DATA PROCESSING AGREEMENT

Latest Update: February 15, 2023

This Data Processing Agreement ("DPA") is incorporated by reference into the Subscription Services Agreement entered into between Veson Nautical LLC, located at 21 Drydock Avenue, Suite 610W, Boston, Massachusetts 02210, USA ("Veson" or "Data Importer"), and Client governing the Client's use of products and services provided by Veson (the "Agreement").

SCOPE AND APPLICATION

This DPA is only valid and legally binding if the Client entity signing it is a party to a Subscription Services Agreement and is a Controller on whose behalf Veson is processing data when providing products or services to Client. This DPA forms part of such Agreement.

When a Client purchases a new subscription or renews a subscription to Products, the then-current DPA will apply. For earlier versions of the DPA, Client may refer to www.veson.com/archive-terms. In the event Veson introduces features or new products, Veson may make updates to the DPA that apply to Client's use of such features or new products.

1. DEFINITIONS.

1.1. **"Agreement"** means a Subscription Services Agreement between Veson and a specific client under which products or services are provided by Veson to that client.

1.2. **"Controller", "data subject", "personal data", "personal data breach," "process", "processing", "processor", "service provider," and "supervisory authority"** have the same meanings as in Data Protection Legislation, even when not capitalized.

1.3. **"CCPA"** means collectively the California Consumer Privacy Act and the California Privacy Rights Act as amended or superseded from time to time

1.4. **"Client"** means the client that is identified on, and is a party to, the Agreement, and any of its affiliates.

1.5. **"Data Exporter"** means the Controller who transfers the Personal Data to a Data Importer.

1.6. **"Data Importer"** means the Processor who agrees to receive Personal Data from the Data Exporter intended for Processing on the Data Exporter's behalf after the transfer in accordance with its instructions and the terms of the Standard Contractual Clauses.

1.7. **"Data Protection Legislation"** means all data protection laws and regulations, including laws and regulations of the European Union, the European Economic Area (EEA) and their member states, Switzerland and the United Kingdom, applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time, including without limitation GDPR, UK GDPR, and CCPA.

1.8. **"GDPR"** means the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.9. **"Personal Data"** means personal data that is submitted to the Products by Client and processed by Veson for the purposes of providing the Products to Client. The types of Personal Data and the specific uses of the Personal Data are detailed in Exhibit A attached hereto.

1.10. **"Products"** means the Veson services and products ordered or subscribed to by Client in an Agreement.

1.11. **"Standard Contractual Clauses" or "Clauses"** means the Standard Contractual Clauses based on the Commission Decision 2021/914,Standard Contractual Clauses (processors) document attached hereto as Exhibit B or any such clauses amending, replacing or superseding those by a European Commission decision or by a legally binding decision made by any other authorized body.

1.12. **"Sub-processor"** means other processors used by Veson to process Client Personal Data, as described in Article 28 of the GDPR.

2. DATA PROCESSING.

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data for the provision of the Products, Client is the Controller and Veson is the Processor or service provider.

2.2. Processing of Personal Data. Veson may process Personal Data on behalf of Client as part the provision of the Products to Client. Veson will process Personal Data as follows:

2.2.1. Veson will comply with applicable Data Protection Legislation. However, Veson is not responsible for compliance with any laws or regulations applicable to Client or Client's industry that are not generally applicable to the provision of Veson's Products;

2.2.2. Veson will implement appropriate technical, administrative, physical and organizational measures to adequately safeguard and protect the security and confidentiality of Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access;

2.2.3. Veson will process the Personal Data only in accordance with any documented Client instructions received by Veson with respect to the processing of such Personal Data and in a manner necessary for the provision of the Products by Veson which will, for the avoidance of doubt, include processing in accordance with this DPA and the Agreement. If Veson is processing Personal Data within the scope of the CCPA, Veson makes the following additional commitments to Client. Veson will process Personal Data on behalf of Client and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Veson sell any such data;

2.2.4. Veson will ensure that persons authorized to process Personal Data on behalf of Veson are committed to confidentiality obligations by law, contract, or policy;

2.2.5. Veson will assist Client by maintaining appropriate technical and organizational measures to help Client fulfill its obligation to respond to requests for exercising a data subject's rights with respect to Personal Data under Chapter III of the GDPR;

2.2.6. Veson will promptly inform Client if in its opinion compliance with any Client instruction would infringe Data Protection Legislation;

2.2.7. Veson will assist Client in complying with its obligations with respect to Personal Data pursuant to Articles 32 to 36 of the GDPR;

2.2.8. Veson will, at Client's option, and subject to the terms of this DPA (i) delete or return all Personal Data to Client after the end of the provision of the Products, and (ii) delete existing copies of Personal Data unless applicable law requires retention of the Personal Data;

2.2.9. Veson will make available to Client all information necessary to demonstrate compliance with its obligations as a Processor as specified in Article 28 of the GDPR, and allow for and

contribute to audits, including inspections, conducted by Client or another auditor mandated by Client, consistent with Section 8 of this DPA;

2.2.10. Veson will maintain a record of all categories of processing activities carried out on behalf of Client in accordance with Article 30(2) of the GDPR; and

2.2.11. Veson and its representatives will cooperate, on request, with the relevant supervisory authority in providing the Products.

2.3. Client Responsibilities. Client will, in its use of the Products, process Personal Data in accordance with the requirements of applicable Data Protection Legislation. For the avoidance of doubt, Client's instructions to Veson for the processing of Personal Data will comply with applicable Data Protection Legislation. Client will have sole responsibility for the accuracy, quality, and legality of Personal Data and for ensuring that the Personal Data was lawfully acquired by Client (including any authorizations or consents if required). Client shall ensure that Client is entitled to transfer the relevant Personal Data to Veson so that Veson and its Sub-processors may lawfully use, process and transfer the Personal Data in accordance with this DPA and the Agreement on Client's behalf as a Processor.

2.4. Processing Instructions. Client instructs Veson to process Personal Data for the following purposes: (a) processing necessary for the provision of the Products and in accordance with the Agreement; (b) processing initiated by Client's end users in their use of the Products; and (c) processing to comply with the other reasonable written instructions provided by Client to Veson (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement, as required to comply with applicable Data Protection Legislation or other applicable laws, or as otherwise mutually agreed by the parties in writing. For the purposes of Clause 8.1(a) of the Standard Contractual Clauses, the foregoing is deemed an instruction by the Data Exporter to process Personal Data.

The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Veson to Client upon Client's written request.

3. RIGHTS OF DATA SUBJECTS.

If Veson receives a request from a data subject to exercise one or more rights under the GDPR or CCPA in connection with a Product for which Veson is a data processor or service provider, Veson shall, to the extent legally permitted, promptly notify Client of such request and Client shall be responsible for responding to any such request. Taking into account the nature of the processing, Veson shall comply with reasonable requests by Client to assist with Client's response to and fulfillment of such a data subject request. To the extent legally permitted, Client shall be responsible for any reasonable costs that Veson may incur in providing such assistance.

4. DATA TRANSFER REQUIREMENTS.

The Standard Contractual Clauses will apply to all processing of Personal Data by Veson where the Personal Data is transferred from the EEA or the United Kingdom to outside the EEA or United Kingdom, from a Data Exporter acting as Controller to a Data Importer acting as Processor, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Legislation), and (b) not covered by a suitable

framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition to the obligations under this section, the parties agree to the following additional safeguards:

1. All Personal Data on the Products shall be encrypted both in transit and at rest using state of the art encryption technology that is robust against the performance of cryptanalysis;
2. Veson represents that as of the date of the Agreement, it has not received any national security data production orders, such as pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") or U.S. Presidential Policy Directive 28;
3. Vendor will, to the extent permitted by applicable law, resist any request under FISA 702 for surveillance whereby a targeted account is not uniquely identified;
4. Veson will use available legal mechanisms to challenge any demands for data access through the national security process that Veson receives;
5. Veson will, to the extent permitted by law, notify Client of any binding legal demand for Personal Data that Veson has received, including national security orders and directives, which shall encompass any process issued under FISA 702.
6. If, for any reason, the transfer of Personal Data under the Standard Contractual Clauses or other lawful data transfer mechanism, approved by the relevant data protection authority, ceases to be lawful or the additional safeguards are no longer effective, Client may, at its discretion, require Veson to: (a) cease transfers of the Personal Data to, or access to such Personal Data from, the relevant jurisdictions; or (b) promptly cooperate with Client to facilitate the use of an alternative lawful data transfer mechanism and any additional safeguards that will permit Client to continue to benefit from the Products in compliance with applicable Data Protection Legislation. If Client and Veson are unable to implement such alternate data transfer mechanism promptly, then Client may, at its option, upon written notice to Veson terminate the Agreement, suspend the transfer, or reduce the scope of Products to exclude Personal Data, without liability or penalty of any kind.

To the extent that there are any new or further measures that are legally required by relevant Data Protection Legislation to be implemented by Veson to ensure ongoing compliance with the Standard Contractual Clauses, Veson shall implement such measures within a reasonable time.

5. SUB-PROCESSORS.

5.1. Sub-processing. The parties agree that Veson may use Sub-processors to fulfill its obligations under this DPA or the Agreement or to provide certain services on its behalf to support Veson in the delivery of the Product to the Client. Client consents to the use of Sub-processors as described in this Section. Such Sub-processors may be Veson affiliate companies. The above authorizations will constitute Client's prior written consent to the subcontracting by Veson of the processing of Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

5.2. Sub-processor Agreements. Veson is responsible for its Sub-processors' compliance with Veson's obligations in this DPA. When engaging any Sub-processor, Veson will ensure via a written contract that the Sub-processor may access and use Personal Data only to deliver the services

for which it has been retained and is prohibited from using Personal Data for any other purpose. Veson will ensure that Sub-processors are bound by written agreements that require them to provide at least the level of data protection required of Veson by this DPA, including the limitations on use, transfer, or disclosure of Personal Data. Veson agrees to oversee the Sub-processors to ensure that these contractual obligations are met.

5.3. Sub-processor List. Information regarding Veson's current Sub-processors, including their location and services provided (the "Sub-processor List"), can be found in Exhibit C and at the following link: https://veson.com/data-protection-terms/. This Sub-processor list may be updated by Veson from time to time in accordance with subsection 5.4 below.

5.4. Changes to Sub-processor List. From time to time, Veson may engage new Sub-processors. Veson shall inform Client of any intended changes concerning the addition or replacement of Sub-processors, thereby giving Client the opportunity to object to such changes. Client may not unreasonably object to any changes, and for this purpose an objection will be considered reasonable only if Client can demonstrate that the change materially increases the risk to Client of a Personal Data security breach or GDPR breach and if Client provides a detailed description of the reason for the objection and measures that would address the objection. Notice of any changes to the list of Sub-processors shall be deemed given by Veson posting an updated version of Exhibit C on the website or in any other manner reasonably determined by Veson. If Client does not object in writing to any such changes within 30 days, the changes are deemed accepted. If Client does object in writing during this period, then Veson shall address the objection by (i) excluding Client's Personal Data from the processing by the Sub-processor to the extent Veson determines is necessary to address Client's objection, (ii) taking the measures stated by Client in the objection notice to address Client's objection, (iii) taking such other measures as Veson reasonably determines address the objection, and/or (iv) modifying the Products to avoid use of the Sub-processor with respect to Client's Personal Data. If Veson is unable to undertake any of the foregoing on terms that Veson believes are commercially reasonable, then either Party may require that the Parties enter into good faith discussions regarding termination or modification of the Agreement without penalty to either Party.

6. SECURITY MEASURES.

Veson implements the physical, technical, and organizational security measures set forth in Appendix 2 of this DPA with respect to the Personal Data ("Security Measures") to ensure a level of security appropriate to the risk in accordance with the standards of Article 32 of the GDPR. Veson is certified under System and Organization Controls (SOC) 2, Type II standards and is audited annually by a third party to ensure its ongoing compliance with these standards. Veson regularly tests, assesses and evaluates the effectiveness of the Security Measures. Veson will not materially decrease the overall security of the Products during the term of the Agreement. Veson will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance.

7. SECURITY INCIDENT NOTIFICATION.

The parties agree that Veson's obligations under Clause 8.6(c) of the Standard Contractual Clauses and under Article 28(3)(f) of the GDPR with respect to Client's compliance with Articles 33 and 34 of the GDPR will be carried out in accordance with this Section 7. If Veson becomes aware of any

unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Client's Personal Data, including any "personal data breach" as defined in the GDPR ("Security Incident"), Veson will notify Client without undue delay after becoming aware of and confirming the Security Incident. Veson will take reasonable steps to: (a) identify the cause of the Security Incident; and (b) remediate the cause of such Security Incident to the extent such remediation is within Veson's reasonable control. Veson will also reasonably cooperate with Client with respect to any investigations and provide any information reasonably requested by Client in relation to the Security Incident.

Veson's notification of or response to a Security Incident under this section is not an acknowledgement by Veson of any fault or liability with respect to the Security Incident.

8. AUDITS.

The parties agree that the audits described in Clauses 8.9(c) and (d) of the Standard Contractual Clauses and Article 28(h) of the GDPR (the "Audit") will be carried out in accordance with the following conditions:

8.1. An Audit of its data processing facilities may be performed no more than once per year at Client's expense during Veson's normal business hours, unless (i) otherwise agreed to in writing by Client and Veson, (ii) required by a regulator or under applicable Data Protection Legislation, or (iii) there is a Security Incident;

8.2. Client will provide Veson with at least thirty (30) days' prior written notice of an Audit, which may be conducted by Client or an independent auditor appointed by Client ("Auditor");

8.3. The Auditor will conduct Audits subject to any appropriate and reasonable confidentiality restrictions requested by Veson;

8.4. The scope of an Audit will be limited to Veson systems, processes and documentation relevant to the processing and protection of Personal Data;

8.5. Prior to the start of an Audit, the parties will agree to reasonable scope, time, duration, place and conditions for the Audit, and a reasonable reimbursement rate payable by Client to Veson for Veson's Audit expenses;

8.6. Client will promptly notify and provide Veson with full details regarding any perceived non-compliance or security concerns discovered during the course of an Audit.

9. GENERAL.

9.1. Term and Termination. This DPA will remain in force until (i) it is replaced or repealed by mutual agreement of Client and Veson, or (ii) the Agreement is terminated or expires.

9.2. Changes in Data Protection Legislation. The terms of this DPA are subject to amendment by Veson at any time as required as a result of any change in, or decision of a competent authority under, applicable Data Protection Regulation, to allow processing of Personal Data to be done (or continue to be done) without breach of such Data Protection Legislation or decision. Client's continued use of the Product after such changes are implemented constitutes Client's acceptance of the changes, except as otherwise stated below.

9.3. Conflicts. In case of conflict or inconsistency between this DPA, the Agreement, and the Standard Contractual Clauses, the following order of precedence shall govern to the extent of the conflict or inconsistency: (i) the Standard Contractual Clauses; (ii) this DPA; and (iii) the Agreement.

Exhibit A

Subject Matter of Processing	The subject matter of Processing are the Products pursuant to the Agreement.
Duration of Processing	For the term of the Agreement, until all final invoices are paid, and thereafter for record retention purposes to the extent permitted by the Data Protection Laws
Categories of Data Subjects	Data subjects subject to processing pursuant to or related to the Agreement are: • Client employees, agents and representatives • Users of the Products • Any other individual whose name or personal information is input by Client into any hosted software service included in the Products or provided to Veson
Nature and Purpose of Processing	Nature: Processing as part of the Products ordered by Client in the Agreement. Purpose: The purpose of the processing of Personal Data by Veson is to provide the Products pursuant to the Agreement.
Types of Personal Data	The categories of Personal Data that may be processed pursuant to or related to the Agreement include: • Name • Job title • Business address • Phone number • Email address • Passwords and user names • Client's customer contact information, including names, titles, business contact information of client's customers • UserIDs • Cookies associated with usage information such as URLs, pages accessed, browser type • Device ID • IP address • Device geolocation

Exhibit B

Standard Contractual Clauses (Processors)

Execution of the Subscription Services Agreement by Client includes execution of this Exhibit B, which is countersigned by Veson Nautical LLC.

The data exporting organisation identified as "Client" in the DPA

(the "data exporter")

- And –

Veson Nautical LLC

21 Drydock Avenue, Suite 610W , Boston, MA 02210 USA

(the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex I.A.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – [Intentionally left blank.]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days' in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other

confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality)

to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested

until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

This Annex forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.

Data exporter/Controller

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of such legal entity established within the European Economic Area (EEA), the United Kingdom and Switzerland that have ordered or subscribed to Products through one or more Agreement(s).

Data importer/Processor

The data importer is (please specify briefly activities relevant to the transfer):

Veson Nautical LLC is a provider of cloud-based software solutions which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees and other authorized users of the Data Exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Personal Data provided by the Data Exporter to facilitate the Data Importer's provision of Products to the Data Exporter, as specified in Exhibit A to the DPA.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The data exporter does not anticipate transferring special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing of the personal data by Data Importer shall be to enable (1) the performance of the Products; (2) to provide any technical and customer support as requested by data exporter, and; (3) to fulfil all other obligations under the Agreement.

Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13

The Data Protection Commission

21 FITZWILLIAM SQUARE SOUTH
DUBLIN 2
D02 RD28
IRELAND

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer:

Veson shall maintain an information security program (including the adoption and enforcement of internal policies and procedures): (a) designed to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Veson products and services, and (c) minimise security risks, including through risk assessment and regular testing. Veson shall designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1. **Be Based on an Industry Standard**. The information security program will be based upon a recognized industry standard such as SOC2 Type 2.

1.2. **Employee Security**. Veson shall ensure that all employees have executed an appropriate written confidentiality agreement and that they complete security and privacy education annually appropriate to their role.

1.3. **Application Development**. Veson shall develop the Veson products and services using a defined system development lifecycle process that includes reviews related to security by design and privacy by design.

1.4. **Subcontractor Security**. Veson shall ensure that all subcontractors have written agreements in place with terms related to confidentiality and security appropriate for the function that they serve and the obligations in the Agreement. Veson shall review all subcontractors who have access to Client Data for their ability to comply with Veson's information security program, giving consideration to the nature of the data and processing that the subcontractor provides. Only subcontractors that are assessed as being able to provide an appropriate level of security will be utilized. Such reviews should be reperformed should there be a change in the nature of the data or processing, if any information is available that raises a concern that the subcontractor is not able to comply, or at least on a 24 month basis.

1.5. **Application Security**. Veson shall maintain measures for the Veson products and services to logically separate and prevent Client Personal Data from being exposed to or accessed by unauthorized persons. Client Personal Data in transit and rest will be encrypted. All encryption algorithms and key lengths will be based upon reasonable commercially available methods.

1.6. **Restricted Access**. Veson shall limit access to Client Personal Data to only those employees and subcontractors who require such access to perform the activities required to provide the Veson products and services to Client.

1.7. **Network Security**. The Veson products and services will be electronically accessible to clients, employees and subcontractors as necessary to provide the Veson products and services. Veson shall maintain access controls and policies to manage what access is allowed to the Veson

products and services from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Veson shall maintain corrective action and incident response plans to respond to potential security threats.

1.8. **Vulnerability Assessments**. Veson shall conduct vulnerability assessments (including penetration testing) of the Veson products and services on a regular basis. Any identified issues shall be remediated in an appropriate timeframe in accordance with Veson policies.

1.9. **Reporting and Advisories.** Veson shall report to Client any actual or reasonably suspected vulnerability, breach, denial, exfiltration, hacking, destruction, or other misuse of customer assets immediately after Veson reasonably believes the any actual or reasonably suspected vulnerability, breach, denial, exfiltration, hacking, destruction, or other misuse of customer assets has occurred. Within 5 business days thereafter, Veson shall provide to Client a written confirmation of the any actual or reasonably suspected vulnerability, breach, denial, exfiltration, hacking, destruction, or other misuse of customer assets and any advisories received by Veson relating to third party products in the Subscription.

1.10. **Disaster Recovery Plan**. Veson shall maintain a disaster recovery plan related to the Hosted Service and a business interruption recovery plan related to its business. Veson shall review such plans at least annually. The plans will be designed to meet the Recovery Point Objective and Recovery Time Objectives specified in the plans.

1.11. **Incident Response Plan**. Veson shall maintain an incident response plan related to the identification of Security Incidents, limiting the impact of Security Incidents, investigation of Security Incidents, maintaining evidence of Security Incidents, and informing required parties of Security Incidents. Such plan shall be reviewed at least annually.

2. **Continued Evaluation**. Veson shall conduct periodic reviews of the security of the Veson products and services and adequacy of its information security program as measured against industry security standards and its policies and procedures. Veson shall continually evaluate the security of the Veson products and services and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Exhibit C/ANNEX III to Standard Contractual Clauses

LIST OF SUB-PROCESSORS

Latest Update: November 1, 2023

Name	***Purpose***	***Location (By Country)***
Absorb Software Inc.	Cloud Platform for both Veson University – Enterprise Services and Veson University Rapid Implementation under Professional Services	Ireland
Amazon Web Services	Cloud Infrastructure	Ireland; Singapore; United Arab Emirates; United States
Atlassian/Jira – US	Veson development services and support	United States
Auth0	User authentication	United States; European Union
Gainsight	Customer Success Management	United States
Google	Cloud infrastructure	Belgium; European Union
Mavenlink	Project management for client professional services projects	United States
Microsoft Office 365	Document storage	United States
MongoDB	Storage Infrastructure	Ireland
Professional services subcontractors	Provision of professional services to clients, if applicable	Client and Sub-processor location(s)
Rackspace	Product message handlers and listeners for Veslink vessel reporting information	Australia; Germany; Hong Kong; United Kingdom; United States
Snowflake Inc.	Cloud database management	Ireland; Singapore; United Arab Emirates; United States
Veson Nautical Subsidiaries	Veson Nautical subsidiary	Greece; Japan; Norway; Poland; Singapore; United Kingdom; United States