be responsible for ensuring its compliance with the PDPA.

16.2 The role of the DPO would include:

a) Developing policies for handling Personal Data, communicating internal Personal Data policies to customers and handling any queries or complaints about Personal Data

b) Understanding the Group's Personal Data inventory and reviewing the data management framework and processes to align them with the PDPA.

c) Assessing the Group's policies, procedures and contracts with 3rd parties and Data Intermediaries to ensure data protection provisions are covered when required.

d) Inform all employees of the Group's Policy and their role in safeguarding Personal Data.

e) Ensure the employees know what the internal processes are with regard to protecting Personal Data.

f) Acknowledge, evaluate and oversee consent/withdrawal/access and correction requests.

g) Assess and alert management of any risk of a data breach or other breaches of the PDPA and to liaise with the PDPC for investigations on breaches, if necessary.

h) Monitor, review and update the Data Inventory Map on a regular basis.

i) Maintain a record of 3rd parties and Data Intermediaries to which the Group discloses or transfer Personal Data (Refer to Appendix 3A and 3B – Third Parties/Data Intermediaries Disclosure List for Corporate Office and Crewing Department)

16.3 Feedback/Complaint handling process

a) Individuals may provide feedback or lodge a complaint to the Group by using the PDPA Complaint/Feedback Form (Appendix 4). The completed form can be sent to the DPO by post or email.

b) Within 30 working days from the date the Feedback/Complaint Form is received, the DPO will reply (by post or email, whichever applicable) to the complainant providing a response or the time by which the Group will be able to respond to the feedback/complaint.

c) The Group is required to consider whether the feedback/complaint received is valid and reasonable. If the Group is satisfied that the feedback/complaint is actionable, the DPO should commence investigation and provide a closed-out plan within 30 working days. Appropriate corrective and preventive action(s) implemented by the Group to rectify the feedback/complaint should be communicated to the complainant in writing.

16.4 The contact details of the DPO are as follows:

dpo@choffshore.com.sg
Data Protection Officer
Tel: +65 6410 9018
12A Jalan Samulun
Singapore 629131

17.0 DATA PORTABILITY OBLIGATION

17.1 This obligation will take effect when the Regulations are issued - end 2021.

17.2 Under this obligation, the Group must, at the request of an individual, transmit his/her Personal Data that is in the Group's possession or under its control, to another organisation in a commonly used machine-readable format.

17.3 Requesting individual may make a request to the Group to make a data port regardless of whether he/she is in Singapore.

17.4 The Group, on receiving an individual's request to port their Personal Data will only be required to port data to receiving organisations that have a presence in Singapore.

17.5 Organisations that receive ported data will be regarded as having collected Personal Data and are subjected to all of the PDPA obligations.

17.6 Upon receiving the ported data, a receiving organisation should check that it can access such data and that all data fields indicated by the requested individual are complete.

17.7 If receiving organisation has any issue receiving the data, it must notify the Group immediately.

17.8 Types of data that can be ported will include:

- Name, contact information, credit card information, delivery address
- Individual's business contact information
- Consumer spending history – data on purchases and payments

- Utilities consumption history – data on mobile data usage and telecommunication utilization

17.9 Exceptions (under 5th Schedule) include:

- Opinion data
- Personal data which is subject to legal privilege
- Data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the Group
- Data that does not exist or is trivial

18.0 EMPLOYEE TRAINING

18.1 Employees who will have access to any kind of Personal Data will have their responsibilities, especially with respect to the Policy outlined on their first day of work. All employees will also be provided access to the Group's Policy.

18.2 Where necessary, Data Users would be sent for PDPA related training.

19.0 MANAGING AND NOTIFYING DATA BREACHES

19.1 A data breach generally refers to the unauthorised access and retrieval of Personal Data or the loss of any storage medium or device on which Personal Data is stored. Data breaches could lead to financial losses, results significant harm to the individuals whose Personal Data have been compromised (the "affected individuals") and cause stakeholders to lose trust and confidence in the Group. It is therefore important for the Group to be accountable towards individuals by preventing, managing and notifying the PDPC and affected individuals of data breaches.

19.2 In the event of a breach or loss of Personal Data, the Group must respond to and manage the incident promptly and effectively. Any issues relating to Personal Data protection shall be escalated to the DPO for review, followed by investigation and/or escalation to the Management team, if necessary.

19.3 In a similar manner, Data Intermediaries have a statutory duty to notify the Group (data controller) in an event of a breach. A Data Intermediary must, without due delay, notify the Group of the occurrence of the data breach involving Personal Data processed on behalf of the Group.

19.4 The suggested actions taken in the event of a data breach should follow four (4) key steps (using the acronym of **C.A.R.E**):

- **Contain** the data breach to prevent further compromise of data and implement mitigation action(s) to minimise potential harms from the breach after an initial appraisal has been conducted to determine the extent of the breach.
- **Assess** the data breach to determine the root cause (where possible) and the effectiveness of containment action(s) taken thus far to contain the data breach. Where necessary, continuing efforts should be made to prevent further harm from the data breach.
- **Report** the data breach to:
  — The PDPC (mandatory if the breach is a notifiable data breach under the Personal Data Protection Act ("PDPA"). Organisations may also inform PDPC of the data breach voluntarily); and/or
  — The affected individuals (if required under the Data Breach Notification Obligation ("DBN Obligation")).

- **Evaluate** the organisation's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

19.5 Steps to be taken to **contain** the Breach to prevent further compromise of data.

a) Determine the cause if the data breach and whether the breach is still ongoing
b) Number of affected individuals
c) Type(s) of Personal Data involved
d) The affected systems, servers, databases, platforms, services etc.
e) Whether help is required to contain the breach
f) The remediation action(s) to that the Group has taken or needs to take to reduce any harm to affected individuals resulting from the breach
g) Isolate the compromised system from the Internet or network by disconnecting all affected systems
h) Re-route or filter network traffic, firewall filtering, closing particular ports or mail servers
i) Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts
j) Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system
k) Stop the identified practices that led to the data breach
l) Establish whether the lost data can be recovered and implement further action to minimise any harm caused by the data breach (e.g., remotely disabling a lost notebook containing Personal Data of individuals, recalling an email that has been accidentally sent or forwarded etc.)
m) Notify the Police if criminal activity is suspected and to preserve evidence for investigation
n) Notify the Cyber Security Agency of Singapore (CSA) through the Singapore Computer Emergency Response Team (SingCERT) for cyber incidents.
o) Other sectoral regulators or law enforcement agency such as MAS, MOH etc.

19.6 Considerations for assessing risks and impact.

a) Risk and impact on individuals
   - How many people were affected?
   - Whose Personal Data had been breached (e.g., minors, vulnerable individuals etc.)?
   - Whether the Personal Data was publicly available before the data breach?
   - Ease with which an affected individual can be identified from the compromised data (e.g., name, age, and personal mobile phone numbers)?
   - Any additional measures in place to minimise the impact of a data breach?

b) Risk and impact on the Group
   - What caused the breach (data was illegally accessed and stolen, was it wrongly sent to recipients or due to computer system weaknesses)?
   - When and for how long had the compromised Personal Data been made publicly accessible for a significant period of time?
   - Who might gain access to the compromised Personal Data?
   - Will compromised data affect transactions with any other 3rd parties?

19.7 Reporting the incident

a) Depending on the outcome of assessment, the Group may have to notify PDPC and the affected individuals.

b) Once the Group has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation is required to:

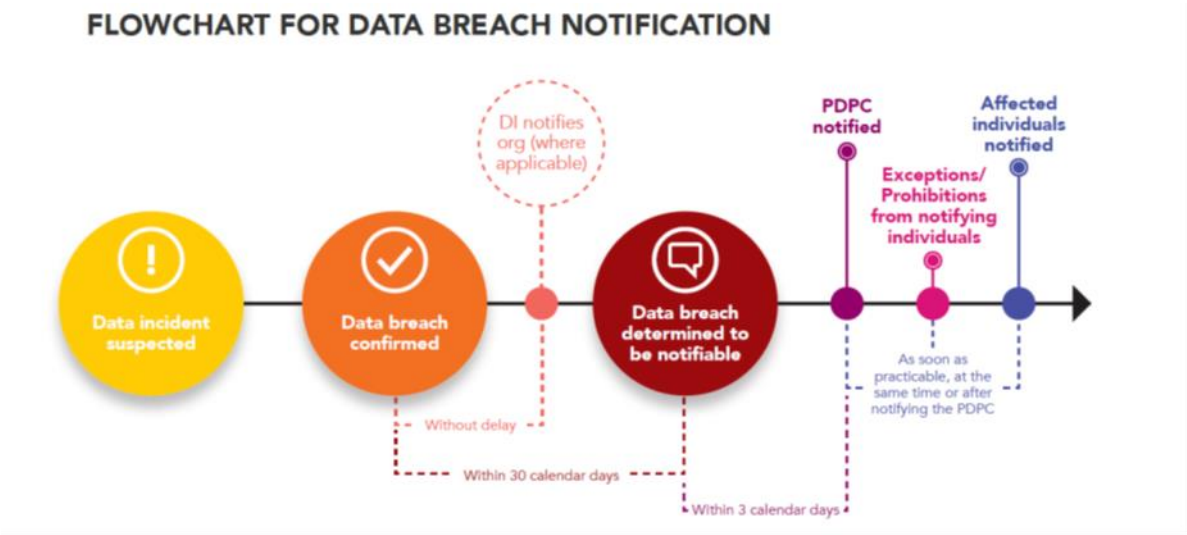
- Assess whether the data breach is notifiable under the PDPA within 30 calendar days
- If the Group is unable to complete its assessment within 30 days, it would be prudent for the Group to be prepared to provide the Commission with an explanation for the time taken/required to carry out the assessment. The Group should document all steps taken in assessing the data breach
- Assess whether the data breach is likely to result in significant harm to the affected individuals. By notifying the affected individuals, they are able to take steps to protect themselves (e.g., change password, cancel credit card, monitor account for unusual activities). The PDP (DNB) Regulations 2021 provides the Personal Data (or classes of Personal Data) that is deemed to result in significant harm to affected individuals if compromised in a data breach.
- Assess if the data breach meets the criteria of significant scale. Data breaches of significant scale are those that involve the Personal Data of 500 or more individuals. Under such circumstances, the Group will be required to notify the Commission, even if the data breach does not involve any prescribed Personal Data in the PDP (DBN) Regulations 2021.
- If the Group is unable to determine the actual number of affected individuals in a data breach, the Group should notify the Commission when it has reason to believe that the number of affected individuals is at least 500. This may be based on the estimated number from an initial appraisal of the data breach. The Group may subsequently update the Commission of the actual number of affected individuals when it is established.

c) There are exceptions to notifying affected individuals.
- Where remedial actions have been taken
- Where the Personal Data is subject to technological protection measures (e,g., encryption)
- The Group must not notify any affected individual of a notifiable data breach if PDPC or a prescribed law enforcement agency instructs it not to do so
- The Group having made a written application to the Commission to waive the requirement to notify an affected individual about a notifiable data breach.

d) Upon determining that a data breach is notifiable, it is mandatory that the Group must notify:
- PDPC as soon as practicable, but in any case, no later than three (3) calendar days / 72 hours; and
- PDPC must be notified before or at the same time as affected individuals are notified, to allow the Commission to assist affected individuals who contact the Commission once they are notified.
- The notification must contain all the information that is prescribed for this purpose and be made in the form and submitted in the manner required by the Commission.
- These timeframes for notifying the Commission and/or affected individuals commences from the time the Group determines that the data breach is notifiable. Any unreasonable delays in notifying the relevant parties will be a breach of the DBN Obligation.

e) The Group may choose to voluntarily notify the PDPC even if they assess that the data breach is not a mandatorily notifiable one under the PDPA. Voluntary notifications send a message that the Group is committed to be accountable for protecting data and has systems and processes in place to mitigate risks should data breaches occur.

f) Details of the data breaches notifications can be sent to PDPC at https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, the Group may also contact the PDPC at +65 6377 3131 during working hours.



19.8 Evaluating the Cause, Response and Recovery to prevent future breaches

a) A review including a root cause analysis of the data breach (e.g., implement fixes to system errors/bugs to prevent future disclosure of/access to Personal Data)
b) A prevention plan to prevent similar data breaches in future
c) Audits to ensure the prevention plan is implemented
d) A review of existing policies, procedures and changes to reflect the lessons learnt from the review
e) Changes to employee selection and training practices
f) A review of data intermediaries involved in the data breach

20.0 REFERENCE

a) Personal Data Protection Act 2012.
b) Advisory Guidelines on Key Concepts in the PDPA (1 February 2021)
c) Guide on Managing and Notifying Data Breaches under the PDPA (15 March 2021)
d) PDP (DNB) Regulations 2021

21.0 APPENDICES

Appendix 1A – Data Inventory Map for Employees
Appendix 1B – Data Inventory Map for Seafarers

Appendix 2 – Declaration Form for Employees / Seafarers

Appendix 3A – Third Parties/Data Intermediaries Disclosure List for Corporate Office
Appendix 3B - Third Parties/Data Intermediaries Disclosure List for Crewing Department

Appendix 4 – Complaint/Feedback Form

REVISION HISTORY

Rev No.	Issue Date	Description of Changes	Clause #	Approved
0	1 Nov 2020	Initial release	N.A.	Board
1	15 May 2023	Adding of new clause 1.4 to comply with the enhancement of the PDPA on 1 February 2021	1.4	Board
1	15 May 2023	Adding of new clause 5.0 to comply with the enhancement of the PDPA on 1 February 2021	5.0	Board
1	15 May 2023	Adding of new clause 6.0 to comply with the enhancement of the PDPA on 1 February 2021	6.0	Board
1	15 May 2023	Adding of new Data Portability Obligation which will come into effect when the Regulations are issued - end 2021	7.1 / 7.1 (j)	Board
1	15 May 2023	Updating of section in accordance with the enhancement of the PDPA on 1 February 2021	8.5 (c)	Board
1	15 May 2023	Updating of section in accordance with the enhancement of the PDPA on 1 February 2021	8.6	Board
1	15 May 2023	Updating of clause 10.5 due to changes in clause nos.	10.5	Board
1	15 May 2023	Updating of table due to changes in clause nos.	14.0	Board
1	15 May 2023	Adding of new clause 16.3 – Complaint/Feedback handling process	16.3	Board
1	15 May 2023	Adding of new clause 17.0 – Data to comply with the enhancement of the PDPA on 1 February 2021	17.0	Board
1	15 May 2023	Updating of section in accordance with the enhancement of the PDPA on 1 February 2021	19	Board
1	15 May 2023	Updating of section in accordance with the enhancement of the PDPA on 1 February 2021	20 (b) / 20 (c) / 20 (d)	Board
1	15 May 2023	Adding of new Appendix 4 - Complaint/Feedback Form	21.0	Board