Celestyal Cruises Limited, including its subsidiaries

("Company")

DATA PROTECTION POLICY

CONTENTS

1 PURPOSE

To establish a systematic and controlled way for protecting personal data flowing through the Company.

2 RESPONSIBILITIES

- Data Protection Officer
- Top Management
- Department Managers
- All Company Employees

3 GENERAL INFORMATION

The Company recognises that everyone has clear rights with regard to the way in which their personal data is processed and that compliance with all relevant and applicable data protection legislation, rules and regulations will maintain confidence in the Company, build and reinforce the trust of its customers, employees and suppliers for the continuation of a successful business.

All data users including all the Company's employees shall comply with the Company's Data Protection Policy when processing personal data on the Company's behalf. Any breach of this policy may result in disciplinary action.

The types of personal data that the Company may be required to process shall include information about its current, past and prospective suppliers, customers, passengers, employees, employees' families (including children), and others with whom the Company communicates from time to time.

The personal data is subject to legal safeguards as incorporated in Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) ("GDPR") as well as national and local laws.

This procedure, and any other documents referred to in it, sets out the basis on which the Company will process any personal data that it collects from data subjects, or that is provided to the Company by data subjects or other sources. It sets out rules on data protection and the legal conditions that must be satisfied when the Company obtains, handles, processes, transfers and stores personal data.

The Data Protection Officer (DPO) is responsible for monitoring compliance with the GDPR and with the Company's Data Protection Policy and procedure. The post of the DPO is held by MR CHRISTODOULOS MELAS, dpo@celestyalcruises.com Any questions about the operation of this procedure or any concerns that the policy or procedure have not been followed should be referred in the first instance to the DPO. The DPO is under a duty to maintain privacy and all such enquiries will be treated with discretion and absolute confidentiality.

4 DEFINITION OF DATA PROTECTION TERMS

Data means information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects means, for the purpose of this procedure, all living identified or identifiable natural persons about whom the Company holds personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her.

Personal data means any information relating to an identified or identifiable natural person (i.e. a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, biometric, mental, economic, cultural or social identity of that natural person.

Data controllers means the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. The Company is the data controller of all personal data used in the Company's business for its own commercial purposes.

Data users means the Company's employees, consultants or agents whose work involves processing personal data on the Company's behalf. Data users must protect the data they handle in accordance with this procedure and any applicable data security procedures at all times.

Data processors means any natural or legal person, public authority, agency or other body which processes personal data on behalf of the Company

Processing means 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.

Special category of personal data means data about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special category of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Binding corporate rules means personal data protection policies which are adhered to by the Company or data processors established in the territory of an EU Member State for transfers or a set of transfers of personal data to a data controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

5 DATA PROTECTION PRINCIPLES

The Company is accountable for demonstrating compliance with the GDPR's six principles of processing personal data. These provide that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

- Accurate and, where necessary kept up to date; every reasonable step must 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)

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose 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, historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject; (storage limitation)

- Processed in a manner to ensure 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)

6 LAWFUL, FAIR AND TRANSPARENT PROCESSING

- The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly, transparently and without adversely affecting the rights of the data subject.

- For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among others:

o the data subject's consent to the processing for one or more specific purposes;

o that the processing is necessary for the performance of a contract with the data subject;

o for the compliance with a legal obligation to which the data controller is subject;

o to protect the vital interests of the data subject or for the legitimate interest of the data controller or the party to whom the data is disclosed.

When special categories of personal data are being processed, additional conditions must be met. When processing personal data as data controller in the course of its business, the Company will ensure that these requirements are met.

7 PROCESSING FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

- In the course of the Company's business, the Company may collect and process the personal data set out in the Schedule. This may include data the Company receives directly from a data subject (for example, by completing forms or by corresponding with the Company by mail, phone, email or otherwise) and data the Company receives from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies).

- The Company will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the GDPR. Should the Company need to process the personal data for another purpose than those set out above, then it will promptly notify the data subject. If the Company processes personal data on other legal grounds than consent or on the basis of EU law or the laws of an EU Member State then the Company will first ascertain whether the new purpose is compatible with the initial purpose, the reasons for processing, the nature of the personal data and the possible consequences for the data subject.

8 NOTIFYING DATA SUBJECTS

Where the Company collects personal data directly from data subjects and where it is required to do so under the GDPR, it will inform the data subject about:

- the purpose or purposes for which it intends to process that personal data and the legal basis upon which it will process that personal data;
- the types of third parties, if any, with which the Company will share or disclose that personal data to;
- details of any transfers of that personal data outside of the Europe Union (see section 14 below);
- the period during which the Company will keep that personal data and, if relevant, the criteria used to determine that retention period;
- the data subject's right to request access to and rectification or erasure of the data subject's personal data or to request restriction of processing of the data subject's personal data, and, if processing is based on the data subject's consent, then the data subject's right to withdraw consent;
- where reasonably possible, the data subject's right to data portability.
- the data subject's right to complain to a supervisory authority;
- whether there are any statutory or contractual requirements to provide the personal data and any consequences of not doing so; and
- whether the Company uses the personal data to undertake any automated decision making.

If the Company receives personal data about a data subject from other sources, it will provide the data subject with this information within a reasonable period of time

The Company will also inform data subjects whose personal data the Company processes that the Company is the data controller with regard to that data, and who the Data Protection Officer is.

9 ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY

The Company will only collect personal data to the extent that it is required for the specific purpose notified to the data subject and kept only as long as is necessary.

10 ACCURATE DATA

The Company will ensure that personal data it holds is accurate and kept up to date. It will check the accuracy of any personal data at the point of collection and at appropriate intervals afterwards. It will take all reasonable steps to rectify or erase any inaccurate or out-of-date data without delay.

11 LIMITATION ON STORAGE

The Company will not keep personal data in a form which permits identification of data subjects longer than is necessary for the purpose or purposes for which they were collected. It will take all reasonable steps to destroy, or erase, from its systems, all data which is no longer required.

12 PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

The company will process all personal data in line with the data subjects' rights, under the GDPR which are captured in this procedure.

13 DATA SECURITY

The Company will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Company will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction or erasure. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

The Company will maintain data security by protecting the confidentiality, integrity and availability of personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means ensuring that personal data is protected against undesirable destruction or loss and that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Company's central computer system instead of individual PCs.

Security procedures include:

Entry controls. Any stranger or unauthorised person seen in entry-controlled areas should be reported and prevented from gaining access to systems where personal data are processed.

Input controls. Data users' activities should be logged enabling the subsequent establishment of whether and by whom Personal Data have been entered, modified or removed from the Company's data processing systems.

Access controls. Personal data should be prevented from being read, copied, modified, removed or exported to other devices or formats by unauthorised persons. Data users entitled to access certain personal data should only be able to access the data they need and are authorised to do so.

Secure lockable desks and cupboards. All desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EU

As an international cruise line company, the Company may transfer certain personal data that it holds on EU data subjects to a country outside the European Union ("EU"), provided that one of the following conditions applies:

- The country to which the personal data is transferred has an adequate level of protection for the data subjects' rights and freedoms;

- The data subjects have given their consent;

- The transfer is covered by one of the exemptions set out in the GDPR, including the performance of a contract between the Company and the data subject, or to protect the vital interests of the data subjects;

- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

- The transfer is authorised by the relevant data protection authority where the Company has adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

The personal data the Company holds will also be processed by the Company's employees, operating outside the EU, who work for the Company or for one of the Company's suppliers. Such employees may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

As an international cruise line company, the Company may share personal data it holds with any member of its group, which means the Company's subsidiaries, or its ultimate holding company and its subsidiaries.

The Company may also disclose personal data it holds to third parties:

- In the event that the Company sells or buys any business or assets, in which case the Company may disclose personal data it holds to the prospective seller or buyer of such business or assets.

- If the Company or substantially all of its assets are acquired by a third party, then any personal data it holds shall be one of the transferred assets.

The Company may be under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation that it is under, or in order to enforce or apply any contract with the data subject or other agreements; or to protect the Company's rights, property, or safety of its employees, customers, or others. This may also include the Company exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

The Company may also share personal data which it holds with selected third parties for the purposes set out in the Schedule.

16 DEALING WITH SUBJECT ACCESS REQUESTS

Data subjects must make a formal request for information the Company holds about them. This request must be made in writing. The provision of the personal data will be free of charge, although the Company reserves the right to charge reasonable administrative charges for subsequent copies of any further data provided or in relation to any excessive or disproportionate requests.

Any Company employee who receives a written data access request must forward it to their department manager and the Company's DPO immediately.

When receiving telephone enquiries, the Company will only disclose personal data it holds on its systems in accordance to the Company's relevant department's policies and procedures.

17 TRAINING

Each department will provide training to promote or reemphasise compliance with this procedure.

18 OWNERSHIP

It is each employee's responsibility to comply with the Company's Data Protection Policy and relevant procedures. Each department manager shall ensure the that the Company's Data Protection Policy and relevant procedures are implemented. Any questions regarding the implementation of the Data Protection policy and procedures should be directed to the DPO.

19 ANNUAL DATA PROTECTION SELF AUDIT

Each department shall review its data collection, processing and security practices annually to ensure compliance with this procedure and where necessary to make recommendations for improvement to the relevant policies and procedures. Such recommendations shall be made in writing and addressed to the DPO.

20 DATA INCIDENT NOTIFICATIONS

Where it is established that a data incident has occurred which may be considered as a data breach immediate notice of this must be given to the department manager and the DPO.

21 CHANGES TO THIS PROCEDURE

The Company reserves the right to change this procedure at any time in order to comply with its legal obligations.

SCHEDULE

DATA PROCESSING ACTIVITIES

A. TYPES OF DATA AND PURPOSE OF PROCESSING

The types of data we collect in the course of and in connection with the provision of our services include without limitation:

- Your name, contact details, identification documents (which may include information relating to your date and place of birth), nationality- Such data may be requested to provide you information as to your request whether submitted via email, call centre or the Website or to handle and complete your booking;
- Valid travel documents and visas, where applicable-Such data is processed to comply with regulatory requirements in the ports of call;
- Data in relation to your health, (ie medical conditions requiring special attention onboard the vessel) for the purpose of identifying and being considerate of any disabilities or special dietary requirements you may have;
- Your name, cabin number, your picture (when embarking the Vessel), people you are travelling with, port of embarkation, port disembarkation and information. Such data is processed on the basis of the need to ensure public security or in the event to manage an emergency.
- Your email, when you have provided your consent, to provide you information as to our latest offers and products, newsletters.
- Details of qualifications and skills, background checks (where applicable), previous employment history and references. Such data is collected during the recruitment process.

B. TRANSFER OF DATA- DATA RECIPIENTS

In order to provide you the services contracted for, we may share information about you with our commercial partners that provide some of the services you may have booked, ie shore excursions. In addition, we do share personal data with local port agents and authorities for immigration purposes.

Where we are obliged to share your personal data and to ensure that your personal data is treated in a manner consistent with, and which respects EU laws on data protection, where appropriate to do so, we have adopted standard contract clauses.

C. RETENTION OF PERSONAL DATA

The Company will only use/store your personal data for as long as necessary to fulfil the purposes for which it was collected (ie for the purposes of satisfying any legal, regulatory, accountancy or reporting requirements as part of a contract) and in compliance with legislative and regulatory requirements.

In some circumstances we may anonimise your persona data (so it can no longer be associated with you) for research or statistical reasons in which case we can use this information without further notice to you.