

5thPort LLC Service Agreement

BY ACCEPTING THIS AGREEMENT, EITHER BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY EXECUTING AN ORDERING DOCUMENT THAT REFERENCES THIS AGREEMENT, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS AND CONDITIONS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

Recitals:

WHEREAS, 5thPort provides access to software-as-a-service offerings to health care industry customers including but not limited to health care providers, pharmaceutical research sponsors, research institutions and Clinical Research Organizations for the purposes of informing patients regarding risks of procedures or participation in any treatment or other health-care related regimen, obtaining the patients' informed consents; and

WHEREAS, Customer desires to access certain software-as-a-service offerings described herein, and 5thPort desires to provide Customer access to such offerings, subject to the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions.

"5thPort" means 5thPort LLC, a Delaware limited liability company with offices located at 131 Continental Drive Suite 409, Newark, Delaware 19713.

"Access Credentials" means any username, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual's identity and authorization to access and use the Services.

"Action" means any claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena, or investigation of any nature, civil, criminal, administrative, regulatory, or other, whether at law, in equity, or otherwise.

"Affiliate" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. The term "control" (including the terms "controlled by" and "under common control with") means

the direct or indirect power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

“Agreement” or **“Service Agreement”** means this 5thPort LLC Service Agreement.

“Customer’s Authorized User(s)” means the Customer’s employees, consultants, contractors, and agents (a) who are authorized by Customer to log in, access and simultaneously use along with other Customer’s Authorized Users the Services under the rights granted to Customer pursuant to this Agreement; and (b) for whom access to the Services has been purchased hereunder. The number of Customer’s Authorized Users shall be equal to the number of User Subscription Fees set forth in the Ordering Document, as the same may be amended from time to time pursuant to the provisions of Section 2.1 of this Agreement.

“Backup Policy” has the meaning set forth in Section 6.

“Business Associate Agreement” or **“BAA”** means the Business Associate Agreement to be executed by the parties, substantially in the form and with such terms and conditions as described in the Health Insurance Portability and Accountability Act of 1996 and the related regulations, as amended from time to time (**“HIPAA”**).

“Caregiver” means a person who provides care for a Patient and/or is authorized to make health care decisions on behalf of a Patient.

“Confidential Information” has the meaning set forth in Section 9.1.

“Customer” means the individual accepting and entering into this Agreement with 5thPort; provided that if such individual is accepting and entering into this Agreement on behalf of a company or other legal entity, then “Customer” means the legal entity on behalf of which such individual is accepting and entering into this Agreement.

“Customer Data” means information, data, and other content, in any form or medium, that is collected, downloaded, or otherwise received, directly or indirectly from Customer or a Customer’s Authorized User by or through the Services, regarding a Patient. For the avoidance of doubt, Customer Data includes Patient Information but does not include Resultant Data (i.e., De-identified).

“Customer Failure” has the meaning set forth in Section 4.2.

“Customer Indemnitee” has the meaning set forth in Section 12.1.

“Customer Systems” means the Customer’s information technology infrastructure, including computers, tablets, iPads, cell phones, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Customer or through the use of third-party services.

“Disclosing Party” has the meaning set forth in Section 9.1.

“Effective Date” has the meaning set forth in the Ordering Document.

“Electronic Consent” means Customer’s provision of an Electronic Informed Consent to Treat Form to a Patient or Caregiver.

“Electronic Health Record” or **“EHR”** is the digital version of a Patient’s paper chart or of the health care services rendered, in the event the intake, treatment, billing and other services are entered directly into an electronic database or system. An EHR contains the medical and treatment history of a Patient from all clinicians involved in a Patient’s care. The EHR may include an audit trail or other evidence of each Engagement. An EHR is capable of being shared with providers across more than one health care organization.

“Electronic Medical Record” or **“EMR”** is the digital version of a Patient’s paper chart in a particular clinician’s office. An EMR contains the medical and treatment history of a Patient in one practice.

“Electronic Protected Health Information” or **“EPHI”** means any Protected Health Information that is produced, saved, transferred, transmitted, maintained, or received by electronic media or in electronic form.

“Encounter” means a specific Engagement Plan that has been assigned to a Patient or Caregiver, whether completed by Patient or Caregiver or not, in order to engage or consent them for a specific treatment episode. If multiple Engagement Plans are assigned for the same treatment episode (i.e., pre-treatment and post-Treatment), each is considered a unique Encounter. If the Patient is undergoing treatments for different diagnoses for which Engagement Plans are assigned to the Patient and/or Caregiver, each Engagement Plan assignment is considered an Encounter. For the elimination of doubt, an Encounter sent to both a Patient and a Caregiver shall be considered as two Encounters.

“Engagement Platform” means the 5thPort Systems and products which allow Customer to design and implement Patient Engagement Plans (each an “Engagement”) using multiple components (i.e., including but not limited to any combination of education videos, comprehension tests, digital documents, acknowledgements, surveys and/or Electronic Consent) to educate Patients and/or Caregivers and obtain informed consent regarding health care treatment and procedures.

“Engagement Plan” means a Customer created engagement protocol in the 5thPort System, including but not limited to any combination of education videos, comprehension tests, digital documents, acknowledgements, surveys and/or Electronic Consent, that is used to engage or consent a Patient and or Caregiver at any time prior to, during, or post medical treatment. An Engagement need not include an Electronic Informed Consent.

“Fees” has the meaning set forth in Section 8.1.

“Force Majeure Event” has the meaning set forth in Section 15.9.

“Harmful Code” means any software, hardware, or other technology, device, or means, including any virus, worm, malware, or other malicious computer code, the purpose or effect of which is to (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (i) computer, software, firmware, hardware, system, or network; or (ii) any application or function of any of the foregoing or the security, integrity, confidentiality, or use of any data Processed thereby; or (b) prevent Customer or any Customer’s Authorized User from accessing or using the Services or 5thPort Systems as intended by this Agreement. Harmful Code does not include any 5thPort Disabling Device.

“Indemnitee” has the meaning set forth in Section 12.3.

“Indemnitor” has the meaning set forth in Section 12.3.

“Initial Term” has the meaning set forth in Section 14.1.

“Intellectual Property Rights” means any and all registered and unregistered rights granted, applied for, or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection, or other intellectual property rights laws, and all similar or equivalent rights or forms of protection, in any part of the world.

“Law” means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction.

“Losses” means any and all losses, damages, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys’ fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“Ordering Document” means the form that sets forth the party names, Fees, Services, Term, Customer’s Authorized Users, User Subscriptions, service managers and such other information as may be included by the parties. The Ordering Document shall be executed by each of the parties (or issued electronically by 5thPort and electronically accepted by Customer) and in the event of any conflict between the terms of this Agreement and the Ordering Document, the terms of the Ordering Document shall control.

“Patient” means a person receiving medical treatment from the Customer or a subject participating in clinical research sponsored by Customer.

“Patient Information” means medical, prescribing or related information, including the Patient’s Electronic Consent, specific to a Patient that has been created in the course of medical treatment or diagnosis.

“Permitted Use” means any use of the Services by a Customer’s Authorized User for the benefit of Customer in the ordinary course of its internal business operations.

“Person” means an individual, corporation, partnership, joint venture, limited liability entity, governmental authority, unincorporated organization, trust, association, or other entity.

“Privacy and Security Policy” has the meaning set forth in Section 7.1.

“Process” means to take any action or perform any operation or set of operations that the Services are capable of taking or performing on any data, information, or other content, including to collect, receive, input, upload, download, record, reproduce, store, organize, compile, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate, or make other derivative works or improvements, process, retrieve, output, consult, use, perform, display, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available, or block, erase, or destroy. **“Processing”** and **“Processed”** have correlative meanings.

“Protected Health Information” or **“PHI”** means individually identifiable health information as defined in HIPAA.

“5thPort Disabling Device” means any software, hardware, or other technology, device, or means (including any back door, time bomb, time out, drop dead device, software routine, or other disabling device) used by 5thPort or its designee to disable Customer’s or any Customer’s Authorized User’s access to or use of the Services automatically with the passage of time or under the positive control of 5thPort or its designee.

“5thPort Equipment” or **“Equipment”** means any 5thPort-owned equipment (including without limitation laptops, tablets, iPads and similar devices) loaned or leased to Customer to facilitate Customer’s use of or access to the Services as described in the Ordering Document.

“5thPort Indemnitee” has the meaning set forth in Section 12.2.

“5thPort Materials” means the Services and 5thPort Systems and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by 5thPort or any Subcontractor in connection with the Services or otherwise comprise or relate to the Services or 5thPort Systems. For the avoidance of doubt, 5thPort Materials include Resultant Data and any information, data, or other content derived from 5thPort’s monitoring of Customer’s access to or use of the Services, but do not include Customer Data.

“5thPort Personnel” means all individuals involved in the performance of Services as employees, agents, or independent contractors of 5thPort or any Subcontractor.

“5thPort Systems” means the information technology infrastructure used by or on behalf of 5thPort in performing the Services, including all computers, tablets, iPads, cell phones, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by 5thPort or through the use of third-party services.

“Receiving Party” has the meaning set forth in Section 9.1.

“Renewal Term” has the meaning set forth in Section 14.2.

“Representatives” means, with respect to a party, that party’s and its Affiliates’ employees, officers, directors, members, managers, consultants, agents, independent contractors, service providers, sublicensees, subcontractors, and legal advisors.

“Resultant Data” means Customer Data related to Patients and Patient Information and Customer’s usage of the Data that has been aggregated and de-identified in accordance with HIPAA or equally stringent standards, and is used by 5thPort for statistical, quality assurance, and clinical outcomes assessments, and to monitor and improve the Services related to Patients, Patient Information, and Customer’s use of the Services.

“Services” means the software-as-a-service offering described in an Ordering Document, including any maintenance, support or implementation services provided by 5thPort as part of its Patient Engagement Platform, including but not limited to modifications, customization, testing, management, hosting, consulting and training services.

“Subcontractor” has the meaning set forth in Section 2.6.

“Term” has the meaning set forth in Section 14.

“Third-Party Materials” means materials and information, in any form or medium, including any open-source or other software, documents, data, content, specifications, products, equipment, or components of or relating to the Services that are not proprietary to 5thPort.

2. Services.

- 2.1 Access and Use. Subject to and conditioned on Customer’s and its Customer’s Authorized Users’ compliance with the terms and conditions of this Agreement, 5thPort hereby grants Customer a non-exclusive, non-transferable (except in compliance with Section 15.8) right to access and use the Services during the Term, solely for use by Customer’s Authorized Users in accordance with the terms and conditions herein and the terms and conditions in the Ordering Document, which is incorporated herein by reference. Such use is limited to Customer’s internal use. 5thPort shall provide to Customer the Access Credentials within a reasonable time following the Effective Date. The total number of Customer’s Authorized Users will not exceed the quantity of User

Subscriptions set forth in the Ordering Document, except as expressly agreed to in the Ordering Document.

2.2 Service and System Control. Except as otherwise expressly provided in this Agreement, as between the parties:

- (a) 5thPort has and will retain sole control over the operation, provision, maintenance, and management of the 5thPort Materials; and
- (b) Customer has and will retain sole control over the operation, maintenance, and management of, and all access to and use of, the Customer Systems, and sole responsibility for all access to and use of the 5thPort Materials by any Person by or through the Customer Systems or any other means controlled by Customer or any Customer's Authorized User, including any: (i) information, instructions, or materials provided by any of them to the Services or 5thPort; (ii) results obtained from any use of the Services or 5thPort Materials; and (iii) conclusions, decisions, or actions based on such use.

2.3 Reservation of Rights. Nothing in this Agreement grants any right, title, or interest in or to (including any license under) any Intellectual Property Rights in or relating to, the Services, 5thPort Materials, or Third-Party Materials, whether expressly, by implication, estoppel, or otherwise. All right, title, and interest in and to the Services, the 5thPort Materials, and the Third-Party Materials are and will remain with 5thPort and the respective rights holders in the Third-Party Materials.

2.4 Service Management. Customer shall, throughout the Term, maintain within its organization one or more service or technology managers to serve as Customer's primary point(s) of contact for day-to-day communications, consultation, technical support, troubleshooting, and decision-making regarding this Agreement. Such service manager or managers shall be responsible for providing first line technical support and troubleshooting in connection with Customer Systems and all day-to-day communications on behalf of Customer under this Agreement, including without limitation relay of all Support Services inquiries to 5thPort and related technical support and troubleshooting emails. Customer's initial service manager(s) are identified in the Ordering Document. If one or more service managers cease to be employed by Customer or Customer otherwise wishes to replace one or more of its service managers, Customer shall promptly name such new service managers by written notice to 5thPort.

2.5 Changes. 5thPort reserves the right, in its sole discretion, to make any changes to the Services and 5thPort Materials that it deems necessary or useful to: (a) maintain or enhance: (i) the quality or delivery of 5thPort's services to its customers; (ii) the competitive strength of or market for 5thPort's services; or (iii) the Services' cost efficiency or performance; or (b) to comply with applicable Law.

2.6 Subcontractors. 5thPort may from time to time in its discretion engage third parties to perform Services (each, a “**Subcontractor**”).

2.7 Suspension or Termination of Services. 5thPort may, directly or indirectly, and by use of a 5thPort Disabling Device or any other lawful means, suspend, terminate, or otherwise deny Customer’s, any Customer’s Authorized User’s, or any other Person’s access to or use of all or any part of the Services or 5thPort Materials, without incurring any resulting obligation or liability, if: (a) 5thPort receives a judicial or other governmental demand or order, subpoena, or law enforcement request that expressly or by reasonable implication requires 5thPort to do so; or (b) 5thPort believes in its good faith that: (i) Customer or any Customer’s Authorized User has failed to comply with any term of this Agreement or Ordering Document, or accessed or used the Services beyond the scope of the rights granted or for a purpose not authorized under this Agreement or in any manner that does not comply with any instruction or requirement communicated by 5thPort; (ii) Customer or any Customer’s Authorized User is, has been, or is likely to be involved in any fraudulent, misleading, or unlawful activities relating to or in connection with any of the Services; (iii) this Agreement expires or is terminated, or (iv) Customer fails to timely make payment in accordance with the provisions of Section 8 of this Agreement. This Section does not limit any of 5thPort’s other rights or remedies, whether at law, in equity, or under this Agreement.

3. Use Restrictions. Customer shall not, and shall not permit any other Person to, access or use the Services or 5thPort Materials except as expressly permitted by this Agreement and, in the case of Third-Party Materials, the applicable third-party license agreement. For purposes of clarity and without limiting the generality of the foregoing, Customer shall not, except as this Agreement expressly permits:

- (a) copy, modify, or create derivative works or improvements of the Services or 5thPort Materials;
- (b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available any Services or 5thPort Materials to any Person, including on or in connection with the internet or any time-sharing, service bureau, software as a service, cloud, or other technology or service;
- (c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Services or 5thPort Materials, in whole or in part;
- (d) bypass or breach any security device or protection used by the Services or 5thPort Materials or access or use the Services or 5thPort Materials other than by a Customer’s Authorized User through the use of his or her own then valid Access Credentials;

- (e) input, upload, transmit, or otherwise provide to or through the Services or 5thPort Systems, any information or materials that are unlawful or injurious, or contain, transmit, or activate any Harmful Code;
- (f) damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, 5thPort Systems, or 5thPort's provision of services to any third party, in whole or in part;
- (g) remove, delete, alter, or obscure any trademarks, EULA, warranties, or disclaimers, or any copyright, trademark, patent, or other intellectual property or proprietary rights notices from any Services or 5thPort Materials, including any copy thereof;
- (h) access or use the Services or 5thPort Materials in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any third party or that violates any applicable Law;
- (i) access or use the Services or 5thPort Materials for purposes of competitive analysis of the Services or 5thPort Materials, the development, provision, or use of a competing software service or product or any other purpose that is to the 5thPort's detriment or commercial disadvantage; or
- (k) otherwise access or use the Services or 5thPort Materials beyond the scope of the access and use rights granted under Section 2.1 or in the Ordering Document.

4. Customer Obligations.

- 4.1 Customer Systems and Cooperation. Customer shall at all times during the Term: (a) set up, maintain, and operate in good repair and in accordance with 5thPort instructions all Customer Systems on or through which the Services are accessed or used; (b) provide 5thPort Personnel with such access to Customer's premises and Customer Systems as is necessary for 5thPort to perform the Services; and (c) provide all cooperation and assistance as 5thPort may reasonably request to enable 5thPort to exercise its rights and perform its obligations under and in connection with this Agreement.
- 4.2 Effect of Customer Failure or Delay. 5thPort is not responsible or liable for any delay or failure of performance caused in whole or in part by Customer's delay in performing, or failure to perform, any of its obligations under this Agreement (each, a "**Customer Failure**").
- 4.3 Corrective Action and Notice. If Customer becomes aware of any actual or threatened activity prohibited by Section 3, Customer shall, and shall cause its Customer's Authorized Users to, immediately: (a) take all reasonable and lawful measures within their respective control that are necessary to stop the activity or threatened activity and to mitigate its effects (including, where applicable, by discontinuing and preventing any unauthorized access to the Services and 5thPort Materials and permanently erasing from

their systems and destroying any data to which any of them have gained unauthorized access); and (b) notify 5thPort of any such actual or threatened activity.

- 4.4 Non-Solicitation. During the Term and for three (3) years after, Customer shall not, and shall not assist any other Person to, directly or indirectly recruit or solicit (other than by general advertisement not directed specifically to any Person or Persons) for employment or engagement as an independent contractor any Person then or within the prior twenty-four (24) months employed or engaged by 5thPort or any Subcontractor involved in any respect with the Services or the performance of this Agreement.

5. Service Support. The Services include 5thPort's standard customer support services ("**Support Services**") in accordance with the 5thPort service support schedule then in effect, a current copy of which is available at **Exhibit A**. 5thPort may amend the service support schedule from time to time in its sole discretion.

6. Availability of Services. This Agreement does not relieve Customer's obligations to maintain Customer Data, including Patient Information such as but not limited to the Electronic Consent, in accordance with applicable laws, regulations, government contracts, and other professional standards. Notwithstanding Customer's obligations in this regard, the 5thPort Systems are programmed to, and 5thPort shall, make Customer Data available during the Term.

7. Security.

7.1 5thPort Systems and Security Obligations. 5thPort will employ security measures in accordance with Law, applicable industry practice, and 5thPort's data privacy and security policy in effect and as amended from time to time.

7.2 Data Breach Procedures. Each party maintains a data breach plan in accordance with Law and applicable industry standard and shall implement the procedures required under such data breach plan on the occurrence of a "Data Breach" (as defined in such plan). Each party shall provide prompt notice to the other party of any Data Breach or other breach in security in such party's Systems, whether internal or external, which could affect the security of any information or Systems of the other party. Customer shall notify 5thPort in writing upon the termination of employment of any Customer's Authorized User. The foregoing notices shall be provided in accordance with Section 15.4. In addition, a copy of any notice required under this Section shall be simultaneously forwarded to the parties at the following email addresses:

5thPort: Subject Line: Legal Notice, legal@5thPort.com

Customer: Per Customer address on the Ordering Document

7.3 HIPAA Compliance. Customer acknowledges that it is a Covered Entity as defined in HIPAA, and Customer agrees to comply with all applicable HIPAA requirements in using and accessing PHI and EPHI through the 5thPort Systems. Customer further

acknowledges that 5thPort shall act as a Business Associate of Customer, as defined by the HIPAA privacy regulations, 45 C.F.R. §160.103, in carrying out 5thPort's responsibilities under this Agreement. Customer and 5thPort shall execute a Business Associate Agreement concurrently with this Agreement, the terms and conditions of which are incorporated herein by reference. Customer and 5thPort each agree to maintain the security of the PHI and EPHI and protect it from loss and destruction. Furthermore, Customer and 5thPort each agree to take all appropriate action to ensure that adequate technical, physical and administrative security measures are in place and utilized so as to prevent the unauthorized use of or access to, or the disclosure, loss or destruction of the PHI and EPHI.

7.4 Customer Control and Responsibility. Customer has and will retain sole responsibility for: (a) all Customer Data, including its content and use; (b) all information, instructions, and materials provided by or on behalf of Customer or any Customer's Authorized User in connection with the Services; (c) the Customer Systems; (d) the security and use of Customer's and its Customer's Authorized Users' Access Credentials; and (e) all access to and use of the Services and 5thPort Materials directly or indirectly by or through the Customer Systems or its or its Customer's Authorized Users' Access Credentials, with or without Customer's knowledge or consent, including all results obtained from, and all conclusions, decisions, and actions based on, such access or use.

7.5 Access and Security. Customer shall employ all physical, administrative, and technical controls, screening, and security procedures and other safeguards necessary to: (a) securely administer the distribution and use of all Access Credentials and protect against any unauthorized access to or use of the Services; and (b) control the content and use of Customer Data, including the uploading or other provision of Customer Data for Processing by the Services.

8. Fees and Payment.

8.1 Fees. Customer shall pay 5thPort the fees set forth in the Ordering Document (the "Fees").

8.2 Taxes. All Fees and other amounts payable by Customer under this Agreement are exclusive of taxes and similar assessments. Without limiting the foregoing, Customer is responsible for all sales, use, and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any foreign, federal, state, or local governmental or regulatory authority on any amounts payable by Customer hereunder, other than any taxes imposed on 5thPort's income.

8.3 Payment. Customer shall pay all Fees in accordance with the terms of the Ordering Document. Fees for Services shall be paid in advance, whether annually or monthly pursuant to the terms and on the day of the year or month specified in the Ordering Document. Customer shall make all payments in U.S. dollars. Customer shall make payments by such method and to such address or account specified in the Ordering

Document or such other address or account as 5thPort may specify in writing from time to time.

- 8.4 Late Payment. If Customer fails to make any payment when and as due then, in addition to all other remedies that may be available, including in the Ordering Document:
- (a) 5thPort may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable Law;
 - (b) Customer shall reimburse 5thPort for all reasonable costs incurred by 5thPort in collecting any late payments or interest, including attorneys' fees, court costs, and collection agency fees; and
 - (c) if such failure continues for 48 hours following 5thPort's email notice of payment failure, 5thPort may suspend performance of the Services until all past due amounts and interest thereon have been paid, without incurring any obligation or liability to Customer or any other Person by reason of such suspension.
- 8.5 No Deductions or Setoffs. All amounts payable to 5thPort under this Agreement shall be paid by Customer to 5thPort in full without any setoff, recoupment, counterclaim, deduction, debit, or withholding for any reason (other than any deduction or withholding of tax as may be required by applicable Law).
- 8.6 Fee Increases. 5thPort may periodically increase Fees in accordance with the procedures set forth in the Ordering Document.
- 8.7 Customer's Professional Practice Responsibilities. Customer shall not rely on 5thPort Materials as the sole means of obtaining or verifying or recording Patient informed consent or communicating life threatening or critically important risk factors or Patient education or intervention.
- (a) The availability of 5thPort Materials is as a convenience tool only and use of such 5thPort Systems shall not relieve Customer or Customer's Authorized Users of the obligation and responsibility for exercising medical judgment and providing appropriate medical advice in accordance with established standards of professional practice. Under no circumstances shall 5thPort be deemed a "health care practitioner" as that term is defined in Title 16 Chapter 25 of the Delaware Medical Orders for Scope of Treatment Act § 2503A as amended from time to time. Customer acknowledges that the professional duty to the Patient in providing healthcare services lies solely with the healthcare professional providing such services. Customer takes full responsibility for the use of information provided in the Services and acknowledges that the Services are in no way intended to replace or serve as a substitute for professional or health care judgment. 5thPort does not assume any responsibility for actions of Customer, any Customer's Authorized User, or any third party acting on behalf of or under the

supervision of Customer which may result in any liability or damages due to malpractice, failure to warn, negligence, strict product liability, breach of regulatory standards applicable to Customer or other basis. Customer shall ensure that Customer's Authorized Users and other healthcare professionals using the Services are aware of the limitations on and assume all risks in connection with the use of the 5thPort Systems and the Services.

(b) The parties acknowledge and agree that the Services do not replace the need for Customer to download and maintain, in accordance with applicable laws and professional standards, regular data reports and backups or redundant data archives of any Customer Data, including Patient Information such as but not limited to each Electronic Consent.

9. Confidentiality.

9.1 Confidential Information. In connection with this Agreement each party (as the “**Disclosing Party**”) may disclose or make available Confidential Information to the other party (as the “**Receiving Party**”). Subject to Section 9.2, “**Confidential Information**” means information in any form or medium (whether oral, written, electronic, or other) that the Disclosing Party considers confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, product offerings, and pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated, or otherwise identified as “confidential”. Without limiting the foregoing: (i) all 5thPort Materials and Resultant Data are the Confidential Information of 5thPort and (ii) the financial terms and existence of this Agreement are the Confidential Information of each of the parties.

9.2 Exclusions. Confidential Information does not include information that the Receiving Party can demonstrate by written or other documentary records: (a) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Agreement; (b) was or becomes generally known by the public other than by the Receiving Party's or any of its Representatives' noncompliance with this Agreement; (c) was or is received by the Receiving Party on a non-confidential basis from a third party that, to the Receiving Party's knowledge, was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; or (d) the Receiving Party can demonstrate by written or other documentary records was or is independently developed by the Receiving Party without reference to or use of any Confidential Information.

9.3 Protection of Confidential Information. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party shall:

- (a) not access or use Confidential Information other than in accordance with the terms of this Agreement and applicable Law and as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement;
- (b) except as may be permitted by and subject to its compliance with Section 9.4, not disclose or permit access to Confidential Information other than to its Representatives who: (i) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Agreement; (ii) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Section 9.3; and (iii) are bound by confidentiality and restricted use obligations at least as protective of the Confidential Information as the terms set forth in this Section 9;
- (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 the Disclosing Party of any unauthorized use or disclosure of Confidential Information and reasonably cooperate with Disclosing Party to prevent further unauthorized use or disclosure; and
- (e) ensure its Representatives' compliance with, and be responsible and liable for any of its Representatives' non-compliance with, the terms of this Section 9.
- (f) Notwithstanding any other provisions of this Agreement, the Receiving Party's obligations under this Section 9 with respect to any Confidential Information that constitutes a trade secret under any applicable Law will continue until such time, if ever, as such Confidential Information ceases to qualify for trade secret protection under one or more such applicable Laws other than as a result of any act or omission of the Receiving Party or any of its Representatives.

9.4 Compelled Disclosures. If the Receiving Party or any of its Representatives is compelled by applicable Law to disclose any Confidential Information or otherwise receives a request from any third party for discovery, including without limitation document requests, subpoenas, notices of deposition, and orders to produce documents, information or individuals, then, to the extent permitted by applicable Law, the Receiving Party shall: (a) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can seek a protective order or other remedy; and (b) provide reasonable assistance to the Disclosing Party in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this Section 9.4, the Receiving Party remains required by Law to disclose any Confidential Information, the Receiving Party shall disclose only that portion of the Confidential Information that the Receiving Party is legally required to disclose and, on the Disclosing

Party's request, shall use commercially reasonable efforts to obtain assurances from the applicable court or other presiding authority that such Confidential Information will be afforded confidential treatment.

10. Intellectual Property Rights.

10.1 5thPort Materials. All right, title, and interest in and to the 5thPort Materials, including all Intellectual Property Rights therein, are and will remain with 5thPort and, with respect to Third-Party Materials, the applicable third-party providers own all right, title, and interest, including all Intellectual Property Rights, in and to the Third-Party Materials. Customer has no right, license, or authorization with respect to any of the 5thPort Materials except as expressly set forth in Section 2.1 or the applicable third-party license, if any, in each case subject to the use restrictions set forth in Section 3. All other rights in and to the 5thPort Materials are expressly reserved by 5thPort. In furtherance of the foregoing, and to the extent allowed by Law, Customer hereby unconditionally and irrevocably grants to 5thPort an assignment of all right, title, and interest in and to the Resultant Data, including all Intellectual Property Rights relating thereto.

10.2 Customer Data. As between Customer and 5thPort, Customer is and will remain the sole and exclusive owner of all right, title, and interest in and to all Customer Data, including all Intellectual Property Rights relating thereto, except for the Resultant Data referenced in Section 10.1 herein and subject to the rights and permissions granted in Section 10.3 herein.

10.3 Consent to Use Customer Data. Customer hereby irrevocably grants all such rights and permissions in or relating to Customer Data as are necessary or useful to 5thPort, its Subcontractors, and the 5thPort Personnel to enforce this Agreement and exercise 5thPort's, its Subcontractors', and 5thPort Personnel's rights and perform 5thPort's, its Subcontractors', and the 5thPort Personnel's obligations hereunder. 5thPort is considered a "processor" of Customer Data as the term "processor" is defined by the European Union's General Data Protection Regulation. 5thPort is considered a "service provider" under the California Consumer Privacy Act, as the term relates to Customer Data and 5thPort is a Business Associate under HIPAA and as outlined in the **Data Protection Addendum**.

11. Representations and Warranties.

11.1 Mutual Representations and Warranties. Each party represents and warrants to the other party that:

- (a) it is duly organized, validly existing, and in good standing as a corporation or other entity under the Laws of the jurisdiction of its incorporation or other organization;

- (b) it has the full right, power, and authority to enter into and perform its obligations and grant the rights, licenses, consents, and authorizations it grants or is required to grant under this Agreement;
- (c) the execution of this Agreement by its representative whose signature is set forth at the end of this Agreement has been duly authorized by all necessary corporate or organizational action of such party;
- (d) when executed and delivered by both parties, this Agreement will constitute the legal, valid, and binding obligation of such party, enforceable against such party in accordance with its terms; and
- (e) the Services are provided at a price that's consistent with fair market value and in compliance with applicable Law, including without limitation, law and regulations regarding the federal Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b)) and Limitation on Certain Physician Referrals, also known as the "Stark Law" (42 U.S.C. § 1395), and the regulations promulgated thereunder, and no part of any consideration paid in connection with this Agreement is a prohibited payment under such laws for the recommending or arranging for the referral of business or the ordering of items or services, nor are the payments intended to induce illegal referrals of business.

11.2 Additional 5thPort Representations, Warranties, and Covenants. 5thPort represents, warrants, and covenants to Customer that 5thPort will perform the Services using personnel of required skill, experience, and qualifications and in a professional and workmanlike manner in accordance with generally recognized industry standards for similar services and will devote adequate resources to meet its obligations under this Agreement.

11.3 Additional Customer Representations, Warranties, and Covenants. Customer represents, warrants, and covenants to 5thPort that Customer owns or otherwise has and will have the necessary rights and consents in and relating to the Customer Data so that, as received by 5thPort and Processed in accordance with this Agreement, they do not and will not infringe, misappropriate, or otherwise violate any Intellectual Property Rights or violate any applicable Law.

11.4 DISCLAIMER OF WARRANTIES.

(a) EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN SECTION 11.1 AND SECTION 11.2, ALL SERVICES AND PROVIDER MATERIALS ARE PROVIDED "AS IS." PROVIDER SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, PROVIDER MAKES NO WARRANTY

OF ANY KIND THAT THE SERVICES OR PROVIDER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, COMPLY WITH LAW, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE. ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

(b) WITHOUT LIMITING OR NARROWING THE ABOVE, BUT SOLELY BY WAY OF EXAMPLE, 5thPort HAS NO OBLIGATION OR LIABILITY FOR ANY LOSS, ALTERATION, DESTRUCTION, DAMAGE, CORRUPTION, OR RECOVERY OF PHI, EPHI, PATIENT INFORMATION, CUSTOMER DATA OR CUSTOMER'S DATA BACKUPS IN CONNECTION WITH ANY CUSTOMER DATA DOWNLOADED TO OR MAINTAINED ON CUSTOMER SYSTEMS.

12. Indemnification.

12.1 5thPort Indemnification for Intellectual Property Infringement. 5thPort shall indemnify, defend, and hold harmless Customer and Customer's officers, directors, employees, agents, permitted successors, and permitted assigns (each, a "**Customer Indemnitee**") from and against any and all Losses incurred by a Customer Indemnitee resulting from any Action by a third party (other than an Affiliate of a Customer Indemnitee) that Customer's or a Customer's Authorized User's use of the Services (excluding Customer Data and Third-Party Materials) in accordance with this Agreement infringes or misappropriates such third party's Intellectual Property Rights. The foregoing obligation does not apply to the extent that the alleged infringement arises from:

- (a) Third-Party Materials or Customer Data;
- (b) access to or use of the 5thPort Materials in combination with any hardware, system, tablet, iPad, cell phone, device, software, network, or other materials or service not provided by 5thPort;
- (c) modification of the 5thPort Materials other than: (i) by or on behalf of 5thPort; or (ii) with 5thPort's written approval in accordance with 5thPort's written specification;
- (d) failure to timely implement any modifications, upgrades, replacements, or enhancements made available to Customer by or on behalf of 5thPort;

- (e) act, omission, or other matter described in Section 12.2(a), Section 12.2(b), Section 12.2(c), or Section 12.2(d), whether or not the same results in any Action against or Losses by any 5thPort Indemnitee; or
- (f) any Action for which 5thPort was not given notice and an opportunity to control the defense in accordance with the process set forth under Section 12.3 of this Agreement.

12.2 Customer Indemnification. Customer shall indemnify, defend, and hold harmless 5thPort and its Subcontractors and Affiliates, and each of its and their respective officers, directors, employees, agents, successors, and assigns (each, a “**5thPort Indemnitee**”) from and against any and all Losses incurred by such 5thPort Indemnitee resulting from any Action by a third party (other than an Affiliate of a 5thPort Indemnitee) arising out of or resulting from, or are alleged to arise out of or result from:

- (a) Customer Data, including any Processing of Customer Data by or on behalf of 5thPort in accordance with this Agreement;
- (b) any other materials or information (including any documents, data, specifications, software, content, or technology) provided by or on behalf of Customer or any Customer’s Authorized User, including 5thPort’s compliance with any specifications or directions provided by or on behalf of Customer or any Customer’s Authorized User to the extent prepared without any contribution by 5thPort;
- (c) allegation of facts that, if true, would constitute Customer’s breach of any of its representations, warranties, covenants, or obligations under this Agreement; or
- (d) negligence or more culpable act or omission (including recklessness or willful misconduct) by Customer, any Customer’s Authorized User, or any third party on behalf of Customer or any Customer’s Authorized User, including without limitation claims of medical malpractice, failure to warn, negligence, strict product liability, and all other bases relating to such parties’ obligations to exercise professional judgment in accordance with established standards of professional practice.

12.3 Indemnification Procedure. Each party shall promptly notify the other party in writing of any Action for which such party believes it is entitled to be indemnified pursuant to Section 12.1 or Section 12.2, as the case may be. The party seeking indemnification (the “**Indemnitee**”) shall cooperate with the other party (the “**Indemnitor**”) at the Indemnitor’s sole cost and expense. The Indemnitor shall promptly assume control of the defense and shall employ counsel of its choice to handle and defend the same, at the Indemnitor’s sole cost and expense. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor shall not settle any Action on any terms or in any manner that affects the

rights of any Indemnitee without the Indemnitee's prior written consent, which shall not be unreasonably withheld or delayed. If the Indemnitor fails or refuses to assume control of the defense of such Action, the Indemnitee shall have the right, but no obligation, to defend against such Action, including settling such Action after giving notice to the Indemnitor, in each case in such manner and on such terms as the Indemnitee may deem appropriate. The Indemnitee's failure to perform any obligations under this Section 12.3 will not relieve the Indemnitor of its obligations under this Section 12, except to the extent that the Indemnitor can demonstrate that it has been prejudiced as a result of such failure.

12.4 Mitigation. If any of the Services or 5thPort Materials are, or in 5thPort's opinion are likely to be, claimed to infringe, misappropriate, or otherwise violate any third-party Intellectual Property Right, or if Customer's or any Customer's Authorized User's use of the Services or 5thPort Materials is enjoined or threatened to be enjoined, 5thPort may, at its option and sole cost and expense:

- (a) obtain the right for Customer to continue to use the Services and 5thPort Materials as contemplated by this Agreement;
- (b) modify or replace the Services and 5thPort Materials, in whole or in part, to seek to make the Services and 5thPort Materials (as so modified or replaced) non-infringing, while providing materially equivalent features and functionality, in which case such modifications or replacements will constitute Services and 5thPort Materials, as applicable, under this Agreement; or
- (c) by written notice to Customer, terminate this Agreement with respect to all or part of the Services and 5thPort Materials, and require Customer to immediately cease any use of the Services and 5thPort Materials or any specified part or feature thereof, provided that if such termination occurs, subject to Customer's compliance with its post-termination obligations set forth in Section 14.4, Customer will be entitled to a refund of all monthly Fees actually paid during the three months immediately preceding termination.

12.5 Sole Remedy. THIS SECTION 12 SETS FORTH CUSTOMER'S SOLE REMEDIES AND PROVIDER'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED CLAIMS THAT THE SERVICES AND PROVIDER MATERIALS OR ANY SUBJECT MATTER OF THIS AGREEMENT INFRINGES, MISAPPROPRIATES, OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

13. Limitations of Liability.

13.1 EXCLUSION OF DAMAGES. EXCEPT AS OTHERWISE PROVIDED IN SECTION 13.3, IN NO EVENT WILL PROVIDER OR ANY OF ITS LICENSORS, SERVICE PROVIDERS, OR SUPPLIERS BE LIABLE UNDER OR IN

CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) LOSS OF PRODUCTION, USE, BUSINESS, REVENUE, OR PROFIT OR DIMINUTION IN VALUE; (b) IMPAIRMENT, INABILITY TO USE OR LOSS, INTERRUPTION OR DELAY OF THE SERVICES; (c) LOSS, DAMAGE, CORRUPTION OR RECOVERY OF DATA, OR BREACH OF DATA OR SYSTEM SECURITY; (d) COST OF REPLACEMENT GOODS OR SERVICES; (e) LOSS OF GOODWILL OR REPUTATION; OR (f) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES, REGARDLESS OF WHETHER SUCH PERSONS WERE ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE, AND NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE.

13.2 CAP ON MONETARY LIABILITY. EXCEPT AS OTHERWISE PROVIDED IN SECTION 13.3, IN NO EVENT WILL THE AGGREGATE LIABILITY OF PROVIDER ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING UNDER OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY, EXCEED THE TOTAL AMOUNTS PAID AND AMOUNTS ACCRUED BUT NOT YET PAID TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM. THE FOREGOING LIMITATIONS APPLY EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

13.3 Exceptions. The exclusions and limitations in Section 13.1 and Section 13.2 do not apply to 5thPort's obligations under Section 12 or liability for 5thPort's gross negligence or willful misconduct.

14. Term and Termination.

14.1 Term. The term of this Agreement shall begin on the Effective Date of the Ordering Document. Any termination of this Agreement under Section 14 shall include the termination of all Services under any Ordering Document.

14.2 Termination. In addition to any other express termination right set forth elsewhere in this Agreement or an applicable Ordering Document:

- (a) 5thPort may terminate this Agreement, effective on written notice to Customer, if Customer: (i) fails to pay any amount when and as due hereunder, and such failure continues for 48 hours following 5thPort's email notice of payment failure; or (ii) breaches any of its obligations under Section 3 or Section 9;

- (b) either party may terminate this Agreement, effective on written notice to the other party, if the other party materially breaches this Agreement, and such breach: (i) is incapable of cure; or (ii) being capable of cure, remains uncured 30 days after the non-breaching party provides the breaching party with written notice of such breach; and
- (c) either party may terminate this Agreement, effective immediately upon written notice to the other party, if the other party: (i) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (ii) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency Law; (iii) makes or seeks to make a general assignment for the benefit of its creditors; or (iv) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

14.3 Effect of Termination or Expiration. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement:

- (a) all rights, licenses, consents, and authorizations granted by 5thPort to the Customer hereunder will immediately terminate;
- (b) Customer shall immediately cease all use and return all 5thPort Equipment and cease all use of any Services or 5thPort Materials;
- (c) notwithstanding anything to the contrary in this Agreement, with respect to information and materials then in its possession or control: each party may retain such information and materials in its backups, archives, and disaster recovery systems until such information and materials are deleted in the ordinary course and all information and materials described in this Section 14.3(c) will remain subject to all confidentiality, security, and other applicable requirements of this Agreement;
- (d) Customer and Customer's Authorized User access to the 5thPort Materials shall immediately terminate and 5thPort may take any action to disable all Customer and Customer's Authorized User access to the 5thPort Materials;
- (e) Customer's access to the Services and Customer Data stored on 5thPort Systems shall end upon termination of this Agreement, except as set forth under (g) below.
- (e) if Customer terminates this Agreement pursuant to Section 14.2(b), Customer will be relieved of any obligation to pay any Fees attributable to the period after

the effective date of such termination; however Customer shall promptly pay any other amounts due and owing to 5thPort;

- (f) if 5thPort terminates this Agreement pursuant to Section 14.2(a) or Section 14.2(b), all Fees that would have become payable had the Agreement remained in effect until expiration of the Term will become immediately due and payable, and Customer shall pay such Fees, together with all previously-accrued but not yet paid Fees on receipt of 5thPort's invoice therefor; and
- (g) if Customer requests in writing within 30 calendar days after termination, 5thPort shall deliver to Customer the then most recent version of Customer Data (including any requested informed consent reports) maintained by 5thPort, provided that Customer has at that time paid all Fees then outstanding and any amounts payable after or as a result of such expiration or termination, including any expenses and fees, on a time and materials basis, for 5thPort's services in transferring such Customer Data UNLESS THE PARTIES SEPARATELY AGREE IN WRITING TO TERMS, CONDITIONS OR FEES APPLICABLE TO RETENTION OF THE DATA ON AN ONGOING BASIS. Further, in accordance with Section 6 of this Agreement, 5thPort shall otherwise have no ongoing obligations with respect to the use, storage, or maintenance of such Customer Data, except as may expressly be set forth in a Business Associate Agreement between the parties.

14.4 Surviving Terms. The provisions set forth in the following sections, and any other right or obligation of the parties in this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: Section 3, Section 9, Section 11.4, Section 12, Section 13, Section 14.3, this Section 14.4, and Section 15.

15. Miscellaneous.

- 15.1 Further Assurances. On a party's reasonable request, the other party shall, at the requesting party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, as may be necessary to give full effect to this Agreement.
- 15.2 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the parties, and neither party shall have authority to contract for or bind the other party in any manner whatsoever.
- 15.3 Public Announcements. Neither party shall issue or release any announcement, statement, press release, or other publicity or marketing materials relating to this Agreement or, unless expressly permitted under this Agreement, otherwise use the

other party's trademarks, service marks, trade names, logos, domain names, or other indicia of source, association, or sponsorship, in each case, without the prior written consent of the other party, provided, however, that 5thPort may include Customer's name and other indicia in its lists of 5thPort's current or former customers of 5thPort in promotional and marketing materials.

- 15.4 Notices. Any notice, request, consent, claim, demand, waiver, or other communications under this Agreement have legal effect only if in writing and addressed to a party as follows (or to such other address or such other person that such party may designate from time to time in accordance with this Section 15.4):

If to 5thPort: 5thPort, LLC
131 Continental Drive
Newark, Delaware 19713
Email: legal@5thPort.com

Attention: Legal Notice for the Chief Executive Officer

An email with a copy of the notice must be simultaneously sent to legal@5thPort.com

If to Customer: See Ordering Document

Notices sent in accordance with this Section 15.4 will be deemed effectively given: (a) when received, if delivered by hand; (b) when received, if sent by a nationally recognized overnight courier; (c) when sent, if by facsimile or email, (in each case, with confirmation of transmission), if sent during the addressee's normal business hours, and on the next business day, if sent after the addressee's normal business hours; and (d) on the third day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.

- 15.5 Entire Agreement. This Agreement, together with the Ordering Document and any exhibits and other documents incorporated herein by reference, constitutes the sole and entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the Ordering Document, and the related exhibits, schedules, attachments, and appendices (other than an exception expressly set forth as such therein) and any other documents incorporated herein by reference, the following order of precedence governs: (a) first, the Ordering Document (b) second, this Agreement, excluding its exhibits, schedules, attachments, and appendices; and (c) third, the exhibits, schedules, attachments, and appendices to this Agreement. However, where European Union resident personal data

is processed by 5thPort, Exhibit B of this Agreement shall take precedence over any conflicting term or condition in any of the documents referenced herein.

15.6 Assignment. Customer shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without 5thPort's prior written consent, which consent shall not be unreasonably withheld, conditioned, or delayed. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation, or reorganization involving Customer (regardless of whether Customer is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Agreement for which 5thPort's prior written consent is required. No assignment, delegation, or transfer will relieve Customer of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section 15.8 is void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

15.7 Force Majeure.

- (a) No Breach or Default. In no event will either party be liable or responsible to the other party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, (except for any obligations to make payments), when and to the extent such failure or delay is caused by any circumstances beyond such party's reasonable control (a "**Force Majeure Event**"), including acts of God, flood, fire, earthquake or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, strikes, labor stoppages or slowdowns or other industrial disturbances, passage of Law or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota, or other restriction or prohibition or any complete or partial government shutdown, or national or regional shortage of adequate power or telecommunications or transportation. Either party may terminate this Agreement if a Force Majeure Event affecting the other party continues substantially uninterrupted for a period of 30 days or more.
- (b) Affected Party Obligations. In the event of any failure or delay caused by a Force Majeure Event, the affected party shall give prompt written notice to the other party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

15.8 No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties hereto and their respective successors and permitted assigns and nothing herein,

express or implied, is intended to or shall confer upon any other Person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

- 15.9 Amendment and Modification; Waiver. No amendment to or modification of or rescission, termination, or discharge of this Agreement is effective unless it is in writing, identified as an amendment to or rescission, termination, or discharge of this Agreement and signed by an authorized representative of each party. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.
- 15.10 Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the parties hereto shall negotiate in good faith to modify this 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.
- 15.11 Governing Law; Submission to Jurisdiction. Unless otherwise prohibited by applicable law, this Agreement is governed by and construed in accordance with the internal laws of the State of Delaware without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of the State of Delaware. Unless otherwise prohibited by applicable law, any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of Delaware in each case located in New Castle County, Delaware, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding. Service of process, summons, notice, or other document by mail to such party's address set forth herein shall be effective service of process for any suit, action, or other proceeding brought in any such court.
- 15.12 Waiver of Jury Trial. Each party irrevocably and unconditionally waives any right it may have to a trial by jury in respect of any legal action arising out of or relating to this Agreement or the transactions contemplated hereby.

- 15.13 Equitable Relief. Customer acknowledges and agrees that a breach or threatened breach by Customer of any of its obligations under Section 9, Section 3, or Section 4.3 would cause 5thPort irreparable harm for which monetary damages would not be an adequate remedy and that, in the event of such breach or threatened breach, 5thPort will be entitled to equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court, without any requirement to post a bond or other security, or 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.
- 15.14 Export Compliance. The Services and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Customer represents that it is not named on any U.S. government denied-party list. Customer will not permit any Customer's Authorized User to access or use any Service in a U.S.-embargoed country or region or in violation of any U.S. export law or regulation.
- 15.15 Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction.
- 15.16 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. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

EXHIBIT A

SUPPORT SERVICES

In order to provide optimal first level support service, all problem and repair requests must first be directed to Customer's designated Service Manager for preliminary assessment and resolution. 5thPort shall have no obligation to provide Support Services for problems, outages, or failures relating to Customer Systems. If, after reasonable investigation, Customer's designated Service Manager is unable to resolve an issue or problem because such Service Manager believes that such problem or issue relates to or arose as a result of problems or issues with 5thPort Systems, 5thPort Equipment, or the Services, the Service Manager shall contact 5thPort's support team by emailing support@5thPort.com, or logging a ticket on 5thPort's Support Portal and providing details concerning the support requested.

Upon receipt of a service support email/ticket from a Service Manager, 5thPort shall do the following:

1. All problems will be recorded and assigned a ticketing number.
2. Problems will be resolved or assigned to the appropriate specialist.
3. Problems will be monitored.
4. Problem resolution will be documented and communicated to the Service Manager.
5. Provide Support Services in accordance with standard 5thPort processes and as may be specified in the Ordering Document.

Support Service response priority will be assigned using the following criteria:

1. Number of customers affected;
2. Effect on availability of Services and Customer Data;
3. Context and cause of problem;
4. Estimated solution time;
5. Application involved;
6. Frequency of problem;
7. Customer's commitment level;
8. Availability of Customer workaround; and
9. Threat to data integrity or computer security.

Data Protection Addendum

This Data Protection Addendum (“**Addendum**”) forms part of the 5thPort LLC Service Agreement (“**SA**”) between: (i) 5thPort LLC.; and (ii) (“**Customer**”).

The terms used in this Addendum shall have the meanings set forth in this Addendum. Except as modified below, the terms of the SA shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the SA. Except where the context requires otherwise, references in this Addendum to the SA are to the SA as amended by, and including, this Addendum.

Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- 1.1.1 “**Applicable Laws**” means United States federal or state law, and/or European Union or Member State laws, and/or laws of the United Kingdom that apply to 5thPort and Customer with respect to the processing of any Customer Personal Data;
- 1.1.2 “**Customer Personal Data**” means any Personal Data Processed by 5thPort on behalf of Customer pursuant to or in connection with the SA;
- 1.1.3 “**Data Protection Law**” shall mean all laws, rules, regulations, and legally binding requirements of any governmental authority or regulator applicable to the processing and security of personal data (or the equivalent) by one or both of the Parties and their Affiliates, including but not limited to the GDPR, the United Kingdom Data Protection Act 2018, and the UK GDPR;
- 1.1.4 “**GDPR**” means EU General Data Protection Regulation 2016/679;

- 1.1.5 “**Standard Contractual Clauses**” or “**SCCs**” means the agreement set out in the **Standard Contractual Clauses** of this DPA, comprising the standard contractual clauses approved by the European Commission for the transfer of Personal Data to Processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and the international data transfer addendum to the European Commission’s standard contractual clauses for international data transfers issued under Section 119A of the United Kingdom’s Data Protection Act 2018, as amended, varied, supplemented or substituted from time to time.
- 1.1.6 “**Services**” means the services and other activities to be supplied to or carried out by 5thPort for Customer pursuant to the SA and any applicable Ordering Document (“**OD**”);
- 1.1.7 “**Subprocessor**” means any person (including any third party, but excluding an employee of 5thPort or any of its sub-contractors) appointed by or on behalf of 5thPort to Process Personal Data on behalf of Customer in connection with the SA; and
- 1.1.8 “**UK GDPR**” shall mean the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018. A reference to the GDPR and/or an Article or Chapter of the GDPR shall, where the context so requires and insofar as the Applicable Data Protection Law is that of the United Kingdom, be construed as a reference to the UK GDPR and/or the equivalent Article or Chapter of the UK GDPR and/or the corresponding provision of such Applicable Data Protection Law (as applicable).
- 1.1.9 “**5thPort**” includes 5thPort LLC and its successors and assigns, as well as any affiliate of 5thPort LLC and its successors and assigns, where “affiliate” means a person or entity that directly, or indirectly, through one or more intermediaries, controls or is controlled by, or is under common control with another person or entity, and “control” means the power to direct the management and policies of the entity, whether through the ownership of securities, by contract or otherwise.
- 1.2 The terms “**Data Subject**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**” and “**Supervisory Authority**” shall have the same meaning as in the GDPR.
- 2. **Processing of Customer Personal Data**
- 2.1 5thPort shall:
 - 2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and
 - 2.1.2 not Process Customer Personal Data other than what has been specified in an applicable OD unless Processing is required by Applicable Laws to which 5thPort is subject, in which case 5thPort shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the relevant Processing of that Personal Data.

- 2.2 Customer instructs 5thPort to Process Customer Personal Data and transfer Customer Personal Data to any country or territory as reasonably necessary for the provision of the Services and consistent with the SA. Notwithstanding the preceding sentence, 5thPort shall not transfer Customer Personal Data unless it takes all such measures as are reasonably required by Customer to ensure such transfer is in compliance with any applicable Data Protection Laws. Such measures may include executing the SCCs with Customer as “data exporter” and 5thPort as “data importer” (as defined in the SCCs). Where and to the extent there is any conflict between this Addendum, the SA, and the SCCs, the SCCs will prevail in all cases.
- 2.3 Customer shall be responsible for compliance with the requirements of any Data Protection Laws imposed on data controllers, including but not limited to Article 6(1)(a) of the GDPR, to obtain consent from Data Subjects to the processing of their Personal Data for the purposes specified in the SA, any applicable OD, and this Addendum. Customer agrees to defend, indemnify and hold harmless 5thPort and its respective officers, directors, shareholders, managers, members, employees and agents (each, a “5thPort Indemnified Party”) against any claim, loss, damage, liability, penalty, fine or expense (including, without limitation, reasonable attorney’s fees and litigation costs and expenses) (a “Claim”) incurred by a 5thPort Indemnified Party by reason of or in connection with Customer’s failure to obtain consent from any Data Subject for such processing.
- 2.4 5thPorts privacy policy sets out certain information regarding 5thPort’s Processing of the Customer Personal Data as required by Article 28(3) of the GDPR. Nothing in 5thPorts privacy policy confers any right or imposes any obligation on any party to this Addendum.

3. 5thPort Personnel

5thPort shall take reasonable steps to ensure that any employee, agent, or contractor of 5thPort or a Subprocessor who may have access to the Customer Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

- 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 5thPort shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
- 4.2 In assessing the appropriate level of security, 5thPort shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Data Subject Rights

- 5.1 Taking into account the nature of the Processing, 5thPort shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 5.2 5thPort shall:

- 5.2.1 promptly notify Customer if 5thPort or a Subprocessor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and
- 5.2.2 ensure that 5thPort and, if applicable, the Subprocessor do not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which 5thPort and/or the Subprocessor are subject, in which case 5thPort shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before 5thPort and/or the Subprocessor responds to the request.

6. Personal Data Breach

- 6.1 5thPort shall notify Customer without undue delay upon 5thPort becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 6.2 5thPort shall cooperate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

7. Data Protection Impact Assessment and Prior Consultation

5thPort shall provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with Supervising Authorities or other competent data privacy authorities which Customer reasonably considers to be required of Customer by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, 5thPort and any Subprocessors.

8. Deletion or return of Customer Personal Data

- 8.1 Subject to sections 8.2, 8.3, and 8.4, 5thPort shall no later than one year after the date of cessation of any Services involving the Processing of Customer Personal Data (the “**Cessation Date**”), delete all copies of those Customer Personal Data.
- 8.2 Subject to section 8.3, Customer may by written notice to 5thPort no later than 60 days prior to the Cessation Date require 5thPort to (a) no earlier than the Cessation Date and no later than 60 days after the Cessation Date, return a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to 5thPort, with the exception that 5thPort will not return any Customer Personal Data that is maintained in off-site storage; and (b) no later than one year after the Cessation Date, delete all other copies of Customer Personal Data Processed by 5thPort, including any Customer Personal Data that is maintained in off-site storage.
- 8.3 5thPort and any Subprocessor may retain Customer Personal Data to the extent required by Applicable Laws and always provided that 5thPort shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

- 8.4 Notwithstanding the foregoing, 5thPort may retain archival copies in accordance with its record retention policies and procedures (a) with respect to backup media which selective deletion of files or data is not feasible and (b) in order to enable 5thPort to comply with its professional standards requirements and substantiate its work in the event of a dispute or otherwise.

9. Audit rights

- 9.1 Subject to sections 9.2 and 9.3, 5thPort shall make available to Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by 5thPort and any Subprocessor(s), subject to the following conditions:
- 9.1.1 Customer and any mandated auditor(s) shall conduct no more than one audit or inspection of 5thPort or any Subprocessor in any calendar year except that Customer may conduct additional audits or inspections when:
 - 9.1.1.1 Customer reasonably considers necessary because of genuine concerns as to 5thPort's compliance with this Addendum; or
 - 9.1.1.2 Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority, or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; and
 - 9.1.2 the cost of any audits conducted by Customer and/or its mandated auditor(s) shall be borne solely by Customer.
- 9.2 Customer may only mandate an auditor for the purposes of section 9.1 if the auditor is identified in the list set out in Exhibit 1 to this Addendum, as that list is amended by agreement between the parties in writing from time to time.
- 9.3 Customer shall give 5thPort reasonable notice of any audit or inspection to be conducted under section 9.1 and shall make (and ensure that each of its mandated auditors makes) reasonable efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to 5thPort's and/or any Subprocessor's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection. 5thPort and any Subprocessor(s) need not give access to its premises for the purposes of such an audit or inspection:
- 9.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;
 - 9.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to 5thPort that this is the case before attendance outside those hours begins; or
 - 9.3.3 for the purposes of more than one audit or inspection of 5thPort or any Subprocessor in any calendar year, except for any additional audits or inspections which:

- 9.3.3.1 Customer reasonably considers necessary because of genuine concerns as to 5thPort's compliance with this Addendum; or
- 9.3.3.2 Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority, or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Customer has identified its concerns or the relevant requirement or request in its notice to 5thPort of the audit or inspection.

10. Payment

Customer shall pay 5thPort for all reasonable expenses, including but not limited to the costs of labor and/or materials, incurred by 5thPort in connection with providing the assistance, cooperation, contributions, and/or information described in this Addendum. 5thPort will invoice Customer for any such expenses, and Customer agrees to pay all balances within fifteen (15) days of the date of invoice.

11. Subprocessing

- 11.1 Customer authorizes 5thPort to appoint (and permit each Subprocessor appointed in accordance with this section 11 to appoint) Subprocessors in accordance with this section 11 and any restrictions in the SA.
- 11.2 5thPort may continue to use those Subprocessors already engaged by 5thPort as of the date of this Addendum, subject to 5thPort as soon as practicable meeting the obligations set out in section 11.4.
- 11.3 5thPort shall give Customer prior written notice of the appointment of any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor. If, within fourteen (14) days of receipt of that notice, Customer notifies 5thPort in writing of any objections (on reasonable grounds to the proposed appointment), 5thPort shall not appoint that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer, and Customer has been provided with a reasonable written explanation of the steps taken.
- 11.4 With respect to each Subprocessor, 5thPort shall:
 - 11.4.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 11.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the SA;
 - 11.4.2 ensure that the arrangement between, on the one hand 5thPort (or an intermediate Subprocessor) and, on the other hand, the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of Article 28(3) of the GDPR;
 - 11.4.3 if that arrangement involves a transfer of Customer Personal Data, ensure that the Subprocessor take all such measures as are reasonably required to ensure such transfer is in compliance with any applicable Data Protection Laws; and

- 11.4.4 provide to Customer for review such copies of 5thPort's agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.
- 11.5 5thPort shall ensure that each Subprocessor performs its obligations as they apply to Processing of Customer Personal Data, as if the Subprocessor were party to this Addendum in place of 5thPort.

12. General Terms

Governing law and jurisdiction

- 12.1 The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the SA with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity.
- 12.2 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the SA.

Order of precedence

- 12.3 Nothing in this Addendum reduces 5thPort's obligations under the SA in relation to the protection of Personal Data or permits 5thPort to Process Personal Data in a manner which is prohibited by the SA.
- 12.4 Subject to section 12.3, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the SA and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Severance

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

EXHIBIT 1: LIST OF MANDATED AUDITORS

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2****Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3****Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e)
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in

Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or

pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

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

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) **GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law

or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

- (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally

liable and the data subject is entitled to bring an action in court against any of these Parties.

- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

You also may have the right to make a complaint under the GDPR to the relevant Supervisory Authority. A list of Supervisory Authorities is available [here](#).

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising

access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or

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

Clause 15

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

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of Legality and Data Minimization

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17****Governing law***

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

*Clause 18****Choice of forum and jurisdiction***

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
 - (b) The Parties agree that those shall be the courts of the Republic of Ireland.
 - (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
 - (d) The Parties agree to submit themselves to the jurisdiction of such courts.
-

APPENDIX TO THE SCCS

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer

Address: See Principle Agreement

Contact person's name, position and contact details: See Principle Agreement

Activities relevant to the data transferred under these Clauses:

Role (controller/processor): Data Controller

Data importer(s):

Name: 5thPort LLC

Address: See Principle Agreement

Contact person's name, position and contact details: See Principle Agreement

Activities relevant to the data transferred under these Clauses:

Receiving data, including collection, accessing, retrieval, recording, and data entry

Holding data, including storage, organization and structuring

Protecting data, including restricting, encrypting, and security testing

Role (controller/processor): Data Processor

B. DESCRIPTION OF TRANSFER

Subject matter and duration of the processing of personal data, the obligations and rights of the customer, categories of data subjects whose personal data is transferred, categories of personal data transferred, frequency of transfer, purpose, retention and nature of the processing are outlined in the DPA and privacy policy.

C. COMPETENT SUPERVISORY AUTHORITY

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority.

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

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

5thPort and its sub-processors will maintain physical, administrative and technical safeguards for the protection of the security, confidentiality, and integrity of Personal Data processed, as described below.

- Data encryption
- Secure storage and data protection
- Access control
- Destruction and/or deletion of extraneous records
 - Information Security and encryption policies
- Regular penetration testing
 - Firewalls

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Microsoft

Decisivedge

12928305.22

12928305.22

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

1. Part 1: Tables**Table 1: Parties**

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: The legal entity that has executed the Standard Contractual Clauses as a Data Controller Trading name (if different): Main address (if a company registered address): See Principle Agreement Official registration number (if any) (company number or similar	Full legal name: The legal entity that has executed the Standard Contractual Clauses as a Data Processor Trading name (if different): Main address (if a company registered address): See Principle Agreement Official registration number (if any) (company number or similar

	identifier): See Principle Agreement	identifier): See Principle Agreement
Key Contact	Full Name (optional): See Principle Agreement Job Title: See Principle Agreement Contact details including email: See Principle Agreement	Full Name (optional): See Principle Agreement Job Title: See Principle Agreement Contact details including email: See Principle Agreement
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See Principle Agreement Reference (if any): Other identifier (if any):
-------------------------	--

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties

Annex 1B: Description of Transfer

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data

Annex III: List of Sub processors

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 0: ☒ Importer ☒ Exporter ☐ neither Party
--	---

Part 2: Mandatory Clauses**1. ENTERING INTO THIS ADDENDUM**

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce

their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

2. INTERPRETATION OF THIS ADDENDUM

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.

Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

3. HIERARCHY

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

4. INCORPORATION OF AND CHANGES TO THE EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

- a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
- c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
- d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
- f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply.”;
- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

5. AMENDMENTS TO THIS ADDENDUM

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a its direct costs of performing its obligations under the Addendum; and/or
- b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

6. ALTERNATIVE PART 2 MANDATORY CLAUSES:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0 of those Mandatory Clauses.
--------------------------	--

12928305.22