SPS Maritime Ltd

TABLE OF CONTENTS

C - Company Policies • Crew Policies • Data Protection Policy

Chapter 1 - General

Purpose

The purpose of this document is to establish guidelines for Personal Data stored and processed by the Company.

The Company shall ensure, as best practical, that it follows the applicable requirements of the European Union General Data Protection Regulation (GDPR) and the Cayman Islands Data Protection Law.

Responsibility

It is the responsibility of the Company assigned Data Processors, the Data Controllers and the Data Protection Officer to comply with this Policy.

Definitions

- **GDPR –** General Data Protection Regulation of the European Union
- **Supervisory Authority –** an independent public authority which is established by a Member State of the GDPR pursuant to Article 51 GDPR
- **Company –** the Company is SPS Maritime Ltd and is responsible for the operational management of the Vessel
- **Data Protection Officer (DPO) –** person who is the head of the Data Controller(s) with additional duties & responsibilities
- **Data Controller(s) –** person(s) who determines the purposes and means of processing personal data; they have accountability for the safety of the data and responsibility for the data.
- **Data Processor(s) –** person(s) who processes personal data on behalf of the controller
- **Data Subject –** person of whom personal data is being processed
- **Employee –** a person employed by the Company
- **Crewmember –** person employed by the Company as crewmember on a Company Ship
- **Special Personnel –** any person sailing on a company ship without being a crew-member
- **Personal Data** - any information relating to an identifiable natural person (data subject) or to one or more factors specific to the identity of that person (e.g. passport, name, social security number)
- **Essential Personal Data –** Personal Data of a Data Subject that is essential for the Company to have in order to establish or upkeep a Professional Relationship with the Data Subject
- **Additional Personal Data -** Personal Data of a Data Subject that is not essential for the Company to have in order to establish or upkeep a Professional Relationship with the Data Subject
- **Voluntary Submitted Unrequested Personal Data –** Personal Data that has been voluntarily submitted by a Data Subject to the Company without the request for it by the Company
- **Professional Relationship of Data Subject with the Company –** relationship that the Data Subject has or wishes to have with the Company (e.g. Crewmember, Special Personnel)
- **Data Breach -** breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **Consent** - any freely (voluntary) given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them
- **Data Processing** - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

No references

SPS Maritime Ltd
POL-CP-0210
Approved: Revision 02 / 05/27/2022

Chapter 2 - Processing of Personal Data

Collection of Personal Data

The Company collects Personal Data via electronic means and via hard-copy.

Electronic means include: e-mail, electronic forms, scanned documents

Hard Copy means: paper copies

Essential Personal Data

The following lists Essential Personal Data that the Company may require from Data Subjects.

Precisely which data this is depends on the specific position that the Data Subject is having within the Company.

The following list contains most, but not all Essential Data.

Data Subjects may at any time request a full list of Essential Data for their current or future position in the Company

For all Data Subjects that have or want to maintain a Professional Relationship with the Company:

Full Name, Nationality, Date of Birth, Passport copy, US Visa copy (if not US or Canadian Citizen), Home Address, Phone Number, E-Mail Address, Next of Kin (Name, Relationship with Data Subject, Contact Details, Languages Spoken), Medical Information (Vaccinations, Blood Group, Allergies, Nutritional Needs, Current Medication, Current Medical Issues), Confidential Information Agreement, Media Release Waiver, Data Protection Consent Form

For Crew Members additionally:

Copies of all Professional Certificates required to perform the position on board for which they are hired, Curriculum Vitae (CV), Personal References, Background Check Information, Drug & Alcohol Test Information, Seafarer Medical Fitness Certificate, Bank Details (for payment of salary), Home-Airport, Uniform Sizes

Requested Personal Data

The Company will request Personal Data to be submitted to the Company by the Data Subject, if it is Essential Personal Data that is required to establish or to maintain the Professional Relationship between the Company and the Data Subject.

Voluntary submitted, unrequested Personal Data

From time to time Data Subjects who either have or don't have a Professional Relationship with the Company are sending Personal Data to the Company without request. Examples are opportunistic job applications that contain Personal Data such as Curriculum Vitae (CV) and Professional Certificates, but also updated Professional Certificates or Additional Personal Data of Crewmembers. Such data will either be deleted or processed under the same rules as Requested Personal Data.

Storage, Processing and Securing of Personal Data

Personal Data shall be stored and processed within secure systems.

Hardcopies of Personal Data shall be stored in locked rooms or cabinets that allow access only by the DPO, Data Controller and Data Processors. Processing shall only be done by DPO, Data Controller and Data Processors.

Electronic copies of Personal Data shall be stored and processed on secured computer systems that allow access only by the DPO, Data Controller and Data Processors. This can be archived by electronic access protection with usernames and passwords.

The company currently uses the following computer systems for processing of Personal Data:

- Company Servers
- Adonis (cloud-based software)
- Google Drive (cloud-based software)
- Smartsheets (cloud-based software)
- Asana (cloud-based software)
- Unisea (cloud-based software)

- E-Mail

Distribution and Sharing of Personal Data with 3rd Parties

The Company shall not share or make accessible Personal Data to 3rd parties other than the ones listed and explained below.

The Company works closely with the following organizations:

- Schmidt Ocean Institute
- Hillspire LLC
- Y.CO
- Eurasian
- Government Authorities of Flag State and Port States

A limited amount of Personal Data may be shared with those organizations.

The Company assures that only Personal Data that is absolutely required for a specific purpose (e.g. running and submitting payroll) is being processed via these organizations.

Time period Personal Data is being stored by the Company

The Company shall be default store Personal Data for the duration of the Professional Relationship and the two years following the termination of the Professional Relationship.

The reason for storing Personal Data for two years after the termination of the relationship are:

- Audit Purposes
- Requests of the Data Subject for References, Testimonials, Payslips
- Reactivation of the Professional Relationship

Deletion of Personal Data

By default Personal Data shall be deleted two years after the termination of the relationship.

The Data Subject may request deletion of any Personal Data that is not Essential Personal Data at any time during an existing Professional Relationship.

The Data Subject may request deletion of any Personal Data if no Professional Relationship exists or if it has been terminated.

If Personal Data has been deleted after the termination of a Professional Relationship, the Company will not be able to fulfil requests of the Data Subject such as References, Testimonials, Payslips.

If the Data Subject requests deletion of any Essential Personal Data while a Professional Relationship is active, this request may be followed with the consequence of terminating the Professional Relationship.

Deletion of Personal Data is the responsibility of the DPO or a Data Controller who has been assigned this task by the DPO.

Processing of Personal Data

Personal Data is being processed for various purposes. A few examples below:

- Fulfilling legal and Company requirements to monitor that the required professional certificates are present and valid
- Reporting to Government Authorities of Flag State and Port State.
- Processing salary payment
- Emergency preparedness (including medical)

No references

Chapter 3 - Roles, Rights and Responsibilities

The following sections lays out the roles, rights and responsibilities of the various persons with which this policy is dealing.

Data Protection Officer (DPO)

The Company appoints the assigned IT Manager to assume the role of Data Protection Officer (DPO).

They can be reached at it@schmidtocean.org

The DPO oversees the data protection strategy of the Company. In this function they report and have access to the highest management level of the Company.

The DPO is primary the link between the Company the Data Subjects and the Supervisory Authority.

The DPO shall:

- Oversees the Data Controllers and Data Processors
- inform Data Subjects about their rights, and raise awareness of the regulation
- answer questions and handle complaints of Data Subjects, Data Controllers and Data Processors
- train Company Staff on aspects of Data Protection
- perform Data Protection Assessments
- take action to prevent Data Breaches
- receive and investigate any reports about Data Breaches, including suspected
- report any confirmed Data Breaches to the Company Management and the Supervisory Authority
- take action to minimize impact of any confirmed Data Breach
- take action to prevent reoccurrence of a similar Data Breach as any confirmed one

Data Controller

Data Controllers work under the supervision of the DPO in regards of Data Protection.

Data Controllers have administrator rights for either parts or the whole Data system of the Company.

The DPO can delegate some of their tasks to Data Controllers.

Examples of Data Controllers within the Company are (but not limited to):

- Vice President of Operations
- Designated Person Ashore (DPA)
- Captain
- AV/IT Engineer
- Electro Technical Officer (ETO)

Data Processor

Data Processors work under the supervision of the DPO and/or of a Data Controller. They usually don't have administration rights, but have access to Personal Data in order to process them.

Examples of Data Processors within the Company are (but not limited to):

- Administrators
- Ship's Officers on various levels
- Company Officers on various levels

Data Subject

Data Subjects are all persons that have, had or are wishing to have a Professional Relationship with the Company and of whom the Company holds and processes Personal Data.

This includes all Employees, Crewmembers, Special Personnel Company.

Rights of the Data Subject

Data Subjects have the following rights:

- Data Subjects may at any time request from the Company a complete overview of the Personal Data that the Company holds about them and

where it is stored

- Data Subjects may at any time request from the Company to delete non-essential Personal Data
- Data Subjects may request from the Company to delete parts or all of their Personal Data after the Professional Relationship has ended

Any requests shall be directed to it@schmidtocean.org

Requests will normally be fulfilled within one month. If requests cannot be fulfilled the DPO will provide an explanation why and will provide guidance for appealing this denial of action.

No references

Exported by: Heiko Volz/SPS @ 2022-05-27T10:06:42.359+02:00

Chapter 4 - Reporting and Documentation

Consent and Data Protection Consent Form

The document "Data Protection Consent Form" is being used by the Company to obtain written consent from all Data Subjects. The form is related to this Policy and signature of the form also confirms that the Data Subject is aware of the contents of this Policy in the version valid on the date of signature.

It is a requirement to sign this form for all Data Subjects who are having, wanting to maintain or wishing to have a Professional Relationship with the Company.

The filled out form shall be e-mailed to falkorcrewing@schmidtocean.org and will be stored in the Unisea.

Updates of this Policy or the Consent Form

Any update of this Policy and/or the Consent Form "Data Protection Consent Form" will be published in Unisea.

Questions, Concerns or Applications

Any Data Subject may at any time raise questions or concerns or make applications (see "Rights of the Data Subject") to the following e-mail addresses: falkorcrewing@schmidtocean.org and it@schmidtocean.org

Data Breach

Any Data Subject, Data Processor or Data Controller who suspects a Data Breach shall raise this as soon as possible to the DPO via this mail address: it@schmidtocean.org

The DPO shall then investigate the suspected breach and if confirmed consider:

- Prepare support and front desk
- Alert the IT Department
- Notify Legal support team
- Notify the Supervisory Authority within 72 hours
- Take measures to minimize impact
- Notify Public Relations Team
- Company-wide notification
- Notify Law enforcement
- Notify Insurance
- Notify Forensic Analyst
- Consider and Implement measures to prevent a repetition of the Data Breach
- Keep reporting person(s) and affected person(s) updated on proceedings

Cyber Security Response Plan

The company maintains the document A.01.15 - Cyber Security Response Plan in which additional details regarding protection of data and the handling of breaches can be found.

The document is linked via the Reference section.

References

Type	Title	Number
QADocument	Chapter 1 - General	SMM-OTMG-0079
QADocument	Chapter 2 - Overview	SMM-OTMG-0080
QADocument	Chapter 3 - Containment, Eradication & Recovery	SMM-OTMG-0081
QADocument	Chapter 4 - Reporting & Documentation	SMM-OTMG-0082
QADocument	Chapter 5 - Scenario Guidance	SMM-OTMG-0083

Exported by: Heiko Volz/SPS @ 2022-05-27T10:06:42.390+02:00