NORTHERN MARINE GROUP LIMITED
GDPR EXTERNAL DATA PROCESSOR POLICY

1. Interpretation

a. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Agreement. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

"Controller", **"Data Subject"**, **"Personal Data", "Joint Controller"**, **"Personal Data Breach"**, **"Processing"** (and the expressions **"Process"**, **"Processed"** and **"Processes"** shall be construed accordingly), "**Processor"** and **"Supervisory Authority"** have the meanings set out in GDPR;

"Data Controller" means Northern Marine Group Limited and any subsidiary company;

"Data Protection Legislation" means the GDPR and any other laws, regulations and provisions relating to Processing applicable in the United Kingdom;

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;

"Services" mean the services and other activities carried out or supplied by the Processor to the Data Controller under the Agreement;

"Sub-Processor" means any person appointed by the Processor to Process the Data Controller Personal Data; and

"Data Controller Personal Data*"* means any Personal Data Processed by the Processor on behalf of the Data Controller.

b. In this Policy, except where the context otherwise requires:
   i. any reference to a Clause or sub-clause shall be to, respectively, a Clause or sub-clause to this Policy;
   ii. clause headings are for ease of reference only and shall not affect the construction or interpretation of any Clause; and
   iii. words importing the singular shall include the plural and vice versa and words denoting any gender shall include all genders.

2. General Undertaking

The purpose of this Policy is to set out the scope of the Processing of Data Controller Personal Data to be carried out by the Processor from 25 May 2018.

3. Data Processing Obligations

The Processor shall:

a. comply with the applicable Data Protection Legislation in the Processing of Data Controller Personal Data;

b. Process Data Controller Personal Data only on the documented instructions from Data Controller (including with regard to transfers Data Controller Personal Data to a third country or an international organisation) unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform Data Controller of that legal requirement before commencing Processing, unless that law prohibits such information on important grounds of public interest;

c. take reasonable steps to ensure the reliability of any individual who may have access to or Process Data Controller Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Data Controller Personal Data, as strictly necessary for the Agreement, and ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

d. taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement and maintain (and provide details of such measures to Data Controller on request) appropriate technical and organisational measures to ensure a level of security appropriate to the risk including but not limited to the following:

e. the pseudonymisation and encryption of Data Controller Personal Data;
    i. the ability to ensure the ongoing confidentiality and access to Data Controller Personal Data in a timely manner in the event of a physical or technical incident;
    ii. the ability to restore the availability and access to Data Controller Personal Data in a timely manner in the event of a physical or technical incident; and
    iii. a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Processing.

f. in assessing the appropriate level of security, take account of the risks that are presented by Processing, in particular from a Personal Data Breach;

g. ensure that any individual acting under its authority who has access to Data Controller Personal Data does not Process the data except on instructions from Data Controller, unless he or she is required to do so by law (in which case this must be notified to Data Controller prior to any such Processing commencing);

h. taking into account the nature of the Processing, assist Data Controller by implementing and maintaining appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Data Controller's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Legislation;

i. assist Data Controller in ensuring compliance with Data Controller's obligations in so far as applicable to the Agreement under the Data Protection Legislation concerning:
    i. the security of Processing pursuant to Article 32 of the GDPR;
    ii. notification of a Personal Data Breach to the Supervisory Authority pursuant to Article 33 of the GDPR;
    iii. communication of a Personal Data Breach to the Data Subject pursuant to Article 34 of the GDPR; and
    iv. data protection impact assessments, including prior consultation with the Supervisory Authority, which Data Controller reasonably considers to be required pursuant to Articles 35 and 36 of the GDPR, in each case solely in relation to Processing of Data Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

j. within thirty (30) days after the end of the provision of Services relating to the Processing delete existing copies of all Data Controller Personal Data unless specifically instructed by Data Controller or where the retention of the Personal Data is required by law and only to the extent and for such period as required by law and always provided that the Processor shall ensure:
    i. the confidentiality of all such Data Controller Personal Data; and
    ii. that such Data Controller Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose, and if requested by Data Controller, provide evidence of the same.

k. immediately inform Data Controller if, in its opinion, an instruction infringes or conflicts with Data Protection Legislation and shall not commence such Processing until it has received confirmed instructions from Data Controller.

4. Personal Data Breach

a. The Processor shall notify Data Controller by email immediately and in any event within at least 24 hours after becoming aware of a Personal Data Breach relating to the Services or the Processing undertaken in relation to Data Controller. Where such notification is not made within 24 hours to Data Controller, the Processor must accompany the notice of such Personal Data Breach with details of the reason for the delay in notification.

b. The notification referred to in Clause 4.a shall include the following information as a minimum, and the Processor shall update such notification as and when more information becomes available:
    i. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
    ii. the name and contact details of the data protection officer or other contact point where more information can be obtained;
    iii. a description of the likely consequences of the Personal Data Breach; and
    iv. a description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

c. The Processor shall co-operate with Data Controller and take such reasonable commercial steps as are directed by Data Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

5. Records

a. The Processor shall maintain a complete and accurate written record of all categories of Processing activities carried out on behalf of Data Controller.

b. Such records shall include as a minimum:
    i. details of the Processor and any data protection officer it has appointed;
    ii. categories of Processing activities performed;
    iii. information regarding any cross border data transfers; and
    iv. a general description of the security measures implemented in respect of Data Controller Personal Data.

c. The Processor shall make available to Data Controller all information necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections, conducted by Data Controller and/or an auditor mandated by Data Controller.

6. Sub-Contracting

a. The Processor shall not engage a Sub-Processor without the prior specific authorisation of Data Controller.

b. Where the Processor engages a Sub-Processor:
   i. the Processor shall impose the same data protection obligations in this Policy and as required by Data Protection Legislation on the Sub-Processor by way of a written contract. In particular such contract must provide sufficient guarantees that the Sub-Processor shall implement and maintain appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the Data Protection Legislation; and
   ii. provide to Data Controller for review copies of such agreement with the Sub-Processor as Data Controller may reasonably request from time to time.

c. The Processor shall remain fully liable to Data Controller for the performance of the Sub-Processor's obligations.

7. Cross Border Data Transfers

The Processor shall not transfer Data Controller Personal Data outside of the European Economic Area without the prior written consent of Data Controller.

8. Severance

Should any provision of this Policy be invalid or unenforceable, then the remainder of this Policy shall remain valid and in force. The invalid or unenforceable provision shall be either: (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.