

## TRITAN INTERNATIONAL PARTICIPATING PROVIDER TERMS & CONDITIONS

These Provider Terms and Conditions (the "**Provider Terms**") are a part of and incorporated by reference into the Tritan International, Ltd. ("**TRITAN**") Provider Agreement (the "**Provider Agreement**"). By entering into the Provider Agreement, Tritan International, Ltd., a Cyprus limited liability company, Reg. # HE425946 ("**TRITAN**") and the identified Provider, agree to be bound by these Provider Terms.

### 1. **The Services**

Provider will provide the Services identified in the Provider Agreement, according to the fees set forth in the Provider Agreement, to Eligible Persons located in the Jurisdiction. The Services are more fully described in Schedule A to the Provider Agreement.

### 2. **Definitions**

Any capitalized terms not defined in this Section 2 or elsewhere in these Provider Terms shall have the meaning set forth in the Provider Agreement.

2.1 "**Application**" means the forms submitted by a potential Provider requesting that TRITAN approve said Provider as a Provider, including, but not limited to evidence of meeting the Credentialing Criteria.

2.2 "**Eligible Persons**" means the natural persons entitled to receive Services on behalf of a Customer. Eligible Persons may include but are not limited to seafarers, crewmembers, employees, passengers and patients.

2.3 "**Services**" means the medical and/or health care services performed by Provider or Provider Professionals pursuant to the Provider Agreement, which are more fully described in Schedule A to the Provider Agreement.

2.4 "**Provider**" means a health care provider who has entered into an agreement with TRITAN to perform one or more of the Services for a Customer.

2.5 "**Participating Customer**" means a party to an agreement with TRITAN under which TRITAN provides, among other things, access to Services for Eligible Persons, provided by Provider. Customers may include but are not limited to; vessel owners and operators.

2.6 "**Customer Agreement**" means an agreement between Customer and TRITAN pursuant to which a Customer agrees to be responsible for payments to Provider for Services provided to Customer's Eligible Persons.

2.7 "**Fee Schedule**" means the list of maximum fee amounts for the Services as set forth in Schedule A to the Provider Agreement.

2.8 "**Credentialing Criteria**" means the criteria set forth on Schedule B to these Provider Terms established by TRITAN for the initial credentialing of Providers when Applications are submitted. The Credentialing Criteria may be amended from time to time by TRITAN in its sole discretion. Providers must provide evidence of meeting the Credentialing Criteria at least once every three years after the initial Application.

2.9 "**Confidential Information**" means information of TRITAN in any form or medium (whether oral written, electronic, or other form) that TRITAN considers confidential or proprietary, including information consisting of or relating to TRITAN's technology, trade secrets, know-how, business operations, plans, strategies, Customers, pricing and other information with respect to which TRITAN has contractual or other confidentiality obligations. Confidential Information shall include, but not be limited to, the presence of the Provider Agreement, these Provider Terms and any related Schedules, lists of Customers and lists of Providers and any information related thereto, information relating to earnings, volume of business, methods, systems, practices or plans of TRITAN, its Participating Customers, and all similar information of any kind or nature whatsoever which is known only to persons having a fiduciary or confidential relationship with TRITAN, its Participating Customers. All medical records, including, but not limited to case histories, case records, x-ray films, personal or regular files relating to patients treated by Provider or Provider Professionals pursuant to this Provider Agreement, including Eligible Persons consulted, interviewed, treated or cared for by Provider or Provider Professionals pursuant to this Provider Agreement.

2.10 "**Data Privacy Laws**" means the data protection and privacy laws in the Jurisdiction, including, but not limited to, the EU General Data Protection Regulation, the US Health Insurance Portability and Accountability Act, the data privacy or breach notification laws imposed by any state or country applicable to this Agreement, all as the same may be amended from time to time.

2.11 "**Jurisdiction**" means the countries, territories, regions or other geographic areas in which Provider has facilities and will be providing Services pursuant to the Provider Agreement.

2.12 "**Medically Appropriate**" means services or supplies which, under the provisions of this Agreement, are determined to be: (i) in accordance with requirements of the employment medical exams as set forth in Section 4.4; (ii) appropriate and necessary for the symptoms, diagnosis or treatment of the injury or disease; (iii) provided for the diagnosis or direct care and treatment of the injury or disease; (iv) in accordance with commonly recognized and accepted medical standards; (v) not primarily for the convenience of the Eligible Person or of any Provider Professional providing Services to the Eligible Person; (vi) an appropriate supply or level of care; (vii) within the scope of the medical specialty education and training of a provider; and (viii) provided in a setting consistent with the required level of care.

2.13 "**Provider Professionals**" means any properly credentialed medical professionals providing Services as an employee or agent of Provider.

### 3. **Obligations of TRITAN**

3.1 **Third-Party Administration.** TRITAN shall act as a third-party administrator facilitating the procurement of Services and the administration of payment to Provider for those Services on behalf of Customers. TRITAN is neither providing nor receiving the Services covered by this Agreement.

3.2 **Composition of Providers and Customer Group.** TRITAN has the sole and exclusive discretion to add or remove providers from the group of Providers, and to determine the Customers entitled to access the Services of the Providers in accordance with the terms of this Agreement.

3.3 **Customer List.** Within thirty (30) days of the Effective Date of the Provider Agreement, TRITAN shall make available to Provider a list of all Customers ("**Participant List**") who are entitled to receive the Fee Schedule for Services as set forth in this Agreement. TRITAN may add or remove Customers from the Participant List by providing Provider an updated copy of the Participant List which will become effective fifteen (15) days after Provider's receipt of the Participant List.

### 4. **Obligations of Provider**

4.1 **Medical Appropriateness.** Provider, directly or through its Provider Professionals, shall provide Medically Appropriate Services to Eligible Persons, located in the Jurisdiction, from any Customer on the Participant List. All Services performed by Provider or its Provider Professionals pursuant to this Agreement shall be invoiced in accordance with the terms of Section 6 of these Provider Terms.

4.2 **Credentials and Qualifications.** Provider is and, at all times during this Agreement, shall be in compliance with the Credentialing Criteria set forth in Schedule B to these Provider Terms. Provider acknowledges and agrees that all information it provides to TRITAN regarding the Credentialing Criteria is and will be true and correct and will not misstate or fail to state any material fact regarding Provider's or the Provider's Professionals' compliance with the Credentialing Criteria.

4.3 **Medical Standards.** Provider, and any Provider Professionals, shall perform the Services pursuant to the requirements of any applicable licensure, certifications, accreditation requirements and/or standards of the Jurisdiction; and treat each Eligible Person in all respects no less favorably than Provider or Provider Professionals treat all other patients.

4.4 **PEME/REME Standards.** All pre-employment or re-employment medical exams ("PEME/REME"), including but not limited to seafarer medical exams, shall be conducted in accordance with the all requirements and medical standards set forth by TRITAN, the Customer, the ILO Maritime Labour Convention (MLC 2006) Guidelines and the Jurisdiction. When an Eligible person meets all criteria, including medical standards for the PEME/REME, Provider shall issue a medical certificate specifying its validity for a period of two (2) years from the date the medical exam was performed.

4.5 **Disciplinary or Malpractice Notices.** Provider shall within ten (10) days of occurrence, notify TRITAN and provide TRITAN with all information regarding:

- (a) any disciplinary action taken against any Provider Professional related to the Provider Professional's performance of Services; or
- (b) any disciplinary action threatened or taken against Provider related to Provider's or Provider Professionals' performance of Services under this Agreement; or
- (c) any malpractice claims asserted against Provider or Provider Professionals related to performance of the Services; or
- (d) any judgements awarded against or settlements agreed to by Provider arising out of, resulting from, or related to performance of the Services.

4.6 Verification of Eligible Persons. Provider shall be responsible for requesting and confirming eligibility of each Eligible Person according to customary verification procedures. Provider will be notified of eligibility through those same customary verification procedures. If Provider performs any Services before receiving verification of such eligibility, and it is later determined the individual was not an Eligible Person, neither TRITAN nor its Customer will have responsibility for such Services, and Provider agrees that it will seek payment for such Services directly from the individual who received Services.

## 5. Confidentiality & Data Privacy

5.1 Confidentiality. Provider, and its officers, directors, employees, agents, successors and assigns, including, but not limited to Provider Professionals ("**Provider Representatives**") shall:

- (a) not access or use Confidential Information other than as necessary to exercise Provider's rights or perform Provider's obligations under and in accordance with this Provider Agreement;
- (b) except as may be permitted by this Provider Agreement, not disclose or permit access to Confidential Information other than to Provider's Representatives who
- (i) need to know such Confidential Information for the purpose of Provider exercising its rights under the Provider Agreement;
- (ii) have been informed of the confidential nature of the Confidential Information and Provider's obligations under this Section; and
- (iii) are bound by confidentiality and restricted use obligations with Provider that are at least as protective of the Confidential Information as the terms set forth in this Provider Agreement; and
- (c) safeguard the Confidential Information from unauthorized use, access, or disclosure using at least the degree of care it uses to protect its most sensitive information and in no event less than a reasonable degree of care; and
- (d) promptly notify TRITAN of any unauthorized use or disclosure of Confidential Information and cooperate with TRITAN to prevent further unauthorized use or disclosure; and
- (e) ensure Provider's Representatives' compliance with, and be responsible and liable for any of Provider Representatives' non-compliance with, the terms of this Section.

5.2 Data Privacy. The Parties agree that TRITAN administers personal and protected data of Eligible Persons in accordance with its obligations as appointed by the Customer. The Provider agrees all personal and protected data shall be considered Confidential Information and subject to the protections of Section 5.1, and in addition Provider and Provider Representatives

- (a) will comply with all applicable Data Privacy Laws;
- (b) have adequate security measures in place in order to protect the personal and protected information that they have in their possession; and
- (c) notify TRITAN promptly on becoming aware of a loss or breach of personal or protected information.

5.3 Consents. Provider warrants that it shall obtain, in accordance with applicable law, the consent of each Eligible Person necessary for the collection, storage, processing, use and sharing of their personal information and protected health information to the extent required in order to provide the Services.

5.4 Business Associate and Data Protection Agreements. To the extent Provider is a covered entity pursuant to the US Health Insurance Portability & Accountability Act ("HIPAA") or either Provider or TRITAN are business associates with respect to a particular Customer, TRITAN and Provider will enter into, and this Provider Agreement will be subject to, the terms of a mutually agreed upon HIPAA Business Associate Agreement ("**BAA**") which shall be attached hereto and incorporated herein. To the extent the Provider is subject to the EU General Data Protection Regulation ("**GDPR**") or either Provider or TRITAN are contractually required to comply with GDPR with respect to a particular Customer, TRITAN and Provider will enter into, and this Provider Agreement will be subject to, the terms of the Data Processing Agreement ("**DPA**") that shall be attached hereto and incorporated herein. Should the parties need to implement both a BAA and a DPA, TRITAN and Provider shall enter into a single agreement to address the requirements of the BAA and the DPA.

5.5 Further Assurances Data Protection Requirements. Each party recognizes the possibility that one or more jurisdictions could implement new data protection laws or regulations applicable to the Services ("**New Data Requirements**"). Each party agrees that in the event of New Data Requirements, they will work together to modify this Provider Agreement or to execute and deliver any and all such documents and instruments, and take all such further actions necessary to bring this Provider Agreement into compliance with the New Data Requirements.

5.6 Legal Restrictions. Neither party hereto shall be in default for failure to supply to the other party information which such party, in good faith, believes cannot be supplied due to prevailing law or regulatory requirement, or for supplying information which such party, in good faith, believes is required to be supplied due to prevailing law or regulatory requirements.

## 6. Fees & Payments

6.1 Fees and Invoices. Provider shall invoice TRITAN, on behalf of Customer, in accordance with the Services and Fee Schedule set forth in Schedule A of the Provider Agreement for all Services provided to Eligible Persons in accordance with the terms of this Agreement. Provider shall use its best efforts to submit invoices within thirty (30) days after providing the Services and to consolidate the submission of all invoices on a monthly basis. TRITAN and/or Customer shall have the right to deny payment for any invoices submitted more than six (6) months after providing the Services.

6.2 Adjustments to Fee Schedule. TRITAN will consider a revision to the Fee Schedule if requested by Provider, but no more frequently than once each calendar year. No single revision to the Fee Schedule shall result in increases to the maximum reimbursable amount of more than 3%.

6.3 Processing and Payment. TRITAN on behalf of Customer, shall review all invoices, apply the applicable Fee Schedule pursuant to the Provider Agreement, if necessary, to determine the amount due to the Provider. TRITAN will then process the payment in accordance with the Customer Agreement for all invoices for Services to the Customer. TRITAN will use its best efforts to ensure that Customer authorizes and remits payment for all invoices within forty-five (45) days of receiving the invoices.

6.4 Responsibility for Payment. Customer shall be solely and exclusively responsible and liable for fulfilling the obligation of payment of the invoices to the Provider. TRITAN shall be responsible only for administering the process of payments as a third party on behalf of the Customer to the Provider. TRITAN shall not be responsible for any action or decision by Customer to delay, reduce or reject payment to Provider and any disputes or grievances shall be addressed and resolved directly with Customer. Notwithstanding the foregoing, TRITAN will make all reasonable efforts to collect and deliver all Customer payments to Provider.

6.5 No Additional Payments. Provider acknowledges and agrees that it will accept the invoice amounts, as adjusted by TRITAN for compliance with the Fee Schedule, as payment in full for all Services provided to Eligible Persons, and Provider agrees not to assess any additional charges to such Eligible Persons for the Services provided pursuant to this Agreement, including, but not limited to any fees, charges, taxes or fees of any other nature.

## 7. Additional Services

Any subcontractor or additional provider with which Provider has an arrangement to provide Services on behalf of Provider (each a "**Subcontractor**") shall abide by all of the terms and conditions of this Agreement, including, without limitation, accepting the Fees as payment in full for Services. Provider is responsible for ensuring all such subcontractors or additional providers are aware of and agree to be bound by the terms of this Agreement.

## 8. Trademarks and Copyrights

Each party acknowledges each other party's sole and exclusive ownership of its respective trade names, commercial symbols, trademarks and service marks, whether presently existing or later established (collectively "**Marks**"). No party shall use the other party's Marks in advertising or promotional materials or otherwise without the owner's prior written consent; PROVIDED, HOWEVER, that TRITAN may, but shall not be required to, list Provider in the directory of Providers or in other materials identifying the status of Provider as a Provider, including, but not limited to TRITAN using Provider's logo, which will be provided to TRITAN promptly following the Effective Date, for such purposes.

## 9. Term and Termination

9.1 Term. The initial term of this Agreement ("**Initial Term**") shall commence on the Effective Date of this Agreement and shall continue for one (1) year. This Agreement shall be automatically renewed for additional periods of one (1) year (each a "**Renewal Term**") unless either party shall give written notice of non-renewal or termination to the other party at least three (3) months prior to the expiration of the then current term.

### 9.2 Termination of Agreement.

- (a) Either party may terminate this Agreement for cause upon the material breach of this Agreement by the other party that is not remedied within thirty (30) days after the breaching party's receipt of notice of the breach from the non-breaching party.

- (b) TRITAN shall have the option to terminate this Agreement at any time, immediately upon written notice to Provider, if TRITAN reasonably concludes that:
  - (i) Provider or Provider Representatives have engaged in fraud; or
  - (ii) the continuation of this Agreement may result in imminent danger to Eligible Persons or the public health, safety or welfare; or
  - (iii) Provider has breached this Agreement and the breach is incapable of cure; or
  - (iv) the laws or regulations applicable to this Provider Agreement have changed such that the continued performance under this Agreement would be in violation of such laws or regulations and the parties are unable to agree on an amendment to the Provider Agreement that would bring it under the requirements of the new law or regulation.

**9.3** Effect of Termination. Upon the termination of this Agreement by either party for any reason, whether for cause or not for cause, whether voluntary or involuntary, all rights and obligations hereunder shall cease, except that

- (a) Provider will immediately issue invoices for any unbilled Services performed prior to the date of termination;
- (b) TRITAN will continue to facilitate the payment of all outstanding invoices including those issued pursuant to Section 9.3(a);
- (c) Provider shall return to TRITAN all Confidential Information, including, but not limited to personally identifiable or protected health information, that Provider received or collected as a result of performance under this Agreement;
- (d) Upon confirmation of TRITAN's receipt of all information returned pursuant to Section 9.3 (c), Provider will destroy all electronic copies it has of such Confidential Information, personal information or protected health information, provided that Provider may retain a copy of such information to the extent Provider is required by law to maintain such information as part of a patient's medical records.
- (e) All rights and obligations which by their nature are intended to survive expiration or termination of the Provider Agreement shall survive such expiration or termination, including, but not limited to Sections 2 (Definitions), 5 (Confidentiality), 9.3 (Effect on Termination), 10 (Warranty), 11 (Limitation of Liability), 12 (Indemnification), and 13.1 (Provider-Patient Relationship), 13.3 (Independent Contractors), 13.4 (Notices), 13.7 (Severability), 13.8 (Conflict of Laws), 13.10 (No Inferences), 13.12 (Counterparts), 13.13 (Electronic Signatures), 13.14 (Anti-Bribery) and 13.15 (Entire Agreement).

**10.** Warranty Provider warrants to TRITAN that

10.1 Provider has not and shall not enter into any conflicting relationships that would affect Provider's ability to perform under this Provider Agreement, including, but not limited to, acting in the best medical interests of the Eligible Persons.

10.2 Provider has, and shall ensure that Provider Professionals have, the required skill, experience, and qualifications to perform the Services and will perform the Services in a professional and workmanlike manner in accordance with the best industry standards for similar Services, using their best efforts to promptly render Medically Appropriate Services to all validated Eligible Persons.

10.3 Provider will, and will ensure that Provider Professionals will, perform the Services in compliance with the ethical rules of the medical profession as well as all applicable federal, state and local laws and regulations, including, by maintaining all licenses, permits and registrations required to perform the Services.

**11.** Limitation of Liability.

11.1 WAIVER. IN NO EVENT WILL TRITAN BE LIABLE UNDER OR IN CONNECTION WITH THIS PROVIDER AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES; (b) INCREASED COSTS, DIMINUTION IN VALUE OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (c) LOSS OF GOODWILL OR REPUTATION; (d) USE, INABILITY TO USE, LOSS, INTERRUPTION, DELAY OR RECOVERY OF ANY DATA, OR BREACH OF DATA OR SYSTEM SECURITY; OR (e) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER TRITAN WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE.

11.2 **MONETARY CAP.** EXCEPT FOR THE OBLIGATION TO ADMINISTER THE PROCESSING OF PAYMENTS ON BEHALF OF CUSTOMER TO PROVIDER FOR SERVICES PROPERLY PERFORMED, IN NO EVENT WILL TRITAN'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE EXCEED THE AMOUNT OF FEES TRITAN RECEIVES OVER A PERIOD OF SIX (6) MONTHS AS A RESULT OF PERFORMANCE UNDER THIS AGREEMENT.

11.3 **General Limitations.** Without limiting the foregoing provisions, TRITAN shall not have any liability whatsoever for any loss, liability, claim, expense, damage or costs suffered or caused by Provider, Provider Professionals, Provider Representatives and/or the Eligible Persons resulting from the Services or from any advice, care, treatment or any acts or omissions, that Provider, Provider Professionals, or Subcontractors or any third party that are used or referred by the Provider to provide the Services including, without limitation, providers of medical services, medical doctors, medical evacuation companies or transportation providers.

**12. Indemnity.**

Provider agrees to indemnify, defend and hold harmless TRITAN, its owners, officers, employees, Customers, representatives and agents ("**TRITAN Indemnitees**") from and against all claims and suits by third parties for damages, injuries to persons (including death), property damages, losses, and expenses including court costs and reasonable attorney's fees, arising out of, or resulting from, Provider's rendering of Services or performance under this Agreement, including all such causes of action based upon common, constitutional, or statutory law, or based in whole or in part, upon allegations of negligent or intentional acts on the part of the Provider, Provider Professionals, Provider Representatives, or Subcontractors. Provider may not settle any claim subject to indemnification without the prior written consent of TRITAN, unless such settlement completely and forever releases all TRITAN Indemnitees from all liability with respect to such claim.

**13. Miscellaneous Provisions**

13.1 **Provider-Patient Relationship.** Nothing contained in this Agreement shall interfere with or in any way alter any provider-patient relationship and Provider or Provider Professionals shall have the sole responsibility for the care and treatment of Eligible Persons under Provider's care. Nothing contained herein shall grant TRITAN the right to govern the level of care of a patient. Obligations performed by TRITAN shall only effect fees paid to Provider for Services and shall not limit the performance of the Services by Provider or Provider Professionals or effect Provider's or Provider Professionals' professional judgment.

13.2 **Non-Exclusivity.** Nothing in this Agreement shall be intended or construed to prevent either party from entering into substantially similar agreements with other entities similar to the other party.

13.3 **Independent Contractors.** Each party, its officers, agents and employees are at all times independent contractors to the other party. Nothing in this Agreement shall be construed to make or render either party or any of its officers, agents, or employees an agent, servant, or employee of, or joint venture of or with, the other.

13.4 **Notices.** All notices or communications permitted or required under this Provider Agreement ("**Notice**") must be in writing. Notice to TRITAN should be addressed to: Tritan International, Ltd.; Triton Quarters, Suite 2A, No. 22 Parallel Road to New Port, 3045 Limassol, Cyprus. Notices to Client should be addressed to the name and address set forth in the Order. Either party may update its address by written notice in accordance with this provision. All Notices must be delivered by personal delivery, internationally recognized overnight courier (with all fees pre-paid), or email (with confirmation of transmission and a copy sent via first class postage on the same day). Notices are effective upon confirmation of receipt or refusal of delivery by the receiving party.

13.5 **Amendment.** Any amendment to or modification of this Agreement must be in writing and signed by an authorized representative of each party. Any waiver of any provisions of this Agreement or rights thereunder must be in writing and signed by the party so waiving. Except as otherwise set forth in this Provider Agreement, (a) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Provider Agreement will operate or be construed as a waiver thereof and (b) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

13.6 **Assignment.** Provider may not assign or transfer any of its rights or delegate any of its obligations hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, without the prior written consent of TRITAN, any purported assignment, transfer, or delegation in violation of this Section is null and void. No assignment, transfer, or delegation by Provider will relieve Provider of any of its obligations hereunder. Subject to the foregoing

restrictions, this Provider Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

13.7 Severability. If any provision of this Provider Agreement is invalid, illegal, or unenforceable in any jurisdiction, the parties shall negotiate in good faith to modify this Provider Agreement so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible. If the parties are unable to reach a mutually acceptable modification, such provisions shall be deemed severed from this Provider Agreement and the remainder of the Provider Agreement shall remain in full force and effect as if such invalid provision had been omitted.

13.8 Conflict of Laws. This Provider Agreement shall be governed by and construed in accordance with the laws of the country of Cyprus, without giving effect to any choice or conflict of law provisions or rule. This Provider Agreement shall not be governed by the United Nations Convention on Contracts for the international sale of Goods, the application of which is expressly prohibited.

13.9 Force Majeure. In no event shall either party be liable to the other, or be deemed to have breached this Agreement, for any failure or delay in performing its obligations under this Agreement, (except for any obligations to make payments), if and to the extent such failure or delay is caused by any circumstances beyond such party's reasonable control, including but not limited to acts of God, flood, fire, earthquake, hurricane, explosion, war, terrorism, invasion, riot or other civil unrest, strikes (other than by a party's employees), industrial disturbances, or passage of law or any action taken by a governmental or public authority that preclude the activities contemplated by this Provider Agreement. The party so affected will give the other party prompt and detailed notice of the Force Majeure, including the probable duration thereof, and will promptly notify the other party when the Force Majeure has ended. During the Force Majeure, the affected party will use commercially reasonable efforts to avoid, reduce or eliminate the Force Majeure's prevention, restriction or delay of the performance of its obligations under this Provider Agreement. If a Force Majeure event exceeds thirty (30) calendar days, the other party may terminate this Provider Agreement by providing written notice to the party asserting Force Majeure.

13.10 No Inferences. The Parties acknowledge that this Agreement has been fully negotiated by the parties and their respective legal counsel. In the event of ambiguities in this Agreement, no inferences shall be drawn against either party on the basis of authorship of this Provider Agreement.

13.11 Equitable Relief. Provider acknowledges and agrees that a breach or threatened breach by Provider of any of its obligations under the Confidentiality Provision of these Provider Terms, would cause TRITAN irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, TRITAN will be entitled to equitable relief, without the need to post a bond or other security, and without the need to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

13.12 Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement.

13.13 Electronic Signatures. The parties agree that any electronic versions of signatures, whether through electronic forms or the transmission of PDF versions of signatures by email or facsimile shall have the same force and effect as original signatures.

13.14 Anti-Bribery. The parties represent, warrant and undertake to each other on a continuous basis that they shall comply with all applicable anti-bribery, anti-money laundering, anti-slavery and human trafficking laws, rules, and regulations of the UK, the European Union and any other applicable jurisdictions. These laws include, without limitation, the currently effective or successor versions of the UK Bribery Act 2010; the UK Anti-Terrorism, Crime and Security Act 2001; the UK Proceeds of Crime Act 2002; The UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and the UK Modern Slavery Act 2015. In addition, the Parties represent, warrant and undertake that they shall each respectively take no action which would subject the other party to fines or penalties under such laws, regulations, rules or requirements. Without prejudice to the above provisions, neither party shall, directly or indirectly, pay salaries, commissions or fees, or make payments or rebates to employees or officers of the other party; or favor employees or officers of the other party or their designees with gifts or entertainment of unreasonable cost or value or services or goods sold at less than full market value; or enter into business arrangements with employees or officers of the other party unless such employees or officers are acting as representatives of the other party.

13.15 Entire Agreement. This Agreement, including, but not limited to these Provider Terms and the schedules hereto, constitute the sole and entire agreement of the parties with respect to the subject hereof and supersedes all prior and contemporaneous understandings and agreements, both written and oral, with respect to such

subject matter. In the event of any inconsistency between this Agreement, these Provider Terms, and the related Schedules, the Agreement shall govern, followed by these Terms and then the schedules.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be duly authorized, executed and entered into as of the Effective Date set forth below.

**Acknowledged and Accepted:**

**Provider**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Tritan International, Ltd.**

DocuSigned by:

By:  \_\_\_\_\_

57BCF98A8A16499...

Name: Andrew Carricarte

Title: President, CEO



**SCHEDULE B  
CREDENTIALING CRITERIA PROFESSIONAL CREDENTIALS**

**1. Valid License.** Provider is either (i) a person with an unrestricted license or other authorization to practice in the location of jurisdiction; or (ii) a partnership, professional service corporation or other entity, all of the partners, shareholders, members and provider employees of which have an unrestricted license or other necessary authorization to practice in the location of jurisdiction. A copy of Provider's current valid license(s) shall be provided to TRITAN with the Application, and thereafter upon TRITAN's request.

**2. Admitting Privileges.** Provider, where applicable, has active full and unrestricted clinical and admitting privileges in Provider's specialty at a minimum of one (1) Provider facility ("Participating Facility") or if Provider is a member of a non-admitting specialty, maintain full and unrestricted privileges appropriate to such specialty at a Participating Facility. Provider shall maintain each Participating Facility and other hospital, medical or professional staff appointment and all clinical and admitting privileges granted in connection therewith that Provider possessed as of the Effective Date of Provider's Provider Agreement. A letter from each Participating Facility stating the Provider has such clinical privileges shall be provided with the Application and thereafter upon TRITAN's request.

**3. Prescribing License.** Provider shall, if permitted under Provider's license, have and maintain unrestricted prescribing privileges. A copy of Provider's current certification, if applicable, shall be provided to TRITAN with the Application and thereafter upon TRITAN's request.

**4. Disciplinary Actions.** Neither Provider nor Provider Professionals, where applicable, have and shall not in the future (i) have any hospital appointment or privileges reduced, limited, suspended or terminated or been placed on probation by any hospital at which Provider or Provider Professional has had a medical or professional staff appointment or privileges; (ii) been restricted from receiving payments from any payors or any other third party payment programs; (iii) been subject to disciplinary action by any medical society, specialty society, board of medical examiners or relevant agency; or (iv) been subject to sanctions of any kind whatsoever by any person or entity for improper prescribing procedures or actions.

**5. Criminal Actions.** Neither Provider nor Provider Professionals have been convicted of a felony or any serious crime, or are under any criminal investigation or proceedings.

**6. Health.** Provider or Provider Professionals, as appropriate, are in good general health and shall report to TRITAN any physical or mental problems that may affect Provider's or Provider Professionals' ability to practice Provider's or Provider Professionals' profession. Provider shall certify to TRITAN that neither Provider nor Provider Professionals have any communicable and/or chronic infectious disease that may be potential danger to patients.

**7. Drugs & Alcohol.** Provider shall certify to TRITAN that neither Provider nor Provider Professionals have a history of and are not presently abusing drugs or alcohol.

**8. Insurance.** Provider shall obtain and maintain, at the sole cost and expense of Provider, policies of professional liability insurance for a minimum amount of one million dollars (\$1,000,000.00) individual/three million dollars (\$3,000,000.00) aggregate. Provider shall furnish to TRITAN a copy of the certificate of coverage with the aforementioned amounts.

**9. Board Certification.** Physician Providers (i) shall be board certified in a specialty recognized by the Jurisdiction or other appropriate boards applicable to the specialty of Provider in the sole discretion of TRITAN. A copy of Provider's board certification or appropriate training shall accompany the Application and thereafter be provided upon TRITAN's request. Expiration or re-certification dates shall be indicated where applicable.

**10. Diagnostic Equipment.** Provider shall: (i) properly maintain, calibrate and license all diagnostic equipment in Provider's offices; (ii) maintain a formal quality control program for all office diagnostic equipment; and (iii) allow diagnostic testing and procedures to be performed and interpreted only by persons with appropriate training and/or certification.

**11. Independent Verification.** TRITAN reserves the right to require independent verification of any and all of the Credentialing Criteria and to perform site visits to the locations of Provider at any time.

**<<HIPAA BUSINESS ASSOCIATE AGREEMENT>>**

**THIS BUSINESS ASSOCIATE AGREEMENT** ("BA Agreement") is effective as of the \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_ (the "Effective Date") by and between the person or entity listed as the covered entity on the signature page hereto ("Covered Entity") and Tritan Software International, Ltd. ("Business Associate")

**WHEREAS**, Covered Entity has determined that it is a covered entity under HIPAA or has components covered by HIPAA;

**WHEREAS**, Covered Entity has retained Business Associate to provide certain goods or services to Covered Entity (collectively, the "Services") and in doing so Business Associate creates, receives, maintains, or transmits PHI that is subject to protection under HIPAA; and

**WHEREAS**, under HIPAA, Business Associate is classified as the business associate of Covered Entity.

**NOW, THEREFORE**, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

**I. Definitions.** The terms used, but otherwise not defined, in this BA Agreement shall have the same meaning as those terms in HIPAA and/or the Master Agreement.

A. "Master Agreement" shall mean that certain Master Software License and Services Agreement, by and between the Business Associate and the Covered Entity pursuant to which Business Associate provides certain goods and/or services to Covered Entity and creates, receives, maintains, or transmits PHI.

B. "Breach" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

C. "Designated Record Set" shall have the meaning set forth in 45 CFR § 164.501, including, without limitation, a group of records maintained by or for Covered Entity that consist of: (i) the medical records and billing records about individuals maintained by or for Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) records used, in whole or in part, by or for Covered Entity to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for Covered Entity.

D. "HIPAA" shall mean: (i) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164, and any subsequent amendments or modifications thereto, and (ii) the HITECH Act, and regulations promulgated thereunder, and any subsequent amendments or modifications thereto.

E. "HITECH Act" shall mean the provisions applicable to business associates under the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

F. "PHI" shall mean Protected Health Information which Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity in connection with the performance of Services by Business Associate for Covered Entity pursuant to the Master Agreement.

G. "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, as may be amended, modified or superseded, from time to time.

H. "Protected Health Information" shall have the meaning set forth in 45 CFR § 160.103, including, without limitation, any information, whether oral, electronic or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

I. "Required by Law" shall have the meaning set forth in 45 CFR § 164.103, including, without limitation, a mandate contained in law that compels Covered Entity or Business Associate to make a use or disclosure of Protected Health Information and that is enforceable in a court of law.

J. "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

K. "Security Incident" shall have the meaning set forth in 45 CFR § 164.304, including without limitation, the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

L. "Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, as may be amended, modified or superseded from time to time.

M. "Unsecured PHI" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, Protected Health Information not secured through the use of encryption, destruction or other technologies and methodologies identified by the Secretary to render such information unusable, unreadable, or indecipherable to unauthorized persons.

## II. Obligations of Business Associate.

A. Permitted Uses. Business Associate is permitted to use PHI in order to provide the Services pursuant to the Master Agreement; provided, however, that Business Associate shall not use PHI in any manner that would constitute a violation of HIPAA if so used by Covered Entity. Business Associate may use PHI: (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) as Required by Law.

B. Permitted Disclosures. Business Associate is permitted to disclose PHI in order to provide the Services pursuant to the Master Agreement; provided, however, that Business Associate shall not disclose PHI in any manner that would constitute a violation of HIPAA if so disclosed by Covered Entity. Business Associate may disclose PHI: (i) for the proper management and administration of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; (ii) to carry out the legal responsibilities of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; or (iii) as Required by Law. To the extent that Business Associate discloses PHI to a third party pursuant to Section 2(b)(i) or (ii) above under Reasonable Assurances, Business Associate must obtain in writing, prior to making any such disclosure: (x) reasonable assurance from the third party that such PHI will be held in a confidential manner; (y) reasonable assurance from the third party that such PHI will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to such third party; and (z) an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of such PHI, to the extent the third party has obtained knowledge of such breach (collectively, "Reasonable Assurances"). Except as Required by Law, Business Associate shall not disclose PHI to a health plan for payment or healthcare operations if the individual subject to the PHI has requested such restriction, the individual (or designee) pays out of pocket in full for the health care item or service to which the PHI relates, and the restriction has been made known to Business Associate in accordance with Section 3(b) of this BA Agreement.

C. De-identification. Business Associate may de-identify PHI in accordance with 45 CFR § 164.514.

D. Appropriate Safeguards. Business Associate shall comply with the applicable provisions of the Security Rules and shall implement appropriate administrative, technical, physical, and security safeguards in compliance with HIPAA that reasonably and appropriately safeguard and protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. As required by HIPAA, Business Associate shall maintain policies, procedures and documentation that address these safeguards and the requirements of HIPAA and which are appropriate to the size and complexity of Business Associate's operations and the nature and scope of its services.

E. Business Associate's Agents and/or Subcontractors. To the extent Business Associate uses one or more subcontractors or agents to provide Services to Covered Entity, and such subcontractors or agents create, receive, maintain, or transmit PHI, Business Associate shall require in accordance with 45 CFR § 164.308(b) and 164.502(e) that each subcontractor or agent agree to be bound by substantially the same restrictions as imposed by the terms of this BA Agreement and HIPAA on Business Associate. Following the discovery of non-compliance by a subcontractor or agent of any of its obligations with respect to PHI, Business Associate shall report such non-compliance to Covered Entity.

F. Access to PHI. Within ten (10) days of receipt of a request, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, available to Covered Entity for inspection and/or copying to enable Covered Entity to fulfill its obligations under 45 CFR § 164.524. If a request for access to PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity. Business Associate shall provide access to a copy of electronic PHI maintained by Business Associate in a Designated Record Set to the Covered Entity in accordance with the provisions of this Section and HIPAA.

G. Amendment of PHI. Within ten (10) days of receipt of a request, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, available to Covered Entity for amendment to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. Business Associate shall amend PHI maintained by Business Associate in a Designated Record Set, in Business Associate's possession or control, as directed by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. If a request for amendment of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity.

H. Accounting of PHI Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Within ten (10) days of receipt of a request by Covered Entity, Business Associate shall make available to Covered Entity the information required to provide an accounting of such disclosures. Any accounting information shall include the information described in 45 CFR § 164.528(b), including, without limitation: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the written request for disclosure. If a request for an accounting of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than ten (10) days after receipt of the request, forward the request to Covered Entity.

I. Governmental Access to Records. Business Associate shall make PHI and its facilities, internal practices, books, records, accounts, and other information relating to the use and disclosure of PHI available to the Secretary in a time and manner designated by the Secretary and shall cooperate with the Secretary concerning any investigation designed to determine Covered Entity's or Business Associate's compliance with HIPAA.

J. Minimum Necessary Use and Disclosure Requirement. In accordance with 45 CFR § 164.502(b), Business Associate shall only request, use and disclose the minimum amount of PHI necessary to reasonably accomplish the purpose of the request, use or disclosure. Further, Business Associate will restrict access to PHI to those employees, contractors, or agents of Business Associate who are actively and directly participating in providing Services to Covered Entity and who need to know such PHI in order to fulfill such responsibilities.

K. Retention of PHI. Business Associate shall retain all PHI throughout the term of the Master Agreement and shall continue to maintain the information required under Section 2(h) of this BA Agreement for a period of six (6) years from its creation.

L. Notification Obligations; Mitigation. During the term of this BA Agreement, Business Associate shall notify Covered Entity within five (5) days (or such shorter time period as required by applicable State law) after the discovery of any use and/or disclosure of PHI not permitted by this BA Agreement, a Breach of Unsecured PHI, or any material Security Incident and shall provide Covered Entity with information regarding the improper use and/or disclosure, Breach or Security Incident as required by law. Business Associate shall take corrective action to mitigate and cure, if possible, any harmful effect that is known to Business Associate of an improper use and/or disclosure of PHI, Breach, or Security Incident. Business Associate shall cooperate with Covered Entity regarding any Breach notification to third parties, and shall reimburse Covered Entity for any reasonable notification costs incurred by Covered Entity in complying with the applicable requirements of HIPAA resulting from a Breach of Unsecured PHI by Business Associate. Business Associate shall be deemed to discover a Breach of Unsecured PHI as of the first day on which such Breach is known, or should have been known, by Business Associate.

M. Additional Obligations. Business Associate shall comply with the requirements of HIPAA, which are applicable to Business Associate as a business associate of the Covered Entity, including all regulations which are issued to implement such requirements, as may be amended, modified or superseded from time to time. To the extent Business Associate carries out one or more of Covered Entity's obligation(s) under 45 CFR Part 164, Subpart E, in the performance of such obligations, Business Associate shall comply with the requirements of 45 CFR Part 164, Subpart E, that apply to Covered Entity to the same extent as required by Covered Entity. Business Associate shall comply will all State laws that affect the privacy or security of PHI received from the Covered Entity.

N. Compliance with Standard Transactions. If Business Associate conducts, in whole or in part, Standard Transactions (as such term is defined in the Standards for Electronic Transactions Rule at 45 CFR Parts 160 and 162, as may be amended, modified or superseded, from time to time) for or on behalf of Covered Entity, Business Associate will comply, and will require any of its subcontractors or agents involved with such Standard Transactions on behalf of Covered Entity to comply, with each applicable

requirement of 45 CFR Parts 160 and 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked "not used" in a Standard Transaction or are not in the Standard Transactions' implementation specification; or (iv) changes the meaning or intent of the Standard Transactions' implementation specifications.

**III. Obligations of Covered Entity.**

A. **Notice of Privacy Practices.** Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

B. **Restrictions on Use or Disclosure.** Covered Entity shall only disclose PHI to Business Associate or to others, pursuant to this BA Agreement, in a manner and to an extent permitted by HIPAA. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individuals to use and/or disclose PHI, to the extent such changes or revocations may affect Business Associate's permitted or required uses and/or disclosures of PHI. Further, Covered Entity shall notify Business Associate of any restriction to the use and/or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's permitted or required uses and/or disclosures of PHI.

**IV. Term and Termination.**

A. **Term.** This BA Agreement shall commence on the Effective Date and will remain effective for the entire term of the Master Agreement, unless earlier terminated in accordance with the terms herein.

B. **For Cause Termination Due to Material Breach.** Either party may terminate this BA Agreement by notice in writing to the other party, if the other party materially breaches this BA Agreement in any manner and such material breach continues for a period of thirty (30) days after written notice is given to the breaching party by the other party specifying the nature of the breach and requesting that it be cured. If termination of this BA Agreement is not feasible, the non-breaching party shall report the breach to the Secretary if required by HIPAA.

C. **Effect of Termination.** Upon termination of this BA Agreement, Business Associate shall return or destroy all PHI (regardless of form or medium), including all copies thereof and any data compilations derived from PHI and allowing identification of any individual who is the subject of the PHI. The obligation to return or destroy all PHI shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. If the return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon notification that return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this BA Agreement to such information and limit further uses or disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for as long as Business Associate maintains such PHI. If Business Associate elects to destroy the PHI, Business Associate shall notify Covered Entity in writing that such PHI has been destroyed.

V. **Construction.** This BA Agreement shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this BA Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA.

VI. **Captions.** The captions contained in this BA Agreement are included only for convenience of reference and do not define, limit, explain or modify this BA Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this BA Agreement.

VII. **Notice.** All notices and other communications required or permitted pursuant to this BA Agreement shall be in writing, addressed to the party at the address set forth at the end of this BA Agreement, or to such other address as any party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be sent by: (i) registered or certified mail, return receipt requested, postage pre-paid; (ii) overnight mail by a reputable carrier; (iii) facsimile with a copy sent by First Class Mail, postage pre-paid; or (iv) hand delivery. All notices shall be effective as of the date of delivery if by hand delivery or overnight mail, two (2) days following the date of facsimile, or if by certified mail on the date of receipt, whichever is applicable.

VIII. **Assignment.** This BA Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred by either party without the prior written consent of the other party and any assignment or transfer without proper consent shall be null and void.

IX. **Governing Law.** This BA Agreement shall be governed by, and interpreted in accordance with HIPAA and the internal laws of the State in which the Business Associate has its principal office, without giving effect to any conflict of laws provisions.

X. **Binding Effect; Modification.** This BA Agreement shall be binding upon, and shall enure to the benefit of, the parties hereto and their respective permitted successors and assigns. This BA Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event any provision of this BA Agreement shall conflict with the requirements of HIPAA, this BA Agreement shall automatically be deemed amended as necessary to conform to such legal requirements at all times.

XI. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

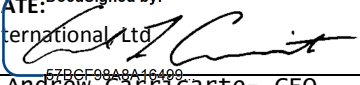
XII. **Severability.** In the event that any provision or part of this BA Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this BA Agreement, with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

XIII. **No Third-Party Beneficiaries.** Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person or entity other than Covered Entity, Business Associate and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

XIV. **Counterparts.** This BA Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which together shall constitute but one BA Agreement.

XV. **Entire Agreement.** This BA Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written agreements, negotiations, commitments, and understandings.

**IN WITNESS WHEREOF,** Covered Entity and Business Associate have each caused this BA Agreement to be executed in their respective names by their duly authorized representatives as of the Effective Date.

**BUSINESS ASSOCIATE:** DocuSigned by:  
Tritan Software International Ltd  
Signature:   
Print Name/Title Andrew Carricarte- CEO  
Address: PO Box 13197  
South City DSU  
Cork, IE T12 C825  
Telephone: +353 21 202 8054  
Facsimile: 1 305 890 1806  
Contact Person: Ms. Tamara Devos

**COVERED ENTITY:**  
\_\_\_\_\_  
Signature: \_\_\_\_\_  
Print Name/Title: \_\_\_\_\_  
Address: \_\_\_\_\_  
\_\_\_\_\_  
Telephone: \_\_\_\_\_  
Facsimile: \_\_\_\_\_  
Contact Person: \_\_\_\_\_

## &lt;&lt;STANDARD CONTRACTUAL CLAUSES &gt;&gt;

**1. DEFINITIONS**

For the purposes of the Clauses:

- (a) **personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);
- (b) **the data exporter** means the controller who transfers the personal data;
- (c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) **technical and organizational security measures** mean those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**2. DETAILS OF THE TRANSFER**

The details of the transfer and in particular the special categories of personal data where applicable are specified in [Annex A](#) which forms an integral part of the Clauses.

**3. THIRD-PARTY BENEFICIARY CLAUSE**

The data subject can enforce against the data exporter this [Clause 3](#), [Clause 4\(b\)](#) to [Clause 4\(i\)](#), [Clause 5\(a\)](#) to [Clause 5\(e\)](#) and [Clause 5\(g\)](#) to [Clause 5\(j\)](#), [Clause 6.1](#) and [Clause 6.2](#), [Clause 7](#), [Clause 8.2](#) and [Clause 9](#) to [Clause 12](#) as third-party beneficiary.

The data subject can enforce against the data importer this [Clause](#), [Clause 5\(a\)](#) to [Clause 5\(e\)](#), and [Clause 5\(g\)](#), [Clause 6](#), [Clause 7](#), [Clause 8.2](#) and [Clause 9](#) to [Clause 12](#), in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this [Clause 3.1](#), [Clause 5\(a\)](#) to [Clause 5\(e\)](#), and [Clause 5\(g\)](#), [Clause 6](#), [Clause 7](#), [Clause 8.2](#), and [Clause 9](#) to [Clause 12](#), in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**4. OBLIGATIONS OF THE DATA EXPORTER**



The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in [Annex B](#) to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to [Clause 5\(b\)](#) and [Clause 8.3](#) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of [Annex B](#) and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with [Clause 11](#) by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and
- (j) that it will ensure compliance with [Clause 4\(a\)](#) to [Clause 4\(j\)](#).

## 5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organizational security measures specified in [Annex B](#) before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  - (ii) any accidental or unauthorized access; and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of [Annex B](#) which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with [Clause 11](#); and
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## 6. LIABILITY

**6.1** The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in [Clause 3](#) or in [Clause 11](#) by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

**6.2** If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in [Clause 3](#) or in [Clause 11](#) because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

**6.3** If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in [Clause 3](#) or in [Clause 11](#) because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

## 7. MEDIATION AND JURISDICTION

**7.1** The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

**7.2** The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**8. COOPERATION WITH SUPERVISORY AUTHORITIES**

**8.1** The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

**8.2** The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

**8.3** The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in [Clause 5\(b\)](#).

**9. GOVERNING LAW**

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely .....

**10. VARIATION OF THE CONTRACT**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

**11. SUB-PROCESSING**

**11.1** The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

**11.2** The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in [Clause 3](#) for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of [Clause 6](#) against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

**11.3** The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....

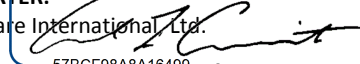
**11.4** The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to [Clause 5\(j\)](#), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES**

**12.1** The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and

the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

**DATA IMPORTER:** DocuSigned by:  
 Tritan Software International Ltd.  
 Signature:   
 Print Name/Title Andrew Carricarte- CEO  
 Address: PO Box 13197  
 South City DSU  
 Cork, IE T12 C825  
 Telephone: +353 21 202 8054  
 Facsimile: +1 305 890 1806  
 Contact Person: Ms. Tamara Devos

**DATA EXPORTER:**  
 \_\_\_\_\_  
 Signature: \_\_\_\_\_  
 Print Name/Title: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 \_\_\_\_\_  
 Telephone: \_\_\_\_\_  
 Facsimile: \_\_\_\_\_  
 Contact Person: \_\_\_\_\_

**ANNEX A  
[TO THE STANDARD CONTRACTUAL CLAUSES]**

This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this [Annex A](#).

**Data exporter**

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

.....  
.....  
.....

**Data importer**

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

*The data importer provides maritime software. In particular, the data importer provides software for individual and organizational health and safety management.*

**Data subjects**

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

*Crew, passengers, contractors, agents and/or employees of maritime vessels operated by the data exporter.*

**Categories of data**

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

*First, middle and last name, Title, Position, Employer, Contact information (company, email, phone, physical business address), ID data, Professional life data, Personal life data, Localization data.*

**Special categories of data (if appropriate)**

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

*Data exporter may submit special categories of data to the data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, religious or philosophical beliefs, or trade-union or insurance membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data regarding health, included but not limited to; diagnoses, medical history, diagnostic results, treatments, prescriptions, etc., or data concerning a natural person's sex life or sexual orientation.*

**Processing operations**

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

*The objective of Processing of Personal Data by data importer is for the performance of the Solutions pursuant to the Agreement.*

**ANNEX B****[TO THE STANDARD CONTRACTUAL CLAUSES]**

This [Annex B](#) forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organizational security measures implemented by the data importer in accordance with [Clause 4\(d\)](#) and [Clause 5\(c\)](#) (or documents/legislation attached):**

1. Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control):

- The data importer has implemented robust security protocols for all data centers, offices and other buildings from which data of the data exporter may be accessed.
- The security protocols include physical protection of buildings against break-ins, as well as access control systems. Security perimeters are established around IT systems hosting personal data. Additionally, the data centers utilized by the data importer maintains an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week and certifications with SSAE16/ISAE 3402 Type II, SOC 2, SOC 3 public audit report, as well as ISO 27001. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly. This also includes formal access procedures for allowing physical access to the data center
- The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only data importer authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved. The electronic card key and biometric access control system is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity. The data importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The IT systems and networks used for the processing of personal data are protected by anti-virus software, anti-malware software, firewalls and intrusion-detection-systems. The data importer also performs an annual Application Vulnerability Assessment Audits via an accredited third party to ensure there are no application vulnerabilities available for exploit.
- The data importer has a Strong Password Policy with a minimum length and character use requirement that ensures that the passwords are non-obvious and complex creating a very difficult scenario that deters human and technical automation discovery. The data importer further requires a scheduled and routine change of passwords to further deter unauthorized access. Employees are also required to take extra measures to guard their credentials carefully and ensure that their accounts are never compromised. These measures include the prohibition of shared access, written passwords or their electronic exchange.
- Devices used to access to data importer's assets must be password protected, in compliance with data importer's Strong Password Policy. The device must lock itself with a password or PIN if it's idle for five minutes. After five failed login attempts, the device should lock

2. Measures to prevent data processing systems from being used without authorization (access control):

- Any access to protected information is restricted to the purposes of performing that individual employee or contractor's responsibilities and only with the prior consent of the data exporter. Activity within the data importer's assets are recorded through a series of audit logs and routinely reviewed for abnormal activity. For all protected information such as medical and personal records, the data importer's employees and contractors are prohibited from access to this information unless required for the purpose of performing their responsibilities in accordance with the parties' agreements.
- Critical access information such as passwords are stored in an encrypted format within secured databases in order to prevent unauthorized access which also includes the restriction of administrator access.

3. Measures 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 personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control):

- The data importer's employees and contractors are provided access to the data importer's assets or software instances solely on an individually required, pre-authorized and restricted basis. They are prohibited from sharing accounts or providing individual accounts to any user without the authorization and approval from the data protection officer (or equivalent). Additionally, the data importer implements a role-based user access management for systems with access rights on a strict need-to-know basis.
- All personal data is encrypted at rest using 256-bit AES encryption. - The data importer diligently monitors the activities of all employees, to include audit records, activity logs and extensive background checks both prior and during employment.

4. Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control):

- All personal data is encrypted during transmission using strong encryption protocols. The Software is required to operate under an SSL Security Certificate utilizing 128-bit encryption. This certificate is authenticated and verified by a publicly accredited certificate authority. The connection uses TLS 1.2 and is encrypted using with SHA for message authentication and RSA as the key exchange mechanism. Secure transmission protocols are used, implementing Perfect Forward Secrecy (PFS). Only SSL encrypted channels are permitted for authorized viewing or accessing of personal data via the Software.
- Only authorized secure channels are permitted by data importer's policies for the transmission of personal or protected data. Insecure transmission channels such as email or FTP are not permitted for the transmission of data unless secondary means have been utilized to appropriately secure the data from unauthorized access. These measures must conform to the strong encryption requirements with appropriate minimum length encryption keys as stipulated by the data importer's policy. Remote access to any hosted data or data on shipboard instances will exclusively take place using secure VPN encryption (AES256).
- The data importer logs transmission activities and transmission rights and regularly reviews these to ensure full compliance.

5. Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control):

- A comprehensive user account control and audit capability is established by the data importer. The data importer monitors the activities of all employees and contractors, to include audit records and activity logs. The recorded logs allow the data importer to verify the activity, time/date and manner in which personal data has been input, modified or removed.

6. Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control):

- The data importer shall ensure that any personnel entrusted with processing the data exporters' data have undertaken to comply with the principle of data secrecy and have been duly instructed on the applicable data protection regulations and the sensibility of data relating to health. The undertaking to secrecy shall

- continue after the termination of the data processing.
- The data importer shall maintain a data protection officer (or equivalent) and implement regular internal controls to ensure that adequate data security measures remain in place at all times and that the data of the data exporter is only processed according to the instructions of the data exporter.
  - The data importer's access to data is restricted to the provision of services pertaining to the agreement between the parties for the support and maintenance of the Software.
  - The data importer monitors the activities of all employees and contractors, utilizing measures such as audit records and activity logs.

7. Measures to ensure that personal data are protected from accidental destruction or loss (availability control):

- Data importer will replicate data over multiple redundant systems to protect against system failure or accidental destruction or loss. Any data hosted by the data importer for the data exporter are to be securely and regularly backed-up. Backups are stored in locations different from the location of the live systems.
- The data centers utilized by the data importer is protected against accidental destruction by fire and flooding and have a redundant climate control unit, a surge protection and an uninterrupted power supply. The infrastructure systems that have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The services are designed to allow the data center to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

8. Measures to ensure that data collected for different purposes can be processed separately:

- The IT systems used to host and/or process the data of the data exporter are physically and logically separated from IT systems used to process data of other clients of the data importer. - Test environments are logically separated from live environments and have a separate set of access credentials with appropriate levels of security.

**Liability**

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.