Data Processing Policy

The General Data Protection Regulation/2018 will be replacing the current Data Protection Act (DPA) on 25th May 2018. As a result, all businesses holding personal data must ensure their procedures are compliant with the new incoming legislation.

This document ensures compliance with the same.

We will always treat such personal information with the utmost respect and be aim to be as open as possible in terms of how information is used. It is used specifically to carry out the requested contractual function and we will never use it for Marketing purposes, nor we will never share it with other organisations for marketing purposes.

General

The Client and S5 (together, the "Parties") have entered into an agreement for the provision of Port agency management services by S5 to the Client and, where applicable, to the Client's Affiliates ("Port Agency Agreement").

In performance of its obligations under the Port Agency Agreement, S5 processes Personal Data on behalf of the Client as set forth herein and in the Port Agency Agreement ("Contract Data Processing"). The Parties agree that, in relation to the Contract Data Processing, S5 is the Processor and the Client is the Controller.

By agreeing to the Data Processing Policy, by submitting information as per our agreement, the Client enters on its own behalf and, to the extent required under applicable data protection laws, on behalf of its Affiliates, if and to the extent S5 processes Personal Data for which such Affiliates qualify as Data Controller.

The Terms forth herein are intended to form a legally binding agreement between S5 and the Client which shall be governed by English law and subject to the exclusive jurisdiction of the English courts in respect of any contractual and non-contractual disputes arising in connection with these Terms. These Terms are intended to apply in addition to any contract for the supply of Services that may be entered into between the parties from time to time. If there is any conflict between these Terms and the terms of any contract for Services (whether entered into before, on or after the date of that these Terms take effect) then the provisions of these Terms shall take priority.

In consideration of the Parties' mutual rights and obligations set out in the Port Agency Agreement and this Policy, the Parties agree as follows:

1. PROCESSING OF PERSONAL DATA

1.1 S5 shall process Client Personal Data only on behalf of the Client and in strict accordance with the Client's written instructions, including with regard to transfers of Personal Data to a Third Country or an international organisation, unless required to do so by Union or Member State law to which S5 is subject. In such a case, S5 hall inform the Client of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest. For the avoidance of doubt, whenever this Policy or the Port Agency Agreement include provisions relating to the Processing of Client Personal Data (e.g. an obligation to anonymise certain Client Personal Data) such Processing shall be considered an instruction of the Controller pursuant to this Policy.

1.2 When processing any Client Personal Data outside of the territory of the European Union or the EEA or engaging in any act or practice regarding Client Personal Data where that act or practice is

subject to data protection laws in jurisdictions outside the territory of the European Union or EEA, S5 shall comply with those applicable data protection laws, and in particular will provide appropriate safeguards to ensure an adequate level of data protection in accordance with Art. 44 et seq GDPR.

1.3 Purpose of Processing. S5 shall process Client Personal Data for the purpose of providing the services described in the Port Agency Agreement ("Contract Services") and any additional services under this policy ("Processing Services") to the Client ("Admissible Purpose"). The Parties agree and acknowledge that the Client will be qualified as Controller and S5 will be qualified as Processor when processing Client Personal Data hereunder.

1.4 Duration of Processing. The duration (term) of this Policy is equal to the term the continuance of the relationship and shall terminate when the relationship terminates, with the exception of any provisions intended to survive termination.

1.5 Categories of Personal Data. This includes but not limited to:

- Crew/ Individual profile Data. Name, telephone number, email, job title, office location, employee number, passport and visa information (including date of birth, nationality, place of birth, passport number and expiry date), Seaman's book, driving licence number and information, mileage and frequent flyer/guest card numbers.
- Passenger Name Record ("PNR") Data. Traveller Profile Data processed in PNR format associated with reservation data, including flight dates and routings, flight numbers, hotel reservations, car rental bookings, rail bookings, ticketing information, authorisation solutions and travel risk management.
- Medical and Special Assistance Information. Provided in connection with sick crew/ medical assistance and medical travel arrangements which potentially concern health conditions or indicate religious belief.
- Insurance data: Processed in connection with insurance and P&I claims, for the purpose of invoicing on behalf of the client
- LOIs/ OKTB: Provided in connection with immigration formalities and boarding of vessels.

2. REQUIRED TECHNICAL AND ORGANISATIONAL MEASURES

2.1 S5 shall take all appropriate technical and organisational measures to ensure a level of security for the Client Personal Data which is appropriate to the risks to individuals that may result from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Client Personal Data. Without prejudice to the generality of the previous sentence, the S5 shall:

(a) prevent (i) unauthorised or unlawful processing of the Client Personal Data; and (ii) the accidental loss or destruction of, or damage to, the Client Personal Data; and

(b) ensure a level of security appropriate to (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the Client Personal Data to be protected,

(c) If there is any conflict or inconsistency between any of these requirements, the requirement that provides the greater level of security shall apply;

including, as appropriate, the measures referred to in Article 32 GDPR ("Data Security Standards").

2.2 Acknowledging that the Data Security Standards are subject to technical progress and development, the Parties agree that S5 shall be authorised to implement adequate alternative technical and organisational measures provided, however, that such measures shall not materially fall

short of the level of security provided by the Data Security Standards and shall comply with the requirements under applicable laws.

3. DATA SUBJECT RIGHTS

3.1 S5 shall correct, delete, block or otherwise process Client Personal Data and shall take any other measures in relation to requests from Data Subjects in relation to their rights under applicable laws ("Data Subject Requests") only in accordance with and subject to the written instructions of the Client. S5 shall promptly provide any required information and use best efforts to assist the Client in dealing with any Data Subject Requests.

3.2 The Client shall be solely responsible for dealing with Data Subject Requests. S5 shall promptly notify the Client of any Data Subject Requests or other enquiries relating to this policy without responding to such requests or enquiries unless expressly otherwise instructed by the Client.

4. FURTHER OBLIGATIONS OF S5

4.1 S5 shall maintain a written record of all categories of processing activities carried out on behalf of a Client in accordance with Art. 30 par. 2 GDPR.

4.2 S5 shall reasonably assist the Client in relation to:

(a) preparation of the records of processing activities in accordance with Art. 30 GDPR in relation to the Processing under this Policy and shall immediately upon request provide the Client with any information required for this purpose in a format reasonably requested by the Client;

(b) data protection impact assessments (DPIA) in accordance with Art. 35 GDPR; and

(c) any requests or consultations with the responsible Supervisory Authority.

4.3 S5 shall ensure that any personnel undertaking or involved in the Processing under this Policy are properly qualified and trained and have committed themselves to keep Client Personal Data confidential or are under an appropriate statutory obligation of confidentiality in accordance with applicable law which shall survive termination of this Policy.

5. SUB-PROCESSING

5.1 S5 shall be authorised to engage other Processors in relation to the Contract Data Processing ("Sub-Processor") only in accordance with and to the extent permitted by applicable laws.

5.2 Where S5 engages a Sub-Processor for carrying out specific processing activities on behalf of the Client, S5 shall enter into an agreement with the Sub-Processor which includes terms which offer at least the same level of protection for Client Personal Data as those set out in this Policy and meet the requirements of Art. 28 par 3 GDPR.

5.3 S5 shall conduct regular audits as required under applicable law to ensure that the Sub-Processor complies with the Data Security Standards, applicable laws and its other contractual obligations.

5.4 In case of non-compliance of the Sub-Processor with its contractual obligations relating to Client Personal Data, S5 shall remain fully liable to the Client for any damages caused by such non-compliance and shall indemnify and hold harmless the Client against any claims or damages in connection with or resulting from the engagement of the Sub-Processor.

6. RESTRICTED TRANSFERS

6.1 The Parties will immediately upon reasonable request of either Party and prior to commencement of any Restricted Transfer (i) enter into the standard clauses set forth in the Commission Decision dated February 5, 2010 (2010/87/EU) and/or (ii) enter into or establish any other appropriate instruments or undertakings required under applicable law to effect such Restricted Transfer without breach of such applicable law. If so required by applicable law, S5 shall cause any Sub-Processor to enter into such instruments or undertakings directly with the Client or shall enter into such instruments or undertakings with the Sub-Processor in the name and on behalf of the Client based on an appropriate Power of Attorney to be issued by the Client promptly upon request of S5.

6.2 "Restricted Transfer" means any transfer of Client Personal Data by or to any of the Parties or a Sub-Processor which would be prohibited by applicable law in the absence of the instruments or undertakings referred to in Section 7.1 above.

6.3 When processing Client Personal Data outside of the territory of the European Union or the EEA or engaging in any act or practice regarding Client Personal Data where that act or practice is subject to data protection laws in jurisdictions outside the territory of the European Union or EEA, S5 shall comply with those data protection laws, and in particular will provide appropriate safeguards to ensure an adequate level of data protection in accordance with Art. 44 et seq GDPR.

7. INSPECTIONS AND AUDITS

7.1 As part of its normal contractual arrangements S5 shall allow the client, its auditors and its authorised representatives, to perform audits of its operations Including the directives set out in this Policy. Seven days' written notice to perform both remote and on-site audits and inspections of the Supplier's premises, systems, employees and relevant records and information as may be reasonably required, to the extent required by applicable law and in accordance with this Section, in order to:

(i) fulfil any legally enforceable request by any regulatory bodies; and/or
(ii) verify that personal data is being processed in accordance with the terms of these Terms.

7.2 S5 shall, upon the Client's request in writing, S5 shall make available to the Client on request all information necessary to demonstrate compliance with this policy and provide the Client with a summary of the results of its latest internal data security audit.

7.4 No documentation or information may be copied, shared, transmitted, except as mutually agreed or required by applicable law. Any non-public documentation and information disclosed to the Client in accordance with this Section shall be deemed proprietary and confidential information of S5. The Client shall not disclose such documentation or information to any third party or use it for any purpose other than evaluating S5's compliance with the Policy.

8. PERSONAL DATA BREACHES AND INCIDENTS

8.1. S5 shall promptly notify the Client of any technical, organisational or other incidents (including incidents at Sub-Processors) which have resulted or may result in a Personal Data Breach in the sense of Art. 33 par. 1 GDPR affecting Client Personal Data ("Data Security Incident"). Data Security Incidents include in particular, but are not limited to, the following:

(a) any actual or suspected unauthorised access, disclosure, loss, download, theft, blocking, encryption or deletion by malware or other unauthorised action in relation to Client Personal Data by unauthorised third parties;

(b) any actual or suspected operational incidents which have an impact on the Processing of Client Personal Data;

(c) any actual or suspected breach of this Policy or applicable law by S5, its employees or agents to the extent that such breach affects the integrity and security of Client Personal Data or materially adversely impacts S5's obligations under this Policy; or

(d) any legally binding request for disclosure or seizure of Client Personal Data by a law enforcement or other public authority unless S5 is prohibited by statutory law to notify such incident to the Client.

8.2 In the event that S5 is required under applicable law to notify a Data Security Incident to a Supervisory Authority or other authority, the Data Subjects concerned or any other third parties (e.g. if the Data Security Incident results in a Personal Data Breach for which S5 is itself responsible as Controller), S5 shall, to the extent permitted under applicable law and reasonably possible, liaise and coordinate with the Client prior to making such notification. The Parties shall use their best efforts to agree on a joint approach with a view to prevent any contradicting or inconclusive notifications. This includes providing each other with the details of any notification and the date and time on which notification will be made.

8.3 In the event of a Data Security Incident, S5 shall promptly take any measures required and appropriate under applicable law and technical standards to restore the confidentiality, integrity and availability of the Client Personal Data and the resilience of the processing systems and services and to mitigate the risk of harm and/or any detrimental consequences for the Data Subjects affected or potentially affected by the Data Security Incident.

8.4 The Parties shall use best efforts to support each other in the event of any audits, enquiries, investigations or other proceedings initiated by a Supervisory Authority or any other public body in relation to the Contract Data Processing. To the extent permitted under applicable law, either Party shall immediately notify the other Party of such proceedings.

9. CLIENT'S OBLIGATIONS

9.1 The Client shall promptly take any action required to comply with its own obligations under applicable law in relation to the Processing of Client Personal Data hereunder (e.g. effect any required notification of Data Subjects).

9.2 The Client warrants that (i) it is entitled to engage and to provide the Client Personal Data to S5 and (ii) the Processing of the Client Personal Data, provided that S5 complies with applicable laws and the provisions of this Policy, does not infringe any third party rights. As Controller the client is responsible for the accuracy and completeness of the data passed to S5 in its capacity as processor.

10. CONTRACT TERMINATION AND DELETION OF CLIENT PERSONAL DATA

In case of Termination S5 shall securely destroy all copies of the client’s Personal Data in its possession or control, that has not been transferred already to the client, unless S5 is required by law to retain any copies of such data. In this case S5 shall process it solely as necessary to comply with its legal obligations.

S5 shall ensure that:

(i) access to the client Personal Data is limited to those individuals who need access in order to meet the Supplier's obligations under these Terms (together the "Authorised Personnel")

(ii) all Authorised Personnel are informed of the confidential nature of the client Personal Data and are bound by appropriate confidentiality obligations when accessing it.

11. DEFINITIONS

"Data Protection Laws" means all applicable laws, rules and regulations applicable from time to time relating to data protection, privacy and/or the processing of data relating to identified or identifiable individuals from time to time, including the UK Data Protection Act 1998, the GDPR (with effect from the date that it takes effect) and any laws and regulations that implement, supplement or amend the GDPR.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

"S5" means S5 Agency World Ltd entity with which the Client is contracting

"Affiliate" means any legal entity directly or indirectly controlling or controlled by or under direct or indirect common control with the specified entity. Where Control is defined as the possession, directly or indirectly, of the power to direct the management and policies of such entity, directly or indirectly, whether through the ownership of voting securities, by contract (including franchise or trademark licence agreement) or otherwise.

"Client" means the entity that has entered into a Port Agency Agreement with S5 and, for the purposes of this Policy only, and except where indicated otherwise, includes the Client's Affiliates.

"Contract Data Processing" has the meaning assigned to the term in the General Section.

"Data Subject" means the identified or identifiable living person to which Personal Data relates.

"Client Personal Data" means any data which can be used to identify an individual, either on its own or together with other data. Means any Personal Data processed by S5 on behalf of the Client pursuant to or in connection with the Port Agency Agreement.

"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"Data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

"Restricted Transfer" means the transfer of any Client Personal Data to any country or organisation, where such transfer would be prohibited by Data Protection Laws (or the terms of data transfer agreements put in place to address data transfer restrictions in Data Protection Laws) in the absence of the instruments or undertakings refers to in section 7.1

"Services" means any goods and/or services provided or to be provided and any other activities to be undertaken by S5 under the Port Agency Agreement that from time to time that may involve the processing of Client Personal Data.

"EEA" means the European Economic Area, which consists of the member states of the European Union, plus Norway, Iceland and Lichtenstein. If the UK leaves the EEA then it will still be treated as part of the EEA for the purposes of these Terms.

"Third Country" means the countries which are not a member of the EU or EEA and have not been recognized by the European Commission as providing an adequate level of Personal Data protection.

“Terms” means these terms.

The terms used in paragraph 1 (including the terms controller, processor, data subject, personal data, and related expressions) shall have the meanings given to them in the Data Protection Laws.