| 1 | PRIVACY POLICY |
|---|---|

Cosmonav Ltd. (hereinafter called "The Company") needs to collect personal information to effectively carry out everyday business functions and activities to provide ship manning and recruitment services and maintains shore staff data for its scope of work.
The Company is committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)*** and any other relevant data protection laws and codes of conduct.

Personal data shall be processed according to the below principles:

**(1) Personal data shall be processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');
Data Subjects must be aware that their data is being processed and

- for what purpose it is being processed,
- how to exercise their rights in relation to the data

There is no obligation to inform data subject of anything that is obvious from the context or from general knowledge: a typical example might be business contact lists.

**(2) Personal data** s**hall be collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, shall not be considered to be incompatible with the initial purposes ('purpose limitation');

**(3) Personal data shall be adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

**(4) Personal data shall be accurate and, where necessary, kept up to date**; every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

**(5) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

**(6) Shall be processed in a manner that ensures appropriate security of the personal data,** including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

It is the Company's Policy to provide data subject, with information about the processing of its personal data from the Company and to inform data subject about the data protection rights under the current legislative and regulatory framework.

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of the Company's top priorities. The Company operates a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of its business.

## 2 PERSONAL DATA THAT COMPANY MAINTAINS

### 2.1 PERSONAL DATA THAT COMPANY MAINTAINS SEAFARERS

The Personal Data that the company maintains, include not only those that the law requires for the conclusion of agreements, but also a number of other which are required and are used in the industry in order to achieve high-level services. For the above reason the type of data that are held and the scope of data processing, depends on the requirements that requested, each time from the legislation and maritime industry. Without data processing the Company, cannot enter into or perform the terms of a contract with data subject.

Indicatively and not limited to, these are:

Basic identification information: Name, Surname, Father's name, Mother's name, date of birth, ID number or passport number, date of issue of ID or passport, competent authority regarding the issuing of ID or passport, family status (married, single etc), social security number, sailor's register number, VAT registration number, contact information ( telephone, including mobile) , address (including country), sex, nationality.

Information regarding work experience: former employers, position held, qualifications, certifications, information regarding use of the Managing Company's equipment, information regarding work performance

Information regarding health: Physical examination, Dental Examination, Psychological Evaluation, Visual testing, Colour Vision (Isihara, Bostrom-Kugelber), Audiometry, Chest X-Ray, Electrocardiogram, Urinalysia, Fecalysis, Blood Count, Blood Typing, Fasting Blood Sugar (FBS),Hepatitis Bs Antigen, Malaria Smear, Disease Research Lavoratory, (VDRL), Lung Function test, Blood Biochemistry (Liver Function test, Kidney function test, Cholesterol, Triglycerides, Uric Acid, Electrolytes), HIV testing, Ultrasound.

Financial information: remuneration, additional benefits, account details, social security information and amounts of any kind to be paid for the Employee's social security

Data that concern: medical fitness, health data, medical certificates, cultural, religion, biometrics, photos, videos, nationality, sex, are ranked as special categories of data.

Where data collection is optional, this is made clear at the point of collection.

#### 2.1.1 Processing Purpose

The Company process seafarer's personal data for one or more of the following reasons:

**a) For the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; Indicatively and not limited to, for:**
- Fulfilling vessels manning needs
- Capacity assessment of the candidate
- Complying with charterers requirements
- Ascertain crew members fitness to work
- Ascertain crew members efficiency for the performance of the work
- Preparation for future potential manning needs of their client
- Provision of clothing
- Identification of crew candidates/ crew members
- Handling different cultural and religious backgrounds respectfully
- Facilitating communication

**b) For compliance with a legal obligation. Indicatively and not limited to, for:**
- The performance of the Ship Management Agreement (SMA)
- ISM Code, STCW and MLC 2006 requirements
- Local port regulations
- Fit for Duty requirements as imposed by the ISM Code and the MLC 2006
- Vessel's Flag Administration requirements
- Support legal proceedings

**c) In order to protect the vital interests of the data subject or of another natural person.**

**d) For the performance of a task carried out in the public interest.**

**e) For the purposes of safeguarding legitimate interests. Indicatively and not limited to, for:**
- Safety and security of the vessel, the cargo and personnel onboard
- Seafarers' vital interest

- Handling different cultural and religious backgrounds respectfully

**f) On the basis of seafarers' consent.**
Any such consent granted, may be revoked at any time by contacting the Company.

**2.2 PERSONAL DATA OF SHORE STAFF**

The Personal Data of shore staff that the company maintains, include not only those that the law requires for the conclusion of agreements, but also a number of other which are required and are used in the industry in order to achieve high-level services. For the above reason the type of data that are held and the scope of data processing, depends on the requirements, that are requested each time from the legislation and maritime industry. Without data processing, the Company, cannot enter into or perform the terms of a contract with data subject.

Indicatively and not limited to these are: name, e-mail, address, phone number, location, rank, marital status, professional history, bank accounts, passport, ID number, social security number, tax identification number, tax office, authentication data (e.g. signature) educational background, diplomas, parents name, next of kin names and address, social security number, performance working capacity, Visa, age, number of children, complaints, position in the company, footage of CCTV in the entrance of the Company, CVS.

Special categories of personal data are also included in the data which the company collects and maintains. Indicatively and not limited to, these are: medical fitness, health data, medical certificates, photos, nationality.

Where data collection is optional, this shall be made clear at the point of collection.

**2.2.1 Processing Purpose**

The Company process personal data of shore staff for one or more of the following reasons:

**a) For the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; Indicatively and not limited to, for:**
- Covering shore staff employment needs
- Capacity assessment of the candidate
- Fulfilment of office employment needs
- Ensuring employees' efficiency for the performance of the work
- Preparation /signing of the contract
- Identification of employee

**b) For compliance with a legal obligation. Indicatively and not limited to, for:**
- Cyprus and International legislation requirements

**c) For the performance of a task carried out in the public interest**

**d) For the purposes of safeguarding legitimate interests. Indicatively and not limited to, for:**
- Safety and security of facilities
- Monitoring CCTV footage at the entrance of the facilities for the safety and security of facilities

**e) On the basis of shore staff consent**
- Any such consent granted, may be revoked at any time by contacting us.

**2.3 HOW LONG THE COMPANY MAINTAINS DATA FOR SEAFARERS AND SHORE STAFF (COMPANY'S RETENTION POLICY)**

Hard copies and electronic files are retained for 5 years after signing off of crew members and shore staff.

If a crew or shore staff candidate is not acceptable hard copies shall be disposed of immediately.

The Company may keep data for longer than the said period for legal and/or regulatory and/or technical reasons. In such cases, the Company shall ensure that privacy is protected, and the data is used only for the purposes stated in the previous paragraph (processing purpose).

In cases where the Company wishes to retain the data with a view to a further job opportunity, the data subject shall be informed accordingly and be given the possibility to object to such further processing. In such cases a notice shall be provided to the data subject, and the data subject's consent to keep their personal data for assessing suitability for future employment possibilities shall be obtained. Such consent shall be renewed every three (3) years.

Data no longer required shall be deleted and disposed of.

**2.4 WHO THE COMPANY SHARES DATA WITH**

No information relating to data subject's personal data shall be disclosed to anyone, other than in the cases permitted by the legal and regulatory framework in force from time to time. These are:

a) Where the Company (or any third party acting on Company's behalf) is legally compelled to do so or where disclosure is required for purposes of compliance with the legal and regulatory framework governing shipping industry (With insurance Companies, P&I Club, Medical Centres, Hospitals, public authorities psychometric test service etc.)

b) Where the Company has contractual obligation to do so (with Managing Companies, Shipowners, charter parties, IT companies, mobile phone companies, class societies, etc.)

c) Where it is in Company's legitimate interests to disclose information (lawyers, legal advisors etc).

d) Where disclosure is made at data subject's request or with data subject's consent or to satisfy the Company's contractual obligations towards the data subject. (Third parties as agents, Travel agents, banks, accounting firms, other manning agents etc.)

e) Companies or individuals that data subject asks the Company to share its data with.

f) To various clients of the company aiming to find a potential employer accepting the profile (qualifications, experience etc) of a particular individual seafarer.

### 2.5 PERSONAL DATA OF THIRD PARTIES

Personal data of third parties may include: Name, Surname, Parents Name, next of kin name, offices, address, VAT number.

Without data processing, the Company cannot enter into or perform the terms of a contract with data subject.

Where data collection is optional, this shall be made clear at the point of collection.

#### 2.5.1 Processing Purpose

The Company process third party's personal data for one or more of the following reasons:

**a) For the performance of a contract to which the data subject represents or is a contractual party**

**b) For compliance with a legal obligation (**Local port regulations)

**c) For the performance of a task carried out in the public interest**

**d) On the basis of third-party consent.** Any such consent granted, may be revoked at any time by contacting the Company.

**e) For a potential employer identification**

#### 2.5.2 How long the Company Maintains Data for Third Parties (Company's Retention Policy)

Hard copies and/or electronic files are retained for 5 years after the termination of the contracts/cooperation.

Company may keep data for longer than the said period for legal and/or regulatory and/or technical reasons.

If the Company do so, will ensure that privacy is protected and the data is used only for the purposes stated in the previous paragraph (processing purpose).

In cases where the Company wishes to retain the data with a view to a further cooperation, the data subject shall be informed accordingly and be given the possibility to object to such further processing. In such cases a notice shall be provided to the data subject, and the data subject's consent to keep their personal data for assessing suitability for future employment possibilities shall be obtained. Such consent shall be periodically renewed in case of "data subject" collaboration discontinuation.

Data no longer required shall be deleted and disposed of.

### 2.6 DATA RECORDING

The Controller in each department shall maintain in hard copies and/or as well as electronically the records of processing activities under its responsibility.

In these records must be documented what personal data is held, where it came from and whom it is shared with, where is held, in what format is held, where it is obtained from, basis for holding it (consent/legal basis).

From the records, conclusion can be drawn if personal data are processed **fairly, lawfully, in transparent manner**, for **limited** purposes (collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes), if they are **minimized** (adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed), if they are **accurate** (and, where necessary, kept up to date), **not kept for longer period than is necessary**, **in line with the data subjects' rights**, **secured, and in case of transfer to other countries if there is adequate protection.**

The controller shall ensure compliance of the processing with the above principles.

**2.7 WHO THE COMPANY SHARES DATA WITH**

Nothing relating to data subject's personal data shall be disclosed to anyone, other than in the cases permitted by the legal and regulatory framework in force from time to time. These are:

a) Where the Company (or any third party acting on Company's behalf) is legally compelled to do so or where disclosure is required for purposes of compliance with the legal and regulatory framework governing shipping industry

b) Where the Company has contractual obligation to do so

c) Where it is in Company's legitimate interests to disclose information (e.g. to protect the Company's interest (in claims etc.).

d) Where disclosure is made at data subject/(your) request or with your consent or to satisfy Company's contractual obligations towards data subject. (Third parties as agents, Travel agents etc.)

e) Where data subject asks our Company to share its data with other Companies or Individual.

**2.8 DATA TRANSFER**

The Company may transfer data subject personal data in and outside of European Union in the following cases:

- Where the data subject has explicitly consented to the proposed transfer for example, where the transfer is necessary for the execution of a payment order to a bank account held at a credit institution in a third country
- Where the transfer is necessary for the execution of a contract,
- Where the transfer is necessary to satisfy local Authorities, statutory and/or commercial auditors and inspectors requirements worldwide, arising of international conventions, rules and regulations and local regulations a vessel is calling too.
- Where such transfer is necessary to establish, exercise, support legal claims or defend Company's rights.
- Where there is an obligation under a legal provision or a transnational or international convention.
- Where the European Committee has issued delegated acts for the adequate protection of the personal data in the specific country or to an international organization.
- Where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- Where the transfer is necessary for important reasons of public interest,
- Where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- To various clients of the company aiming to find a potential employer accepting the profile (qualifications, experience etc) of a particular individual seafarer.

**2.9 MAIN RIGHTS OF DATA SUBJECT**

The following are the rights that data subject has pursuant to the provisions of the GDPR as well as any other legislation in relation to data protection:

**1. Information and access right to personal data**

Data subject has the right to request access to its personal data.

This enables data subject to have incomplete or inaccurate data held by the Company corrected, though the Company may request to verify the accuracy of the new data that the data subject provides.

Data subject's access requests must be in writing.

A standard request form will be available through the Company's website.

Where the person managing the access (DPO) does not know the individual personally, the identity of this individual shall be checked and verified before handing over any information.

*(The above has been deleted as at the beginning all seafarers will be unknown to our company and even later new candidates will be coming. How is possible their identity to be checked. It is common practice of the industry an auditor to find something which is missing than to be included in our policy things which cannot be implemented resulting more serious concerns)).*

**2. Right to rectification**

Data subject has the right to request correction of the personal data that are hold from the "Company". With this right, the data subject may request any incomplete or inaccurate data be corrected and the Company may need to verify the accuracy of the new data provided.

**3. Right to erasure**

Data subject has the right to request erasure of the personal data that are hold from the Company where there is no valid reason for the Company to continue processing it.

In such cases the Company may be entitled to keep the data if it still has legitimate grounds to process the personal data.

**4. Right to restrict processing of personal data**

Data subjects shall have the right to obtain from the controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

**5. Right to data portability**

Data subjects can demand that their personal data be ported to them or to a new provider (transmitted directly to another organization where technically feasible) in a structured, commonly used, and machine-readable format, and to the extent this will not undermine the rights of others. The request must be made within one month (with extensions for some cases) and any intention not to comply must be explained to the individual**.**

The case that data relates to more than one data subject and how to address the difficulties this creates must be considered.

The Controller, in coordination with the external IT consultant, shall ensure that formatting capabilities are developed to meet access requests for providing portable data.

**6. Right to object and automated individual decision making**

The Company does not make decisions on the basis of automated processing.

**7. Right to withdraw consent**

Data Subjects may, at any time and free of charge, withdraw any consent they previously provided regarding the processing of their Personal Data.

This will not affect the lawfulness of the Processing before the consent withdrawal.

**8. Right to lodge a complaint**

Data subject has the right to lodge a complaint to the Company on how its personal information has been used or to the Data Protection Authority in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

### 2.10 LIMITING PHYSICAL ACCESS TO THE COMPANY'S PERSONNEL TO VIEW/EDIT SUBJECT'S DATA (INTEGRITY/CONFIDENTIALITY)

According to the principle of integrity/confidentiality, data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Therefore, data information shall be accessed only by the departmental personnel that will use them for the completion of their duties. Access in this case means not just by staff, but also by people outside the Company (refer also to section 4 of this manual).

The data must not be shared with the other departments informally.

Personal data transferred to the Company shore facilities shall be transmitted only to the competent employees and not to an uncontrolled group of personnel or any other recipients.

Personal data shall not be disclosed to unauthorized people either within the company or externally.

Staff members who have access to personal data are subject to a confidentiality obligation (e.g. via a clause in the employment agreement) and also a Confidential Disclosure Agreement (CDA) shall be signed with third parties to protect private or confidential information from becoming public or more widely known.

For each confidentiality level it may be worth setting out the broad security measures to be followed, such as password protection, clear desk policy, entry control (refer to section 4 for confidentiality levels).

This principle may be relaxed in the case of information which poses a low risk: for example, a list of business contacts may be made generally available, even if this means people having access who don't strictly need it.

The Company's personnel shall be trained in order to understand the responsibilities when handling data (refer also to section 5 of this manual).

### 2.11 STORAGE SAFETY/SECURITY GUIDELINES FOR HARD COPIES AND ELECTRONIC FILES AND COMMUNICATION OF DATA AND SENSITIVE DATA

Hard files shall be secured in locked cupboards. Keys/ access to the cupboards shall be provided only to personnel whose duties are directly involved with the respective documents/ records.

Appropriate digital security/ organizational measures are established for controlling the access to the electronic filing system (refer to section 4 of this manual), including backup procedures (both for data and for key staff availability) and emergency planning.

Strong passwords shall be used for accessing electronic files/ user accounts. These passwords shall never be shared with other persons either within the Company or externally.

The access to the server room is prohibited. The door shall be always locked, and digital security measures are established by the Company (refer to section 4 of this manual).

All employees shall implement the "Clear and lock" policy which means to "keep the desk clear" and "the computer screen locked" practice when the controller is away from his desk.

Employees should keep all data secured, by taking sensible precautions and following the guidelines below:

Encryption tools must be used when the controller communicates sensitive data via email.

Implementation of technical and organizational measures to ensure that data compliance measures are considered and integrated in the data processing activities (privacy by design) (i.e. email accounts: To use official email addresses – not unofficial, private, or any other non-secured email accounts or non-licensed programs).

For online services, it must be ensured that there is an automated way for privacy notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'.

The controller has to respect and treat everyone's personal data with the same respect he/she would wish for his/her own. For that reasons the following shall be considered:

a) *Minimizing* the generation of personal data by email and on paper – the less personal data are being created and circulated, the easier it is to protect. Only send information which is necessary for the handling of the case.

b) *Cybersecurity* – Ensure that computer systems are secured and make use of security measures such as password protection and secured email servers when transferring attachments containing passports, medical reports, contracts of employment etc.
c) *Anonymization* – Aim to use identifiers for individuals, like crewmember, broker, surveyor etc. instead of names and dates of birth. Other identifiers could be the vessel name, the nature of the incident, or the port of disembarkation, with a reference number. This applies not just to the subject heading and body of an e-mail but also, where possible, to any documents which support the claim. If there is no alternative to using a name, it is recommended that it is cited with as few other identifiers as possible. This approach should be made also for claim descriptions. If these steps are put into practice, except for those directly handling the claim, it will not be possible to identify the individual who is the subject matter of the claim.
d) *Start afresh* - if the controller cannot avoid identifying an individual, do so once and then start a new email so that the same personal data is not repeated in the email chain.
e) Before using "reply all", check that it is appropriate that everyone in the circulation list should actually receive the e-mail you are about to send.
f) It may be worth setting out special precautions to be taken when information is in particularly risky situations, such as being worked from home, from personal mobile phones etc.
g) Common situations which may be worth mentioning include whether staff contact details may be given over the phone This principal may be relaxed in the case of information which poses a low risk: for example, a list of business contacts may be made generally available, even if this means people having access who don't strictly need it.

When access to data or sensitive data is required between Company's personnel department a request must be send to DPO of the Company. In that case there will always be cases where the organisation feels it is right to break confidentiality, and the DPO will decide on a case-by-case basis whether this is appropriate.

### 2.12 MODIFICATION OF PRIVACY NOTICE FOR PROTECTION OF PERSONAL DATA

Changes of Company's privacy policy may take place from time to time preferable every three years.

The revised privacy policy will be available either in Company's premises or by providing privacy notices.

### 2.13 COMMUNICATION WITH DATA SUBJECTS

It is Company's recommendation that data subject review Companies website periodically so as to be always informed as to how Company protect and process its personal information.