GENERAL DATA PROTECTION POLICY

The Company fully adopts the **General Data Protection Regulation (GDPR)** requirements and supports Natural Persons' "rights and freedom" to ensure that their **Personal Data** is not processed without their knowledge and consent. This includes any information such as Name, Identification Number, location Data, online Identifiers or any factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The above commitment especially applies for **Sensitive Data** that may give rise to strong stigmatization or discrimination. These are a special Personal Data subcategory that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership as well as the processing of genetic / biometric Data for the purpose of uniquely identifying a natural person and expands further to Data concerning health, sex life or sexual orientation.

In full compliance with the GDPR Regulations, the Company is committed to take all reasonable protection measures to safeguard the Personal & Sensitive Data of its Office and Shipboard Personnel, as well as any such Data of any 3rd Party Staff which are maintained by the Company.

Top Management, making this policy a Top Priority, has adopted a set of procedures that ensure:

- **Lawfulness, Fairness and Transparency**: All Personal & Sensitive Data is processed in a lawful, fair and transparent manner and, where appropriate, with the knowledge and consent of the natural person ("Data subject").
- **Limited Purpose:** Personal & Sensitive Data is collected for specified, explicit and legitimate purposes and not further processed in a way not compatible with those original purposes.
- **Data Minimization:** The collection of Personal & Sensitive Data is limited and relevant to accomplish a specific purpose.
- **Data Quality & Accuracy:** Personal & Sensitive Data, which is stored and managed are accurate, complete and where necessary, kept up to date.
- **Storage Time Limitation:** Personal & Sensitive Data is not kept longer than is necessary for the purpose for which such Personal Data is processed.
- **Confidentiality and Integrity:** Personal & Sensitive Data is:
  - Processed in a manner which ensures security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage by using appropriate technical or organizational measures.
  - Available only to Personnel who need the Personal Data for their work and are permitted to access them.
  - Not informally shared and / or disclosed to unauthorized persons or organizations.
  - May be disclosed to Law Enforcement Organizations, after fully ensuring that the request is legitimate.
- **Robust Security Safeguards:** Personal & Sensitive Data is kept secured and protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.
- **Openness and Individual Participation:** Company Employees and / or 3rd Party staff are entitled to access information about their Personal & Sensitive Data, who is holding it and what they are using it for. They have the right to challenge the Data Controller for refusing to grant access to their Personal & Sensitive Data, as well as challenge the accuracy of the Data.
  Should such Data be found to be inaccurate, the Data should be erased or rectified.
- **Accountability:** This Policy requirements apply to the Company's **Data Controllers** i.e. persons responsible to protect Personal Data, and **Data Processors** i.e. Persons & 3rd Party Contractors processing Data.
  Data Controllers & Data Processors are held accountable for complying with the above principles.

All Employees who work for or with the Company, are held responsible for ensuring that Personal & Sensitive Data is collected, stored, and handled appropriately, in a manner that aims to minimize breaches of confidentiality and reputational damage.

Signed by COO:

George A. Kouleris