DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("**DPA**") to the Agreement (as defined below) is entered into as of the Addendum Effective Date by and between ClearNote Health Inc., with registered address at 10578 Science Center Drive, Suite 210, San Diego, CA 92121, USA ("**Vendor**"); and the customer identified on the Agreement ("**Customer**"), together the "**Parties**" and each a "**Party**."

1. INTERPRETATION

1.1 In this DPA, the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Addendum Effective Date**" means the effective date of the Agreement.

(b) "**Agreement**" means the Test Requisition Form and any other written or electronic agreement entered into by and between the Parties.

(c) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction directly applicable to the Vendor's Processing of Customer Personal Data under the Agreement, including, as and to the extent applicable, GDPR and CCPA.

(d) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Customer Personal Data.

(e) "**Customer Personal Data**" means any information Processed by Vendor or its Sub-Processor on behalf of Customer to perform the Services under the Agreement that constitutes "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws, except that Customer Personal Data does not include the contact information pertaining to Customer's personnel or representatives who are business contacts of Customer (where Vendor acts as a controller of such information).

(f) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(g) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Customer Personal Data and the Processing thereof.

(h) "**Deidentified Data**" means data Processed by Vendor or its Sub-Processor on behalf of Customer to perform the Services under the Agreement that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or device linked to such person.

(i) "**EEA**" means the European Economic Area.

(j) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(k) "**Personal Data Breach**" means a breach of Vendor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data in Vendor's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(l) "**Personnel**" means a person's employees, agents, consultants or contractors.

(m) "**Process**" and any inflection thereof means any operation or set of operations which is performed on Customer Personal Data or on sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(n) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data on behalf of the Controller.

(o) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Customer Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "**EEA Restricted Transfer**"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(p) “**SCCs**” means collectively (i) the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914 of 4 June 2021 (“**EU SCCs**”) and (ii) the UK Transfer Addendum to the EU SCCs, issued by the Information Commissioner (Version B1.0, in force on 21 March 2022) (“**UK SCCs**”).

(q) “**Services**” means those services and activities to be supplied to or carried out by or on behalf of Vendor for Customer pursuant to the Agreement.

(r) “**Sub-Processor**” means any third party appointed by or on behalf of Vendor to Process Customer Personal Data.

(s) “**Supervisory Authority**” (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner’s Office.

2. SCOPE OF THIS DATA PROCESSING ADDENDUM

2.1 This DPA applies generally to Vendor’s Processing of Customer Personal Data under the Agreement.

2.2 The Parties acknowledge and agree that the details of Vendor’s Processing of Customer Personal Data (including the respective roles of the Parties relating to such Processing) are as described in 0 (Data Processing Details) to this DPA.

2.3 Annex 2 (European Annex) to this DPA applies only if and to the extent Vendor’s Processing of Customer Personal Data under the Agreement is subject to the GDPR.

2.4 Section 9 (Compliance Assistance; Audits) of this DPA applies to Vendor’s Processing of Customer Personal Data to the extent required under any requirements concerning contracts with Processors under Applicable Data Protection Laws, and in such cases, only in respect of Processing of Customer Personal Data subject to such laws.

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 Vendor shall not Process Customer Personal Data other than on Customer’s written instructions or as required or permitted by applicable laws. For purposes of the Services and this DPA, Vendor shall be considered as the Processor (or “service provider” as defined under Applicable Data Protection Laws).

3.2 Customer instructs Vendor to Process Customer Personal Data to provide the Services to Customer and in accordance with the Agreement (including this DPA). Customer acknowledges and agrees that Vendor may reuse that data (i) to identify future opportunities for development and to improve and personalize the Services, and (ii) to identify customer opportunities and market these to Customer. Customer acknowledges and agrees that these processing purposes are compatible with the processing to provide the Services under the Agreement. Customer grants to Vendor a non-exclusive, worldwide right to use Personal Data (a) in order to provide the Services to Customer; (b) to compile, use and disclose anonymous, aggregated statistics, provided that no such information will directly identify and cannot be used to identify Customer; and (c) as necessary to maintain and improve the Service. The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on Vendor only pursuant to any written amendment to this DPA signed by both Parties. Where required by Applicable Data Protection Laws, if Vendor receives an instruction from Customer that, in its reasonable opinion, infringes Applicable Data Protection Laws, Vendor shall notify Customer.

3.3 The Parties acknowledge that Vendor's Processing of Customer Personal Data authorized by Customer's instructions stated in the Agreement (including this DPA) are integral to the Services and the business relationship between the Parties. Access to Customer Personal Data does not form part of the consideration exchanged between the Parties in respect of the Agreement or any other business dealings.

4. VENDOR PERSONNEL

4.1 Vendor shall require that its Personnel who are authorized to access Customer Personal Data are subject to appropriate confidentiality obligations.

5. SECURITY

5.1 Vendor shall implement and maintain technical and organizational measures in relation to Customer Personal Data that are designed to protect Customer Personal Data against Personal Data Breaches as described in Annex 3 (Security Measures) (the "**Security Measures**").

5.2 Vendor may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Customer Personal Data.

6. DATA SUBJECT REQUESTS

6.1 Taking into account the nature of the Processing of Customer Personal Data by Vendor, Vendor shall provide Customer with such assistance by implementing appropriate technical and organizational measures as Customer may reasonably request to assist Customer in fulfilling its obligations under Applicable Data Protection Laws to respond to Data Subject Requests.

6.2 Vendor shall:

(a) promptly notify Customer if it receives a Data Subject Request; and

(b) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except as required by Applicable Data Protection Laws. Customer will be responsible for responding to any such request.

7. PERSONAL DATA BREACH

Breach notification and assistance

7.1 Vendor shall notify Customer without undue delay upon Vendor's confirmation of a Personal Data Breach affecting Customer Personal Data. Vendor's notification of or response to a Personal Data Breach shall not be construed as Vendor's acknowledgement of any fault or liability with respect to the Personal Data Breach.

7.2 To the extent the Personal Data Breach resulted from Vendor's breach of its security obligations under the Agreement, Vendor shall provide Customer with reasonably requested information (insofar as such information is within Vendor's possession and knowledge and does not otherwise compromise the security of any Customer Personal Data Processed by Vendor or the Vendor's other confidentiality or nondisclosure obligations, including any imposed by a law enforcement, a Supervisory Authority, or other governmental authority) to allow Customer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. If the Personal Data Breach did not result from Vendor's breach of its security obligations under the Agreement, Vendor shall reasonably cooperate with Customer; provided, however, Customer shall reimburse Vendor for any costs incurred by Vendor. Customer is solely responsible for complying with notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breaches.

Notification to Vendor

7.3 If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority or other governmental authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Vendor, where permitted by applicable laws, Customer agrees to:

(a) notify Vendor in advance in writing; and

(b) in good faith, consult with Vendor and consider any clarifications or corrections Vendor may reasonably recommend or request to any such notification, which: (i) relate to Vendor's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

8. SUB-PROCESSING

8.1 Customer generally authorizes Vendor to appoint Sub-processors in accordance with this Section 8. Without limitation to the foregoing, Customer authorizes the engagement of the Sub-processors listed as of the effective date of the Agreement at the Sub-processor Site, as defined below.

8.2 Information about Sub-processors, including their functions and locations, is available at: https://www.avantect.com/subprocessors/ (as may be updated by Vendor from time to time, subject to Vendor's obligations pursuant to Section 8.4 below) or such other website address as Vendor may provide to Customer from time to time (the "**Sub-processor Site**").

8.3 When engaging any Sub-processor, Vendor will enter into a written contract with such Sub-processor containing data protection obligations not less protective than those in this DPA with respect to Customer Personal Data and to the extent applicable to the nature of the services provided by such Sub-processor. As between the Parties, Vendor shall be liable for the acts and omissions of all Sub-processors under or in connection with this DPA to the same extent Vendor would be liable under the terms of this DPA if performing such services itself directly.

8.4 When Vendor engages any Sub-processor after the effective date of the Agreement, Vendor will notify Customer of the engagement (including the name and location of the relevant Sub-processor and the activities it will perform) by updating the Sub-processor Site or by other written means at least 15 days before such Sub-processor Processes Customer Personal Data. If Customer objects to such engagement in a written notice to Vendor within 15 days after being notified of the engagement on reasonable grounds relating to the protection of Customer Personal Data, Customer and Vendor will work together in good faith to consider a mutually acceptable resolution to such objection. If the Parties are unable to reach a mutually agreeable resolution within a reasonable timeframe, Customer may, within 30 days of its initial notification of its objection to Vendor, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Vendor and pay Vendor for all amounts due and owing under the Agreement as of the date of such termination. If Customer does not object to Vendor's appointment of a Sub-processor during the objection period referred to in this Section 8.4, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-processor.

9. COMPLIANCE ASSISTANCE; AUDITS

9.1 Taking into account the nature of the Processing of Customer Personal Data by Vendor and the information available to Vendor, Vendor shall provide such information and assistance to Customer as Customer may reasonably request (insofar as such information is available to Vendor and the sharing thereof does not compromise the security, confidentiality, integrity or availability of any data Processed by Vendor) to help Customer meet its obligations under Applicable Data Protection Laws, including in relation to the security of Customer Personal Data, the reporting and investigation of Personal Data Breaches, the demonstration of Customer's compliance with such obligations and the performance of any data protection assessments and consultations with Supervisory Authorities or other government authorities regarding such assessments in relation to Vendor's Processing of Customer Personal Data, including those required under Articles 35 and 36 of the GDPR.

9.2 Subject to Section 9.4 below, Vendor shall make available to Customer such information as Customer may reasonably request for Vendor to demonstrate compliance with Applicable Data Protection Laws and this DPA. Without limitation of the foregoing, Customer may conduct (in accordance with Section 9.3), at its sole cost and expense, and Vendor will reasonably cooperate with, reasonable audits (including inspections, manual reviews, automated scans and other technical and operational testing that Customer is entitled to perform under Applicable Data Protection Laws), in each case, whereby Customer or a qualified and independent auditor appointed by Customer using an appropriate and accepted audit control standard or framework may audit Vendor's technical and organizational measures in support of such compliance and the auditor's report is provided to Customer and Vendor upon Customer's request.

9.3 Customer shall give Vendor reasonable advance notice of any such audits. Vendor need not cooperate with any audit (a) performed by any individual or entity who has not entered into a non-disclosure agreement with Vendor on terms acceptable to Vendor in respect of information obtained in relation to the audit; (b) conducted outside of Vendor's normal business hours at the relevant site; or (c) on more than one occasion in any calendar year during the term of the Agreement, except for any additional audits that Customer is required to perform under Applicable Data Protection Laws. The audit must be conducted in accordance with Vendor's safety, security or other relevant policies, must not impact the security, confidentiality, integrity or availability of any data Processed by Vendor and must not unreasonably interfere with Vendor's business activities. Customer shall not conduct any scans or technical or operational testing of Vendor's applications, websites, services, networks or systems without Vendor's prior approval (which shall not be unreasonably withheld).

9.4 If the controls or measures to be assessed in the requested audit are assessed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified and independent third-party auditor pursuant to a recognized industry standard audit framework within twelve (12) months of Customer's audit request ("**Audit Report**") and Vendor has confirmed in writing that there have been no known material changes to the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures. Vendor shall provide copies of any such Audit Reports to Customer upon request.

9.5 Such Audit Reports and any other information obtained by Customer in connection with an audit under this Section 9 shall constitute the Confidential Information of Vendor, which Customer shall use only for the purposes of confirming compliance with the requirements of this DPA or meeting Customer's obligations under Applicable Data Protection Laws. Nothing in this Section 9 shall be construed to obligate Vendor to breach any duty of confidentiality.

10. RETURN AND DELETION

10.1 Within 30 days after the expiration or earlier termination of the Agreement, Vendor shall, to the fullest extent technically possible in the circumstances, either (i) return and/or delete all Customer Personal Data in Vendor's care, custody or control in accordance with Customer's instructions as to the post-termination return and deletion of Customer Data expressed in the Agreement, or subject to Section 11.5, Customer's further instructions or (ii) irreversibly anonymize or deidentify all Customer Personal Data in Vendor's care, custody or control.

10.2 Notwithstanding the foregoing, Vendor may retain Customer Personal Data where required by law (or in the case of Customer Personal Data subject to the GDPR, the laws of the UK or European Economic Area, as applicable), provided that Vendor shall (a) maintain the confidentiality of all such Customer Personal Data and (b) Process the Customer Personal Data only as necessary for the purpose(s) and duration specified in the applicable law requiring such retention.

11. CUSTOMER'S RESPONSIBILITIES

11.1 Without limiting Section 1.4 of the Agreement, Customer agrees that, without limiting Vendor's obligations under Section 5 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Vendor uses to provide the Services; and (d) backing up Customer Personal Data.

11.2 Customer shall ensure:

(a) that there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Vendor of Customer Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable)); and

(b) that (and is solely responsible for ensuring that) all required notices have been given to, and all consents, permissions, and rights have been obtained from, Data Subjects and others as may be required by Applicable Data Protection Laws or otherwise for Vendor to Process Customer Personal Data as contemplated in the Agreement.

11.3 Customer agrees that the Services, the Security Measures, and Vendor's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Customer Personal Data.

11.4 Customer shall not, and agrees to ensure its Authorized Users do not, provide or otherwise make available to Vendor any Customer Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) biometric information; (c) credentials to any financial accounts or credit, debit or other payment card data subject to the Payment Card Industry Data Security Standard (PCI DSS); (d) tax return data; (e) precise geolocation; (f) data revealing racial or ethnic origin, religious beliefs, sex life or sexual orientation, union membership, citizenship, or immigration status; (g) data collected from a known child; (h) any information that constitutes a special category of personal data (as described in Article 9(1) of the GDPR) other than health data; and (i) any online account credentials. Customer acknowledges that Vendor is not a business associate (as that term is defined under HIPAA) or a payment card processor. Customer acknowledges that the Service is not designed to be PCI DSS compliant.

11.5 Except to the extent prohibited by applicable law, Customer shall compensate Vendor at Vendor's then-current professional services rates for, and reimburse any costs reasonably incurred by Vendor in the course of providing, cooperation, information or assistance requested by Customer pursuant to Sections 6 (Data Subject Requests), 9 (Compliance Assistance; Audits), and 10.1 (in Return and Deletion) of this DPA, beyond providing self service features included as part of the Services.

12. DEIDENTIFIED, ANONYMIZED OR AGGREGATED DATA

12.1 To the extent Vendor processes or generates any Deidentified Data, Vendor shall (i) take reasonable measures to ensure that such data cannot be associated with a natural person, and (ii) publicly commit to maintaining and using Deidentified Data only in a de-identified fashion and without attempting to re-identify such data.

12.2 If Vendor's creation and/or use of aggregated, anonymized or deidentified personal information is subject to Applicable Data Protection Laws, then Vendor's creation and/or use of such data, including but not limited to Deidentified Data, shall be permitted only to the extent such data constitutes "aggregate consumer information" or has been "deidentified" (as such terms are defined under the Applicable Data Protection Laws).

13. LIABILITY

13.1 The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA and the SCCs (if and as they apply) is limited per event (a series of related events counts as one event) to an amount that is the lesser of the payments made by Customer to Vendor in the twelve (12) months prior to the event that caused damage, or €5,000; provided that, nothing in this Section 13 will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the SCCs (if and as they apply).

14. CHANGE IN LAWS

14.1 Vendor may on notice vary this DPA to the extent that (acting reasonably) it considers necessary to address the requirements of Applicable Data Protection Laws from time to time, including by varying or replacing the SCCs in the manner described in Paragraphs 2.1 and 2.2 of Annex 2 (European Annex).

15. INCORPORATION AND PRECEDENCE

15.1 This DPA shall be incorporated into and form part of the Agreement with effect from the Addendum Effective Date.

15.2 In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Paragraph 2 of Annex 2 (European Annex) and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1
Data Processing Details

VENDOR / 'DATA IMPORTER' DETAILS

Name:	As set out in the preamble to the DPA
Address:	As set out in the preamble to the DPA
Contact Details for Data Protection:	Name: Wayne Volkmuth Email: dp@clearnotehealth.com Role: SVP Informatics and Data Discovery
Vendor Activities:	Supply kits for customers, offer technical support to customers, process blood samples and track associated data, generate and deliver patient reports after processing blood samples, receive and process payments for service.
Role:	Processor
Signature and date:	DocuSigned by: Signature: ____________ 0F8060E476F94C1... Date: Addendum Effective Date

CUSTOMER / 'DATA EXPORTER' DETAILS

Name:	As set out in the TRF
Address:	As recorded in the Vendor's Customer Relationship Management system
Contact Details for Data Protection:	As set out in the TRF
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Services under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of its ongoing business operations.
Role:	Controller
Signature and date:	Signature: As set out in the TRF

	Date: Addendum Effective Date

DETAILS OF PROCESSING

Categories of Data Subjects:	Relevant Data Subjects include: • End-users of the Services • Patients Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Relevant Personal Data includes: • Identification data (name, first name, address, etc.) • Contact details (email, phone number, etc.) • Financial data (invoices, etc.) • Electronic identification data (IP address, cookies, etc.)
Sensitive Categories of Data, and associated additional restrictions/safeguards:	Categories of sensitive data: • Genetic data • Data concerning health • Date of birth • Sex at birth • Ethnicity Additional safeguards for sensitive data: N/A
Frequency of transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the Agreement, such as collection, recording, organizing, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

Purpose of the Processing:	Customer Personal Data will be processed: (i) as necessary to provide the Services as initiated by Customer in its use thereof, and (ii) to comply with any other reasonable instructions provided by Customer in accordance with the terms of this DPA.
Duration of Processing / Retention Period:	Concurrent with the term of the Agreement and then thereafter pursuant to Section 10 (Return and Deletion) of this DPA.
Transfers to Sub-processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with the DPA).

Annex 2

European Annex

1. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

1.1 Taking into account the nature of the Processing of Customer Personal Data by Vendor and the information available to Vendor, Vendor shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by Vendor.

2. RESTRICTED TRANSFERS

EEA Restricted Transfers

2.1 To the extent that any Processing of Customer Personal Data under this DPA involves an EEA Restricted Transfer from Customer to Vendor, the Parties shall comply with their respective obligations set out in the EU SCCs, which are hereby deemed to be:

(a) populated in accordance with Part 1 of Attachment 1 to this Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

UK Restricted Transfers

2.2 To the extent that any Processing of Customer Personal Data under this DPA involves a UK Restricted Transfer from Customer to Vendor, the Parties shall comply with their respective obligations set out in the UK SCCs, which are hereby deemed to be:

(a) The EU SCCs as varied to address the requirements of the UK GDPR in accordance with the UK Transfer Addendum and populated in accordance with Part 2 of Attachment 1 to this Annex 2 (European Annex); and

(b) entered into by the Parties and incorporated by reference into this DPA.

Adoption of new transfer mechanism

2.3 Vendor may on notice vary this DPA and replace the relevant SCCs with:

(a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or

(b) another transfer mechanism,

that enables the lawful transfer of Customer Personal Data by Customer to Vendor under this DPA in compliance with Chapter V of the GDPR.

Provision of full-form SCCs

2.4 In respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request (made to the contact details set out in Annex 1 (Data Processing Details); accompanied by suitable supporting evidence of the relevant request), Vendor shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with Attachment 1 to this Annex 2 (European Annex) in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

3. **OPERATIONAL CLARIFICATIONS**

3.1 When complying with its transparency obligations under Clause 8.3 of the EU SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect Vendor's and its licensors' trade secrets, business secrets, Confidential Information and/or other commercially sensitive information.

3.2 Where applicable, for the purposes of Clause 10(a) of Module Two of the EU SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Vendor to notify any third-party controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

3.3 For the purposes of Clause 15.1(a) of the EU SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

3.4 The terms and conditions of Section 8 of this DPA apply in relation to Vendor's appointment and use of Sub-processors under the EU SCCs. Any approval by Customer of Vendor's appointment of a Sub-processor that is given expressly or deemed given pursuant to Section 8 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-processors if and as required under Clause 8.8 of the EU SCCs.

3.5 The audits described in Clauses 8.9(c) and 8.9(d) of the EU SCCs shall be subject to any relevant terms and conditions detailed in Section 9 of this DPA.

3.6 Certification of deletion of Customer Personal Data as described in Clauses 8.5 and 16(d) of the EU SCCs shall be provided only upon Customer's written request.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

ATTACHMENT 1 TO EUROPEAN ANNEX

POPULATION OF SCCs

Notes:

- In the context of any EEA Restricted Transfer, the EU SCCs populated in accordance with Part 1 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 2.1 of Annex 2 (European Annex) to the DPA).
- In the context of any UK Restricted Transfer, the UK SCCs (i.e. the EU SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Attachment 1) are incorporated by reference into and form an effective part of the DPA (if and where applicable in accordance with Paragraph 2.2 of Annex 2 (European Annex) to the DPA).

PART 1: POPULATION OF THE SCCs – EU SCCs

1. **SIGNATURE OF THE EU SCCs:**

Where the EU SCCs apply in accordance with Paragraph 2.1 of 0 2 (European Annex) to the DPA, (a) each of the Parties is hereby deemed to have signed the EU SCCs at the relevant signature block in Annex I to the Appendix to the EU SCCs; and (b) those EU SCCs are entered into by and between the Parties with effect from (i) the Addendum Effective Date; or (ii) the date of the first EEA Restricted Transfer to which they apply in accordance with Section 10 of this DPA, whichever is earlier.

2. **MODULES**

The following module of the EU SCCs apply in the manner set out below (having regard to the role(s) of Customer set out in **Error! Reference source not found.** to 0 (European Annex) to the DPA): Module Two of the EU SCCs applies to any EEA Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is a Controller in its own right.

3. POPULATION OF THE BODY OF THE EU SCCs

3.1 For Module Two of the EU SCCs, the following applies as and where applicable to that Module and the Clauses thereof:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Section 8.4 of the DPA; and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the EU SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed and all text therein is retained.

(e) In Clause 17: OPTION 1 applies, and the Parties agree that the EU SCCs shall be governed by the law of Ireland in relation to any EEA Restricted Transfer; and OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the EU SCCs in relation to any EEA Restricted Transfer shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

3.2 In this Paragraph 3, references to "**Clauses**" are references to the Clauses of the EU SCCs.

4. POPULATION OF ANNEXES TO THE APPENDIX TO THE EU SCCs

4.1 Annex I to the Appendix to the EU SCCs is populated with the corresponding information detailed in 0 (Data Processing Details) to the DPA, with: Customer being 'data exporter'; and Vendor being 'data importer'.

4.2 Part C of Annex I to the Appendix to the EU SCCs is populated as below:

(a) Where Customer is established in an EU Member State, the competent supervisory authority shall be the supervisory authority of that EU Member State in which Customer is established.

(b) Where Customer is not established in an EU Member State, Article 3(2) of the EU GDPR applies and Customer has appointed an EU representative under Article 27 of the EU GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which Customer's EU representative relevant to the processing hereunder is based (from time-to-time).

(c) Where Customer is not established in an EU Member State, Article 3(2) of the EU GDPR applies, but Customer has not appointed an EU representative under Article 27 of the EU GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to Vendor's contact point for data protection identified in Annex 1 (Data Processing Details) to the DPA, which must be an EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

4.3 Annex II to the Appendix to the EU SCCs is populated as below:

General:

- Please refer to Section 5 of the DPA and the Security Measures described therein.
- In the event that Customer receives a Data Subject Request under the EU GDPR and requires assistance from Vendor, Customer should email Vendor's contact point for data protection identified in 0 (Data Processing Details) to the DPA.

Sub-Processors: When Vendor engages a Sub-Processor under these Clauses, Vendor shall enter into a binding contractual arrangement with such Sub-Processor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the DPA – including in respect of:

- applicable information security measures;
- notification of Personal Data Breaches to Vendor;
- return or deletion of Customer Personal Data as and where required; and
- engagement of further Sub-Processors.

PART 2: UK RESTRICTED TRANSFERS – UK SCCs

1. UK TRANSFER ADDENDUM

1.1 Where relevant in accordance with Paragraph 2.2 of 0 (European Annex) to the DPA, the EU SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum (UK SCCs) in the manner described below –

(a) *Part 1 to the UK Transfer Addendum*. The Parties agree:

(i) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in 0 (Data Processing Details) to the DPA and the foregoing provisions of this **Error! Reference source not found.** (European Annex) (subject to the variations effected by the UK Mandatory Clauses described in (b) below); and

(ii) Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

(b) *Part 2 to the UK Transfer Addendum*. The Parties agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum.

1.2 As permitted by Section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner set out in Paragraph 1.1 of this Part 2; **provided that** the Parties further agree that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of the UK Mandatory Clauses).

1.3 In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in Paragraph 1.1 of this Part 2.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Annex 3

Security Measures

As from the Addendum Effective Date, Vendor will implement and maintain the Security Measures as set out in this 0.

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Vendor’s information security program.

2. Data security controls which include at a minimum: logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilization of commercially reasonable encryption technologies for Customer Personal Data.

3. Logical access controls designed to manage electronic access to data and system functionality, based on authority levels and job functions.

4. Password controls designed to manage and control password strength, expiration and usage.

5. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

6. Physical and environmental security of data centers, server room facilities and other areas containing Customer Personal Data designed to protect information assets from unauthorized physical access or damage.

7. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Vendor’s possession.

8. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Vendor’s technology and information assets.

9. Incident management procedures designed to allow Vendor to investigate, respond to, mitigate and notify of events related to Vendor’s technology and information assets.

10. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

11. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

12. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Vendor may update the Security Measures from time to time in accordance with Section 5.2 (in Security) of the DPA.

[REMAINDER OF PAGE INTENTIONALLY BLANK]