OneOcean

Data Processing Agreement (DPA)

PARTIES

Ocean Technologies Group operating as "OneOcean"
("**Supplier**" or **Data Processor**" or "**Processor**")

And

Customer
("**Customer**", "**Data Controller**" or "**Controller**")

1 BACKGROUND AND PURPOSE OF THIS AGREEMENT

1.1 The Parties have entered into an agreement under which Supplier grants to the Customer a licence to use Supplier's software, products, and services (the "**Subscription Agreement**"). The Subscription Agreement may require Supplier to process Customer Personal Data on behalf of the Customer. This Data Processing Agreement ("**DPA**") sets out the additional terms, requirements and conditions on which Supplier will process Customer Personal Data when providing services under the Subscription Agreement.

1.2 This Data Processing Agreement is an addendum to the Standard Terms and Conditions of Ocean Technology Group which shall apply to the extent not governed by this Agreement.

1.3 This DPA contains the mandatory clauses required by Article 28 of the GDPR.

1.4 This Agreement defines the roles of the Parties regarding the processing of Customer Personal Data and regulates the rights and obligations of the Parties pursuant to the relevant data protection legislation in force from time to time.

2 DEFINITIONS AND INTERPRETATION

2.1 "**Data Protection Legislation**" all applicable legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications), including, without limitation, the GDPR, as amended from time to time;

The terms "**Personal Data**", "**Personal Data Breach**", "**Data Subject**", "**Controller**" "**Processor**" and "**Process**" (and its derivatives) shall have the meanings given to them in the Data Protection Legislation.

"**EEA**" means the countries that comprise the European Economic Area, and Switzerland;

"**GDPR**" means either the UK GDPR or the EU GDPR, as applicable;

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

"**Restricted Transfer**" means an international transfer of Personal Data which would be prohibited by the Data Protection Laws in the absence of Standard Contractual Clauses.

"**Standard Contractual Clauses**" means i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, (a) the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office under section 119A(1) of the Data Protection Act 2018 which came into force on 21 March 2022; or alternatively (b) the International Data Transfer Agreement issued by the Information Commissioner's Office under section 119A(1) of the Data Protection Act which came into force on 21 March 2022 (together the "**UK SCCs**"), as the case may be.

"**UK GDPR**": has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

2.2 This DPA is incorporated into the Subscription Agreement. Interpretations and defined terms set forth in the Subscription Agreement apply to the interpretation of this DPA.

2.3 A reference to writing or written includes email.

2.4 In the case of conflict or ambiguity between:

a. any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;

b. any of the provisions of this DPA (including the Annexes) and the provisions of the Subscription Agreement, the provisions of this DPA will prevail.

3 THE ROLES OF THE PARTIES

3.1 Both Parties shall comply with the Data Protection Legislation.

3.2 The Parties agree that for the purpose of the Data Protection Legislation, Supplier is the Data Processor and the Customer is the data controller of any Personal Data processed under the Subscription Agreement.

3.3 The Customer retains control of the Personal Data and remains responsible for its compliance with its obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Supplier.

3.4 The Parties acknowledge that from time-to-time Supplier may also act as controller for certain Personal Data for purposes specifically agreed between the Parties in writing.

4 OBLIGATIONS OF SUPPLIER

4.1 Supplier shall process the Personal Data on behalf of, and according to the documented instructions of, the Customer and for the purposes of providing the services under the Subscription Agreement and for no other purpose unless required to do so by UK, EU, or Member State law (as applicable), in which case Supplier shall inform the Customer of that legal requirement before processing, unless prohibited from doing so by UK, EU, or Member State law (as applicable).

4.2 Notwithstanding Clause 4.1, Supplier may gather statistical data, analytics, trends and other aggregated or otherwise de-identified data derived from the Data Subject's use of Supplier software, products, and services ("**Aggregate Data**"). Supplier may use Aggregate Data to improve, support and operate Supplier software, products and services, and to create and distribute reports regarding use of such software, products and services. The Parties agree that Aggregate Data is not Personal Data and that, therefore, this DPA shall not apply to the Aggregate Data.

4.3 Supplier shall:

a. 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 natural persons, implement appropriate technical and organisational measures in such a manner as is designed to ensure a level of security appropriate to the risk, the determination of such appropriate measures to be made solely by Supplier (a general description of Supplier's security measures as at the date of this DPA is outlined in Annex 2);

b. on termination of the Subscription Agreement, at the Customer's option either return or destroy the Personal Data (including all copies of it) immediately, unless required to continue to store that Personal Data under UK, EU or Member State law (as applicable);

c. ensure that all persons authorised to access the Personal Data are subject to obligations of confidentiality.

d. make available to the Customer a statement of all information necessary to demonstrate compliance with the obligations laid out in Article 28 of the GDPR and, subject to Clause 5, allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer; provided that, in respect of this provision Supplier shall immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Legislation;

e. taking into account the nature of the processing, provide assistance to the Customer, insofar as possible, in connection with the fulfilment of the Customer's obligation to respond to requests for the exercise of Data Subjects' rights pursuant to Chapter III of the GDPR (as applicable); Also, Supplier shall notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and ensure that it does not respond to that request except on the documented instructions of the Customer or as required by Applicable Laws to which the Customer is subject, in which case Supplier shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before Supplier responds to the request

f. provide the Customer with assistance in ensuring compliance with Articles 32 to 36 (inclusive) of the GDPR (concerning security of processing, data breach notification, communication of a personal data breach to the data subject, data protection impact assessments, and prior consultation with supervisory authorities) to the extent applicable to the Customer, taking into account the nature of the processing and the information available to Supplier; and

g. notify the Customer without undue delay on becoming aware of a Personal Data Breach in respect of Personal Data that it processes on behalf of the Customer. Supplier shall co-operate with the Customer and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each Personal Data Breach.

5 OBLIGATIONS OF THE DATA CONTROLLER

5.1 The Customer shall ensure that it is entitled to transfer the Personal Data to Supplier under the Data Protection Laws and it has a valid legal basis and has given all necessary notices required under the Data Protection Laws to allow Supplier to process the Personal Data for the purposes set out in this DPA and to fulfil its obligations under the Subscription Agreement.

5.2 In relation to exercising its right of audit, including inspections, set out in Clause 4.3d above, the Customer shall:

a. be entitled to carry out such an audit at least once every 12 months;

b. provide at least 14 days' notice of any intended audit;

c. carry out such an audit only during business hours as set by Supplier;

d. carry out such an audit to a mutually agreed scope or as determined by Supplier to meet the specific requirements of the customer.

e. only audit the business areas and activities of Supplier which relate directly to the processing of Personal Data under the Subscription Agreement; and

f. at Supplier's request, require that any auditor enters into a confidentiality agreement with Supplier.

5.3 In relation to the exercise of Supplier's obligations under Clauses 4.3d, 4.3e and 4.3f of this DPA, Supplier shall be entitled to charge, and the Customer shall be bound to pay, a fee to cover any additional administrative costs incurred by Supplier in carrying out those obligations. Such fee is to be determined by Supplier.

5.4 The Customer shall consult with Supplier in respect of any notification to any applicable supervisory authority or data subjects of a Personal Data Breach notified to it under Clause 4.3g above, or otherwise relating to Supplier's processing of Personal Data under the Subscription Agreement.

5.5 [The Customer shall indemnify Supplier in full and on demand against all claims, losses damages or fines received by or paid by Supplier in respect of any use of the Personal Data by Supplier in accordance with the Customer's instructions howsoever arising.

6 SUB-PROCESSORS

6.1 The Customer hereby grants Supplier permission to appoint sub-processors under this DPA, including those sub-processors appointed at the date of this DPA, as set out in Annex 1. Supplier shall notify the Customer of any intended changes concerning the addition or replacement of other sub-processors at least ten days prior to adoption, thereby giving the Customer the opportunity to object to such changes. Customer will be required to provide response within a 10-day period to ensure no interruption to services.

6.2 Supplier shall ensure that any sub-processor that is engaged to process Personal Data by Supplier is subject to data protection obligations that are similar to those applicable to

Supplier under this DPA and shall remain liable for the performance of its sub-processors' obligations.

6.3 SCC shall be fully effective, as applicable.

7 INTERNATIONAL TRANSFERS

Neither party shall transfer the Personal Data outside the EEA or the UK unless it has in place appropriate safeguards in respect of such transfer, as set out in Article 46 of the GDPR and the respective provisions of the DPA 2018 and the accompanying SCCs.

7.1 CONTROLLER TO CONTROLLER

Where to Parties agree that they are both controllers in respect of the Personal Data then, to the extent that a transfer of Personal Data from Customer as Supplier or vice versa is a Restricted Transfer, the Standard Contractual Clauses shall apply between Supplier and the Customer as set out below.

a. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply as follows:

   i. Module One will apply;

   ii. in clause 7, the optional docking clause will apply;

   iii. in clause 11, the optional language will not apply;

   iv. in clause 17, option 1 will apply, and the EU SCCs will be governed by Irish law;

   v. in clause 18(b), disputes shall be resolved before the courts of Ireland;

   vi. Annex I of the EU SCCs shall be deemed completed with the relevant information set out in Annex 1 to this Agreement, and the competent supervisory authority for the purposes of clause 13 to the EU SCCs shall be the supervisory authority in the country in which the main establishment or the single establishment of Supplier is located (the "Main Establishment"). If the Main Establishment is outside the EU, the competent supervisory authority shall be the Irish supervisory authority; and

   vii. Annex II of the EU SCCs shall be deemed completed with the relevant information set out in Annex 2 to this Agreement.

b. Subject to clause 7.1c, in relation to Personal Data that is protected by the UK GDPR, the EU SCCs, completed as set out above in clause 7.1a of this Agreement, shall also apply to transfers of such Personal Data, and the UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("UK Addendum") shall be deemed executed between Supplier and the Customer and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data and in respect of that UK Addendum:

   i. Table 1 shall be deemed completed with the relevant information set out in clause 7.1 and the Annexes to this Agreement;

   ii. Table 2 shall be deemed completed with the relevant information set out in clause 7.1a of this Agreement;

iii. Table 3 shall be deemed completed with the relevant information set out in clause 7.1 and the Annexes to this Agreement; and

iv. Table 4 shall be deemed completed to provide that neither party may terminate the UK Addendum.

c. Notwithstanding clause 7.1b, in relation to Personal Data that is protected by the UK GDPR, to the extent that the Customer is subject to the UK GDPR, in circumstances where the UK Addendum is deemed not to apply, the UK International Data Transfer Agreement issued by the Information Commissioner's Office under s119A(1) of the Data Protection Act 2018 ("IDTA") shall be deemed executed between the Parties in its place and, in respect of that IDTA, Tables 1 – 4 shall be completed on the same basis of the UK Addendum as set out in clause 7.1b and it shall be governed by the law of England and Wales with the primary place for legal claims to be made by the Parties being England and Wales.

7.2 CONTROLLER TO PROCESSOR

To the extent that the transfer of Personal Data from the Controller to the Processor is a Restricted Transfer, the Standard Contractual Clauses shall apply between the Controller and the Processor as set out below.

a. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

i. Module Two will apply;

ii. in clause 7, the optional docking clause will apply;

iii. in clause 9, option 2 will apply, and the time period for prior notice of sub-processor changes shall be 10 calendar days;

iv. in clause 11, the optional language will not apply;

v. in clause 17, option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in clause 18(b), disputes shall be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs shall be deemed completed with the relevant information set out in clause 0 and Annex 1 to this Agreement, and the competent supervisory authority for the purposes of Clause 13 shall be the supervisory authority in the country in which the main establishment or the single establishment of which Supplier is located (the "Main Establishment"). If the Main Establishment is outside the EU, the competent supervisory authority shall be the Irish supervisory authority;

viii. Annex II of the EU SCCs shall be deemed completed with the relevant information set out in Annex 2 to this Agreement;

ix. Annex III of the EU SCCs shall be deemed completed with the relevant information set out in Annex 2 to this Agreement.

b. Subject to clause 7.2c, in relation to Personal Data that is protected by the UK GDPR, the EU SCCs, completed as set out above in clause 7.2a of this Agreement, shall also apply to transfers of such Personal Data, and the UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**") shall be deemed executed between the

Controller and the Processor, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data and in respect of that UK Addendum:

i. Table 1 shall be deemed completed with the relevant information set out in clause 0 and the Annexes to this Agreement;

ii. Table 2 shall be deemed completed with the relevant information set out in clause 7.2a of this Agreement;

iii. Table 3 shall be deemed completed with the relevant information set out in clause 0 and the Annexes to this Agreement; and

iv. Table 4 shall be deemed completed to provide that neither party may terminate the UK Addendum.

c. Notwithstanding clause 7.2b, in relation to Personal Data that is protected by the UK GDPR, to the extent that the Processor is subject to the UK GDPR, in circumstances where the UK Addendum is deemed not to apply, the UK International Data Transfer Agreement issued by the Information Commissioner's Office under s119A(1) of the Data Protection Act 2018 ("**IDTA**") shall be deemed executed between the Parties in its place and, in respect of that IDTA, Tables 1 – 4 shall be completed on the same basis of the UK Addendum as set out in clause 7.2b and it shall be governed by the law of England and Wales with the primary place for legal claims to be made by the Parties being England and Wales.

7.3 PROCESSOR TO CONTROLLER

To the extent that the transfer of Personal Data from Supplier as a Processor to the Customer as a Controller is a Restricted Transfer the Standard Contractual Clauses shall apply between Supplier and the Customer as set out below.

a. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

i. Module Four will apply;

ii. in clause 7, the optional docking clause will apply;

iii. in clause 11, the optional language will not apply;

iv. in clause 17 the EU SCCs will be governed by Irish law;

v. in clause 18 disputes shall be resolved before the courts of Ireland; and

vi. Annex I of the EU SCCs shall be deemed completed with the relevant information set out in clause 7.3a and Annex 1 to this Agreement.

b. Subject to clause 7.3c, in relation to personal data that is protected by the UK GDPR, the EU SCCs, completed as set out above in clause 7.3a of this Part A, shall also apply to transfers of such personal data, and the UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**") shall be deemed executed between Supplier and the Customer, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data and in respect of that UK Addendum:

i. Table 1 shall be deemed completed with the relevant information at clause 7.3 and the Annexes to this Agreement;

ii. Table 2 shall be deemed completed with the relevant information set out in clause 7.3a;

iii. Table 3 shall be deemed completed with the relevant information set out in clause 7.3 and the Annexes to this Agreement; and

iv. Table 4 shall be deemed completed to provide that neither party may terminate the UK Addendum.

c. Notwithstanding clause 7.3b, in relation to Personal Data that is protected by the UK GDPR, to the extent that the Customer is subject to the UK GDPR, in circumstances where the UK Addendum is deemed not to apply, the UK International Data Transfer Agreement issued by the Information Commissioner's Office under s119A(1) of the Data Protection Act 2018 ("**IDTA**") shall be deemed executed between the Parties in its place and, in respect of that IDTA, Tables 1 – 4 shall be completed on the same basis of the UK Addendum as set out in clause 7.3b and it shall be governed by the law of England and Wales with the primary place for legal claims to be made by the Parties being England and Wales.

7.4 AMENDMENTS TO SCCs

Where the EU SCCs and/or the UK SCCs are amended or replaced by the European Commission or Information Commissioner's Office respectively in accordance with the Data Protection Laws ("**Replacement SCCs**"), those Replacement SCCs shall apply and shall be deemed completed on a mutatis mutandis basis as set out in clauses 7.1 to 7.3.

8 DURATION AND TERMINATION

8.1 This DPA shall commence on the date of the last Party to sign this DPA, and it shall remain in force so long as the Customer engages Supplier to process Personal Data on its behalf under the Subscription Agreement, unless terminated earlier in accordance with the terms hereof.

8.2 This DPA may be terminated: (a) automatically upon termination or expiry of the subscription Agreement; (b) by either Party giving 30 days written notice to the other Party; (c) immediately by either Party upon written notice in the event of a material breach of this DPA by the other Party, provided that such breach is not remedied within 30 days of written notice of the breach.

8.3 Upon Termination of this DPA, the Processor shall: (a) cease all processing of Personal Data except to the extent necessary for the performance of any continuing obligations; (b) at the Customer's election, return or securely destroy all Personal Data and delete existing copies (save to the extent storage is required by applicable law); and (c) provide written confirmation to the Customer that these requirements have been fulfilled.

9 LIABILITY

9.1 In the event of a breach of this Agreement, liability shall be assigned in accordance with any terms and conditions specifically agreed between the parties, or in the absence of such agreement, in accordance with the Standard Terms & Conditions of Ocean Technologies Group.

10 MISCELLANEOUS

10.1 This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. No counterpart shall be effective until each Party has executed at least one counterpart.

10.2 Any amendments to this Agreement, as well as any additions or deletions, must be agreed in writing by both the Parties.

10.3 This DPA shall be governed and construed in accordance with the laws of England and Wales. The English Courts will have exclusive jurisdiction to deal with any dispute which has arisen or may arise out of or in connection with this DPA.

ANNEX 1

DETAILS OF PROCESSING

Subject matter, nature and purposes of the processing	In accordance with the Subscription Agreement, Supplier will provide e-learning and competence management systems to the Customer. The systems are used as a basis for training and certification of the seafarer, tests, results etc.
Duration of the processing	For the duration of the Subscription Agreement
Type of Personal Data	Name, contact information, employee number, employment details incl. position/job role and rank
Categories of data subject	Personnel (ship management and crew) of the Customer

LOCATION AND SUB-PROCESSORS

The Personal Data is stored and processed in cloud architecture, based on the Customer's jurisdiction, unless agreed otherwise between the Parties.

When using the services offline on a vessel or mobile device, the necessary data is stored locally on the device providing the offline service.

ANNEX 2

Description of the technical and organisational security measures implemented by the Data Processor

Data Processor will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of the Data Controller's data including but not limited to those set forth in the underlying agreement between the Data Processor and the Data Controller to which these Clauses are attached. In the event that the underlying agreement does not specify technical and organisational security measures, the parties agree that, at a minimum, the following measures shall apply.

Technical and Organisational Security Measures Implemented by the Data Processor

Data Processor agrees and warrants that it has implemented technical and organisational measures appropriate to protect Confidential Information (including Personal Data) against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

The measures Data Processor has taken include, as appropriate, proportionate and without limitation:

1. Implementing and complying with a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of Confidential Information and designed to protect such information from: unauthorised access, destruction, use, modification, or disclosure; unauthorised access to or use that could result in substantial harm or inconvenience to Data Controller or its employees; and any anticipated threats or hazards to the security or integrity of such information;

2. Adopting and implementing reasonable policies and standards related to security.

3. Assigning responsibility for information security management and data protection and to provide to Data Controller contact details of responsible persons of the Data Processor;

4. Devoting adequate personnel resources to information security.

5. Carrying out verification checks on permanent staff that will have access to Confidential Information.

6. Conducting appropriate background checks and requiring employees, vendors and others with access to the Confidential Information to enter into written confidentiality agreements.

7. Conducting training to make employees and others with access to Confidential Information aware of information security risks and to enhance compliance with its policies and standards related to data protection, as well as requiring such personnel to sign an obligation to keep all Confidential Information confidential and secure (data secrecy) during their assignment and thereafter.

8. Preventing unauthorised access to the Confidential Information through the use, as appropriate, of physical and logical (passwords) entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with its policies and standards related to data protection on an ongoing basis. In particular, Data Processor has implemented and complies with, as appropriate and without limitation:

    - Physical access control measures to prevent unauthorised access to data processing systems such as entry controls including the legitimisation of authorised persons (e.g., access ID cards, card readers, desk officers, alarm systems, motion detectors, burglar alarms, video surveillance and exterior security);

    - Denial-of-use control measures to prevent unauthorised use of data protection systems by technical (keyword/password protection) and organisational (user master record) measures concerning user identification and authentication (e.g., automatically enforced password complexity (inter alia special characters, minimum length, regular change of keyword), automatic disabling (e.g., keyword or screensaver password activation) and change requirements, creation of one master user record per user, encoding of data carriers, firewalls);

- Requirements-driven authorization scheme and access rights (including different forms of profiles, roles, transactions and objects), and monitoring and logging of system access to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Confidential Information cannot be read, copied, modified or removed without authorization.

- Data transmission control measures to ensure that Confidential Information cannot be read, copied, modified, or removed without authorisation during electronic transmission, transport or storage on data media, and transfer and receipt records. Data Processor's information security program shall be designed:

  i. To encrypt in storage any data sets in Data Processor's possession that includes sensitive Confidential Information.

  ii. To ensure that any sensitive Confidential Information transmitted electronically (other than by facsimile) to a person outside of Data Processor's IT system or transmitted over a wireless network uses encryption to protect the security of the transmission.

  iii. To use adequate measures for any other Confidential Information (e.g., encryption, encoding/tunnel connection (VPN = Virtual Private Network), electronic signature, logging, transport security).

- Penetration tests conducted on Data Processor's IT systems and application platforms no less frequently than once annually by an independent third-party security firm.

- Data entry control measures to ensure that it is possible to check and establish whether and by whom Confidential Information has been input into data processing systems, modified, or removed by logging and log evaluation systems.

- Subcontractor supervision measures to ensure that, where the Data Processor is permitted to subcontract under the Services Agreement and any part of the Services involves (i) the processing of Confidential Information, (ii) access to systems through which access to Confidential Information may be gained or (iii) the fulfilment of information security functions, the Data Processor shall (a) notify Data Controller of the relevant subcontractor(s) and (b) execute formal agreements with each approved subcontractor that require the subcontractor to implement security controls at least as stringent and comprehensive as those provided in the Services Agreement and this Exhibit.

- Measures to ensure that Confidential Information is protected from accidental destruction or loss including, as appropriate and without limitation, data backup (mirroring of data), retention and secure destruction policies, secure offsite storage of data sufficient for disaster recovery, uninterrupted power supply, and disaster recovery and emergency programs.

- Measures to ensure that data collected for different purposes can be processed separately including, as appropriate and without limitation, physical or adequate logical separation of client data (e.g., "internal client capability"/purpose limitation, separation of functions as production and test).

- The ability to correct, delete or block the Confidential Information processed on behalf of Data Controller only in accordance with the instructions of Data Controller.
- Secure destruction shall include numerous overwriting of hard drives in accordance with recognised industry standards and confidential disposal of data carriers through specialised vendors with prior demagnetisation of storage media. The same applies to test material and discarded material. Records of any deletions or destructions must be presented to Data Controller upon demand.

9. Reporting incidents to Data Controller that threaten the Data Processor's IT systems, including any unauthorised access, disclosure or use of Confidential Information or a compromise of the security, integrity, confidentiality or availability of the Data Processor's IT system or Confidential Information ("Security Incident") within 24 hours of the Security Incident being detected by notifying:

   Data Controller Contact Details:

   Email: compliance.OTG@oneocean.com

10. Taking such other steps as may be appropriate under the circumstances.