DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the active agreement (the "**Agreement**") entered into by and between Emerald X, LLC, a Delaware limited liability company (**"Emerald"** or "**Company**") and any business entity ("**Vendor**") (collectively, the "**Parties**") from which Emerald procures goods or services (identified either as "Services", and hereinafter defined as "**Services**"). This DPA reflects the Parties' agreement with regard to the Processing of Company Personal Data.

In the course of providing the Services to Company pursuant to the Agreement, Vendor may Process Company Personal Data on behalf of Company and the Parties agree to comply with the following provisions with respect to Company Personal Data.

1. DEFINITIONS

1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. In this DPA, the following terms shall have the meanings set out below:

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means ownership (directly or indirectly) of more than 50% of the voting rights in the applicable entity.

"**Company Group Member**" means Company or any Company Affiliate.

"**Company Personal Data**" means any Personal Data Processed by Vendor or Vendor's Subprocessor on behalf of Company pursuant to the Agreement.

"**Data Protection Assessment**" means an assessment of the impact of processing operations on the protection of Personal Data and the rights of Data Subjects, or is otherwise defined as a "Data Protection Assessment," "Data Protection Impact Assessment," or "Risk Assessment" by applicable Data Protection Laws.

"**Data Protection Laws**" means any and all applicable data protection, security, or privacy-related laws, statutes, directives, or regulations, including but not limited to: (a) the EU General Data Protection Regulation 2016/679 ("**GDPR**") together with any amending or replacement legislation, and any EU Member State laws and regulations promulgated or incorporated thereunder; (b) the UK Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (c) the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**"), together with any amending or replacement legislation, including the California Privacy Rights Act of 2020 and any regulations promulgated thereunder; (d) the Virginia Consumer Data Protection Act of 2021, Va. Code Ann. § 59.1-571 to -581; (e) the Colorado Privacy Act of 2021, Co. Rev. Stat. § 6-1-1301 et seq.; (f) Connecticut Public Act No. 22-15, "An Act Concerning Personal Data Privacy and Online Monitoring"; (g) the Utah Consumer Privacy Act of 2022, Utah Code Ann. § 13-61-101 et seq.; and (h) all other equivalent or similar laws and regulations in any relevant jurisdiction relating to Personal Data and privacy, and as each may be amended, extended or re-enacted from time to time.

"**Data Subject**" means an identified or identifiable natural person whose Personal Data is being Processed. Where applicable, the term "Data Subject" shall refer to a "Consumer" as that term is defined under Data Protection Laws.

"**Deidentified Data**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, be linked directly or indirectly with, or be reasonably be used to infer information about an identifiable natural person.

"**Downstream Participant**" means any third party that Processes Company Personal Data that is not Company, Vendor, or a Subprocessor.

"**Personal Data**" means information that identifies, relates to, describes, is capable of being associated with, or can reasonably be linked, directly or indirectly, with a particular individual or household, or is otherwise defined as "personal data," "personal information," or "personally identifiable information" by applicable Data Protection Laws.

"**Personnel**" means officers, directors, employees, Subprocessors, agents and representatives.

"**Regulatory Authority**" means the applicable public authority or government agency responsible for supervising compliance with Data Protection Laws, including, but not limited to: the UK Information Commissioner's Office; EU Member State supervisory authorities; the California Privacy Protection Agency; and U.S. state attorneys general.

"**Security Breach**" means any actual or suspected event that has, or may have, compromised or adversely impacted the confidentiality, security, integrity, availability, or resilience of Company Personal Data including any (i) unauthorized access, use, disclosure, modification, or destruction of Company Personal Data; (ii) act that violates any law with respect to Company Personal Data; (iii) loss or misuse (by any means) of any Company Personal Data; or (iv) inadvertent, unauthorized and/or unlawful Processing of any Company Personal Data.

"**Subprocessor**" means any third party appointed by Vendor to Process Company Personal Data as a Service Provider or Processor on behalf of Company in connection with the Agreement.

The terms "**Business**," "**Business Purpose**," "**Controller**," "**Process**," "**Processor**," "**Sale**," "**Service Provider**," "**Share**" and "**Third-Party**" shall have the same meaning as in the Data Protection Laws, and their cognate terms shall be construed accordingly.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Company Personal Data, Company is the Controller or Business (as applicable), Vendor is the Processor or Service Provider (as applicable), and that Vendor will engage Subprocessors pursuant to the requirements set forth in Section 5 below. The Parties acknowledge and agree that neither Party has reason to believe that the other Party is unable to comply with the provisions of this DPA or otherwise that such Party is in violation of any Data Protection Law.

2.2 **Vendor's Processing of Personal Data.** Vendor shall treat Company Personal Data as confidential and shall only Process Company Personal Data as necessary to perform its obligations on behalf of and in accordance with Company's documented instructions for the following permitted purposes: (i) in accordance with the Agreement and applicable order or scope of work; (ii) if initiated by Data Subjects in their use of the Services; and/or (iii) to comply with other documented reasonable instructions provided by Company (e.g., via email) where such instructions are consistent with the terms of the Agreement and Data Protection Laws.

2.3 **Company's Processing of Personal Data.** Company shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Company's instructions to Vendor related to the Processing of Company Personal Data shall comply with Data Protection Laws.

2.4 **Personal Data Processing.** To the extent that the Agreement or Company's instructions to Vendor involve the processing of Company Personal Data concerning California Data Subjects, and to the extent that the CCPA governs the processing of the Company Personal Data, the Parties acknowledge and agree that with respect to such information:

2.4.1 Company shall disclose Company Personal Data to Vendor only for the limited and specified purposes specified in the Agreement. Company reserves the right, upon reasonable notice, to take reasonable and appropriate steps to help ensure that Vendor uses Company Personal Data transferred in a manner consistent with Company's obligations under the CCPA, including reasonable and appropriate steps to stop and remediate unauthorized use of Company Personal Data.

2.4.2 When acting as a Service Provider under the CCPA, or when acting as a Processor and to the extent required by applicable Data Protection Laws, Vendor shall not: (a) Sell or Share Company Personal Data; (b) retain, use, or disclose Company Personal Data for any purpose other than for the Business Purposes specified in the Agreement; (c) retain, use, or disclose Company Personal Data outside of the direct business relationship between Vendor and Company; or (d) combine Company Personal Data with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with Data Subjects, provided that Vendor may combine Personal Data to perform a Business Purpose. Vendor shall comply with applicable obligations and provide the same level of privacy protection as required by Data Protection Laws, and shall assist Company through appropriate technical and organizational measures to comply with the requirements of Data Protection Laws, taking into account the nature of the processing. Vendor shall notify Company if it makes a determination that it can no longer meet its obligations under Data Protection Laws.

2.4.3 To the extent Vendor is authorized by Company to act as a Third Party (as defined under the CCPA), Vendor is not required to comply with the obligations described in Section 2.4.2(a)-(d) (but, for the avoidance of doubt, solely when acting as a CCPA Third Party, it being understood these obligations shall still apply when Vendor is acting as a Processor under other Data Protection Laws or when acting as a Service Provider under CCPA); however, when acting as a Third Party, Vendor shall comply with all other obligations in this DPA applicable to Processors or Service Providers as required by applicable Data Protection Laws, including under § 7053 of the CCPA regulations, and any other requirements under the Agreement that are consistent with Vendor's obligations as a Third Party, including the following:

(a) Vendor's use of the Company Personal Data is limited to the specific purposes identified in the Agreement and Vendor shall not exceed such specific purposes;

(b) Vendor shall comply with the same level of privacy protection as required of a business pursuant to the CCPA with respect to the Company Personal Data;

(c) Company grants Vendor the right to take reasonable and appropriate steps to ensure that Vendor uses the Company Personal Data in a manner consistent with this Agreement and applicable Data Protection Laws;

(d) Company grants Vendor the right, upon notice, to take reasonable and appropriate steps to stop and remediate the unauthorized use of Company Personal Data made available to Vendor; and

(e) Vendor shall notify Company after it makes a determination that it can no longer meet its obligations under applicable Data Protection Laws.

1. In addition, a Vendor that is a Third Party shall not share any Personal Information with a Downstream Participant, unless expressly permitted by the Agreement. Without limiting the foregoing, Vendor agrees to defend, indemnify, and hold harmless Company from and against any and all damages in any way arising by reason of, relating to, or based upon, the Processing of Personal Data by a Downstream Participant, including any related acts or omissions.

2.5 Details of the Processing. The subject matter of Processing, the duration of the Processing, the nature and purpose of the Processing, the types of Company Personal Data, the categories of Data Subjects Processed under this DPA, and the authorized Subprocessors are specified in Exhibit 1 attached to the Parties' relevant SOW ("**Exhibit 1**").

2.6 Instructions for Processing. Each Company Group Member instructs Vendor and each Vendor Affiliate (and authorizes Vendor and each Vendor Affiliate to instruct each Subprocessor) to Process Company Personal Data, and in particular, transfer Company Personal Data to any country or territory, solely as necessary for the provision of the Services and consistent with the Agreement and this DPA. Vendor shall immediately inform Company if, in its opinion, an instruction violates Data Protection Laws.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Request Notifications. Vendor shall, to the extent legally permitted, promptly (in no event more than forty-eight (48) hours after receipt) notify Company if Vendor receives a request from a Data Subject to exercise the Data Subject's rights, including the rights to: knowledge/access; correction; deletion; restriction; objection; data portability; opt out of the Processing of and/or the Sale or Sharing of Personal Data; limit the use or disclosure of sensitive Personal Data; or any other request with respect to Personal Data of the applicable Data Subject, as set forth under applicable Data Protection Laws ("Data Subject Request"). With respect to a Data Subject Request exercising the right to deletion and to the extent required by Data Protection Laws, Vendor shall notify its Subprocessors to delete any Company Personal Data that they are Processing on behalf of Vendor.

3.2 Assistance With Data Subject Requests. Taking into account the nature of the Processing and the Company Personal Data, Vendor shall assist Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Company's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Company, in its use of the Services, does not have the ability to address a Data Subject Request directly, Vendor shall, upon Company's written request, exercise reasonable efforts to assist Company in responding to such Data Subject Request, to the extent Vendor is legally permitted to do so. This shall include, to the extent required by Data Protection Laws, Vendor

taking affirmative steps to delete (or enabling Company to delete) Company Personal Data collected, used, processed, or retained by Vendor. Nothing in this Section 3 shall require Vendor to disclose or reveal any trade secrets.

4. VENDOR PERSONNEL

4.1 **Confidentiality.** Vendor shall ensure that its Personnel engaged in the Processing of Company Personal Data are informed of the confidential nature of the Company Personal Data, have executed written confidentiality agreements, and have received appropriate training regarding the Processing of Company Personal Data.

4.2 **Reliability.** Vendor shall endeavor, in the exercise of its reasonable business discretion, to ensure the reliability of any Personnel engaged in the Processing of Company Personal Data.

4.3 **Limitation of Access.** Vendor shall ensure that Vendor's access to Company Personal Data is limited to those Personnel performing Services in accordance with the Agreement.

4.4 **Data Protection Officer.** To the extent required by applicable Data Protection Laws, each party has appointed a data protection officer.

5. SUBPROCESSORS

5.1 **Appointment of Subprocessors.** With respect to the Processing of Company Personal Data, each Company Group Member authorizes Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this Section 5.1 to appoint) Subprocessors in accordance with this Section 5. Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as of the date of this DPA, subject to Vendor and each Vendor Affiliate in each case, as soon as practicable, meeting the obligations set out in this Section 5. Vendor or a Vendor Affiliate has entered or will enter into a written agreement with each Subprocessor containing data protection obligations substantially similar to those in this Agreement with respect to the protection of Company Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor. Upon Company's request, Vendor shall provide Company with copies of such Subprocessor written contractual obligations. Vendor shall promptly (and in all cases within five (5) business days) notify Company of any failure by a Subprocessor to fulfill its obligations under such contractual obligations. Vendor shall make reasonable efforts to monitor Subprocessors compliance and ensure that all Subprocessors comply with Data Protection Laws.

5.2 **Prior Authorization for Appointment of New Subprocessors.** Company authorizes Vendor's engagement of Subprocessors from the list in Exhibit 1. Vendor shall give Company written notice of the appointment of any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor, and shall not disclose any Company Personal Data to any such new Subprocessor without Company's prior written authorization. Vendor shall submit such written notice and request for Company's authorization to Company at least 30 days prior to the engagement of any new Subprocessor, along with information sufficient to allow Company to decide whether to authorize the new Subprocessor. In the event Company does not authorize a Subprocessor, Vendor shall not engage such Subprocessor to Process Company Personal Data. If, as a result, Vendor is unable to provide the Services, Vendor and Company shall cooperate to identify alternative Subprocessor or Services. In the event Vendor and Company are unable to come to an agreement within a reasonable time with respect to a Subprocessor or alternative Services, Company may immediately terminate the Agreement, in whole or in part, for cause, and

at Company's option, with or without any cure period. Vendor remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error, or omission of its Subprocessors.

6. SECURITY

6.1 Controls for the Protection of Company Personal Data. The Parties shall maintain appropriate physical, technical and organizational measures designed to protect the security (including against unauthorized or unlawful Processing of, and against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to data), confidentiality, and integrity of Company Personal Data, including, inter alia, as appropriate ("**Security Controls**"): (i) the pseudonymization and encryption of Company Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Company Personal Data, Services, and Processing systems and services; (iii) the ability to restore the availability of and access to Company Personal Data in a timely manner in the event of a Data Security Incident (as defined below); and (iv) a process for regularly testing, assessing and evaluating the effectiveness of Security Controls. The Parties shall monitor compliance with these measures in accordance with their respective internal information security programs. Vendor shall, taking into account the nature of processing and the information available to Vendor, assist Company in meeting Company's obligations in relation to the security of processing Company Personal Data. Vendor shall, at a minimum, implement and maintain the security measures specified in the following:

6.1.1 **Physical Security**. Vendor shall maintain reasonable and sufficient physical barriers and controls to prevent unauthorized physical access to Company Personal Data or compromise of Company Personal Data by human or environmental causes

6.1.2 **Access Controls.** Vendor shall limit access to Company Personal Data to the minimum number of its Personnel who require such access in order for Vendor to perform the Services, ensure that only those Personnel who are specifically authorized to gain access to the Company Personal Data gain such access, and shall take all reasonable steps to prevent unauthorized access to, or destruction, alteration or loss of, any Company Personal Data. This includes password requirements at least as stringent as those in the then-current NIST guidelines.

6.1.3 **Technical Controls**. Vendor agrees to maintain a secure Processing environment for Company Personal Data. This includes timely application of anti-virus updates, system patches, fixes and updates to all operating systems and applications, enforced use of complex and long (at least 12 character) passwords, use of multifactor authentication on at least all internet-facing systems (including third-party systems), implementation of firewalls and other similar measures designed to ensure the confidentiality, integrity, and availability of Company Personal Data. Vendor further agrees that any and all Company Personal Data shall be encrypted at all times in transit and at rest, including, that all Company Personal Data stored on any portable or laptop computing device or any portable storage medium shall be encrypted and that any Company Personal Data stored as part of Vendor's designated backup and recovery processes shall also be in encrypted form, using a commercially supported encryption solution. Encryption solutions shall be deployed with no less than a 128-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption. Secure email (SMTP/TLS) must be enabled for all Vendor's domains.

6.1.4 **Business Continuity.** Vendor agrees to maintain a sufficient business continuity plan so that Company Personal Data is protected and in the event of a disruption to, or loss of

data or Service, delivery of Services and access to Company Personal Data are restored without more than de minimis adverse impact to the Services or Company Personal Data and continue at the applicable service levels. Such a plan must be reviewed and approved by management and regularly tested (no less frequent than annually). The plan and results or evidence of its testing must be available to Company for review.

6.2 **Data Security Incident Management and Notification.** Vendor shall maintain security incident management policies and procedures, and if at any time Vendor determines that any individual or entity has attempted to circumvent or has circumvented the security of any computer, system, or device containing Company Personal Data, or that there has been an actual or potential Security Breach (each an "**Incident**"), Vendor shall: (i) immediately terminate any applicable access and notify Company in writing of such Incident (in no event more than twenty-four (24) hours after first becoming aware of the Incident); (ii) promptly, and in full cooperation with Company, investigate and take steps to remediate the Incident, including restoring security, restoring or reconstructing Company Personal Data from backups, mitigating adverse effects of the Incident, and promptly providing information reasonably requested by Company; (iii) provide access to its premises, books, logs, and records to the forensic and other auditors, as determined by Company, to the extent necessary or appropriate to perform a thorough security review and to validate Vendor's compliance with Data Protection Laws and this DPA, and (iv) assist Company with respect to documentation of such Incident.

6.2.1 The notices provided for in this section shall be made to: Bill.Charles@emeraldx.com which may be updated by Company in writing (including by adding additional required notifications, whether telephonic, electronic, or otherwise). Such notices shall contain, to the extent reasonably known: (i) a description of the nature of the breach or Incident, including where possible or applicable, the categories, locations, and approximate number of Data Subjects and third parties concerned and the categories and approximate number of Company Personal Data records concerned; (ii) the name and contact details of the data protection officer, or other contact point where more information can be obtained by Company or third parties; (iii) a description of the likely consequences of the breach or Incident; and (iv) a description of the measures taken or proposed to be taken to address the breach or Incident, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide the foregoing information at the same time, the information may be provided in phases without undue further delay.

6.2.2 Vendor shall be responsible for all damages, costs, fees, losses and other liabilities (whether direct, indirect, special, consequential, or otherwise, including any incurred in enforcement of this provision), incurred by Company with respect to an Incident, breach of this DPA, or violation of Data Protection Laws, and remedy any harm or potential harm caused thereby, including: costs of investigation, third party claims, notifying individuals, entities, or governmental bodies; establishment of call/response centers; and the provision of credit monitoring and/or identity theft protection services to affected individuals (each a "Remedial Action").

6.2.3 In the event of an Incident, Vendor shall not, without Company's written consent, notify any third party regarding an Incident or violation of Data Protection Laws, and agrees that Company has the sole right to determine whether to notify Data Subjects and or Regulatory Authorities as required by Data Protection Laws, and Vendor, taking into account the nature of processing and the information available to Vendor, shall assist Company in relation to such notification obligations and other Remedial Action. Nothing

in this DPA shall be construed to require Vendor to violate, or delay compliance with, any legal obligation it may have with respect to an Incident.

7. INFORMATION PROVISION AND COOPERATION

7.1 **Demonstration of Vendor's Compliance.** Vendor shall, upon Company's reasonable request and to the extent required by Data Protection Laws, make available to Company all information in Vendor's possession necessary to demonstrate Vendor's compliance with its obligations under Data Protection Laws.

7.2 **Audits and Assessments.**

7.2.1 Vendor shall reasonably cooperate with Company in relation to any audit of Vendor reasonably necessary to enable Company to comply with its obligations under Data Protection Laws ("Audit"), and shall seek the equivalent cooperation from relevant Subprocessors. Any Audit shall be: (i) conducted by Company or an independent third party who has signed a nondisclosure agreement; and (ii) subject to the confidentiality obligations set forth in the Agreement. Company shall use reasonable endeavours to minimize any disruption caused to the Vendor's business activities as a result of an Audit. Audits shall take place no more than once in any calendar year unless and to the extent that Company (acting reasonably and in good faith) has reasonable grounds to suspect a Data Security Incident or any material breach of this DPA by Vendor.

7.2.2 To the extent permitted by Data Protection Laws, Vendor may, with Company's consent and as an alternative to the requirements set forth in Section 7.1, arrange for a qualified and independent assessor to conduct an assessment of Vendor's policies and technical and organizational measures in support of Vendor's obligations under Data Protection Laws, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Such assessment shall be conducted at least annually and at Vendor's expense. Vendor shall provide a report of such assessment to Company upon request ("Assessment Report").

7.2.3 Any Assessment Report or information disclosed in connection with an Audit shall be the Confidential Information of Vendor and/or the applicable Vendor Affiliate (and/or Subprocessor, as the case may be).

7.3 **Data Protection Assessments.** Upon Company's request and to the extent required under Data Protection Laws, Vendor shall provide Company with the necessary information and with reasonable cooperation and assistance needed to fulfill Company's obligation to carry out a Data Protection Assessment related to Company's use of the Services, to the extent that Company does not otherwise have access to the relevant information and that such information is reasonably available to Vendor. To the extent required under the GDPR or UK GDPR, Vendor shall provide reasonable assistance to Company in its cooperation or prior consultation with a Regulatory Authority in the performance of its tasks relating to this Section 7.

7.4 If, as a result of any Audit or Data Protection Assessment, Company deems Vendor's security measures insufficient, then, within five (5) business days after the date Company raises its security concerns, a senior Vendor technology executive shall meet with a representative of Company to discuss the matter. If the Assessment Report in its final and issued version contains a qualified opinion relating to security matters including risks to Vendor's computer systems and physical facilities which could result in the unauthorized destruction, loss, alteration of or access

to Company Personal Data, or the Services being materially affected, then, within five (5) business days after Vendor receipt of the Assessment Report, Vendor shall, at its own expense, promptly take actions to address the matters raised by the qualification so that the cause of the qualified opinion may be resolved and, after consultation with Company, reduce any risk to Company Personal Data

7.5 If Vendor or any of its systems or processes (i) fail to comply with any provision of this Section 7 or (ii) have, or are subject to, an Incident (whether or not impacting Company Personal Data), in addition to Vendor's other obligations, Vendor shall: (i) promptly perform a root cause analysis to identify the cause of the failure; (ii) provide to Company for approval Vendor's plan for remedying such failure; and (iii) upon Company's approval, implement the plan and remedy the failure. Without limitation of the foregoing, if Service Provider fails to take the actions set forth in Section 7.4 within fifteen (15) days after the date set forth for such actions, Company may immediately terminate the Agreement, in whole or in part, for cause and material breach, and at Company's option, with or without any cure period.

8. RETURN AND DELETION OF VENDOR DATA

9. Upon the termination or expiration of the Agreement, Vendor shall return or destroy all Company Personal Data to Company and/or at Company's request delete the same from its systems as well as any copies of the same within 60 days. Vendor shall certify destruction of the Company Personal Data in writing to Company. Any Company Personal Data retained beyond termination or expiration (such as where required by applicable law) shall remain subject to this DPA until returned or destroyed.

2. TRANSFER MECHANISMS FOR CROSS-BORDER DATA TRANSFERS

9.1 **Transfers of EEA, Swiss, or UK Personal Data.** If the Processing of Company Personal Data includes transfers from the EEA, Switzerland, or the United Kingdom to countries which are deemed to provide inadequate levels of data protection ("Other Countries"), if required by Data Protection Laws, the Parties shall: (i) execute the model clauses adopted by the relevant data protection authorities of the European Commission or the UK Secretary of State as set forth in this Section 9 (if applicable); or (ii) comply with any of the other mechanisms provided for under Data Protection Laws for transferring Company Personal Data to such Other Countries. Additional information required by the Standard Contractual Clauses is set forth in Exhibit 1.

9.2 **EU SCCs Modules.** The Parties agree that for transfers of Company Personal Data from the European Economic Area ("EEA"), the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "**EU SCCs**"), as annexed to Commission Implementing Decision 2021/914, are hereby incorporated by reference into this DPA as follows:

a. Where Vendor Processes Personal Data as a Controller pursuant to the terms of the Agreement, Vendor and its relevant Affiliates are located in non-adequacy approved third countries, and Company and its relevant Affiliates are established in the EEA or are otherwise transferring the Personal Data of EEA Data Subjects (either directly or via onward transfer); Module 1: Transfer controller to controller, Clauses 1 to 8, and 10 to 18 apply.

b. Where Vendor Processes Personal Data as a Processor for Company pursuant to the terms of the Agreement, Vendor and its relevant Subprocessor Affiliates are located in non-adequacy approved third countries, and Company and its relevant Affiliates are

established in the EEA or are otherwise transferring the Personal Data of EEA Data Subjects (either directly or via onward transfer); Module 2: Transfer controller to processor, Clauses 1 to 18 apply.

c. Where Company Processes Personal Data as a Processor under the instructions of a third-party Controller, Vendor Processes Personal Data as a Subprocessor for Company pursuant to the terms of the Agreement, Vendor and its relevant Subprocessor Affiliates are located in non-adequacy approved third countries, and Company and its relevant Affiliates are established in the EEA or are otherwise transferring the Personal Data of EEA Data Subjects (either directly or via onward transfer); Module 3: Transfer processor to processor, Clauses 1 to 18 apply.

d. Where Vendor Processes Personal Data as a Processor for Company pursuant to the terms of the Agreement, Vendor and its relevant Subprocessor Affiliates are located in the EEA or are otherwise transferring the Personal Data of EEA Data Subjects (either directly or via onward transfer), and Company and its relevant Affiliates are located in non-adequacy approved third countries; Module 4: Transfer processor to controller, Clauses 1 to 8, 10 to 12, and 14 to 18 apply.

9.3 **EU SCCs Optional Provisions.** In addition to Section 9.2, where the EU SCCs identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

a. In Clause 7 (Docking Clause) (Modules 1, 2, 3, or 4) – the Optional provision shall NOT apply;

b. In Clause 9(a) (Use of sub-processors) (Module 2 or 3) – Option 1 shall apply (and the parties shall follow the process and timings agreed in the DPA to appoint sub-processors);

c. In Clause 11(a) (Redress) (Module 1, 2, 3, or 4) – the Optional provision shall NOT apply;

d. In Clause 17 (Governing Law) (Module 1, 2, 3, or 4) – Option 1 shall apply, and the courts of Ireland shall govern; and

e. In Clause 18 (Choice of forum and jurisdiction) (Module 1, 2, 3, or 4) – the courts of Ireland shall have jurisdiction.

9.4 **UK Model Clauses.** The Parties agree that for transfers of Company Personal Data from the United Kingdom, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK ICO under S119A(1) Data Protection Act 2018 and in force March 21, 2022 (the "**UK Addendum**"), shall apply. The start date in Table 1 of the UK Addendum shall be the date that the Parties have executed Exhibit 1. The selection of modules and optional clauses shall be as described in Sections 9.2 and 9.3 above, subject to any revisions or amendments required by the UK Addendum. All other information required by Tables 1-3 is set forth in Exhibit 1. For the purposes of Table 4, the parties agree that the Exporter may end the UK Addendum as set out in Section 19.

9.5 **Swiss Data Transfers.** The Parties agree that for transfers of Company Personal Data from Switzerland, the terms of the EU SCCs shall be amended and supplemented as specified by the

relevant guidance of the Swiss Federal Data Protection and Information Commissioner, and the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

10. DEIDENTIFIED DATA

1. To the extent that Vendor receives Deidentified Data from Company or processes Company Personal Data in such a way that it becomes Deidentified Data, Vendor shall: (i) take reasonable measures to ensure that the Deidentified Data cannot be associated with an individual or household; (ii) publicly commit to maintain and use the Deidentified Data only in a de-identified fashion and not attempt to re-identify the data, unless otherwise permitted by Data Protection Laws; and (iii) contractually obligate any recipients of the Deidentified Data, including any Subprocessors, to comply with the requirements of this Section 10.

11. MARKETING

3. Vendor agrees to comply with Data Protection Laws with respect to marketing and direct marketing communications and the Processing of Customer Personal Data therefor. Vendor shall not use any Company Personal Data for marketing unless expressly agreed by Company in each instance.

12. NO LIMITATION OF LIABILITY

4. NO PROVISION OF THE AGREEMENT OR THIS DPA SHALL OPERATE TO EXCLUDE OR LIMIT VENDOR'S LOSSES OR LIABILITY UNDER THIS DPA, INCLUDING WITH RESPECT TO LIABILITY RELATING TO AN INCIDENT, BREACH OF THIS DPA, OR ALLEGED OR ACTUAL VIOLATION OF DATA PROTECTION LAWS.

13. INDEMNIFICATION.

5. Vendor shall indemnify, defend, and hold harmless Company and its Affiliates, and each of their officers, directors, parents, shareholders, employees, and agents from and against all claims, demands, suits, causes of action, awards, judgments and liabilities, including reasonable attorneys' fees and costs (collectively "Claims") arising out of or alleged to have arisen out of (i) Vendor's breach of its obligations under this DPA (including any purpose or use restrictions relating to Company Personal Information) as may be contained in the Agreement, or (ii) any security incident, or (iii) any breach by Vendor's employees, contractors, Subprocessors, and any Downstream Participants under this DPA, or (iv) any violation of Data Protection Laws.

1. EQUITABLE RELIEF

1. Vendor agrees that a breach or threatened breach of this Addendum by Vendor or its agents, Subprocessors, contractors or Subprocessors may cause irreparable harm to Company such that monetary damages may not provide an adequate remedy. Vendor accordingly agrees that Company may seek injunctive relief to prevent or remedy such breach or threatened breach without requirement of bond or notice.

2. GOVERNING LAW

2. Without prejudice to the relevant provisions of any applicable transfer mechanisms identified in Section 9 of this DPA, including the EU SCCs and UK Addendum, the Parties to this

DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and is governed by the laws of the country or territory stipulated for this purpose in the Agreement.

3. BREACH AND TERMINATION

6. Any breach of this DPA shall be deemed a material breach of the Agreement, and Company may immediately terminate the Agreement, in whole or in part, for cause and material breach, and at Company's option, with or without any cure period.

4. CHANGE IN DATA PROTECTION LAWS

1. In the event of any change to or new Data Protection Law(s), Company shall have the right, upon written notice to Vendor, to make any amendments or revisions to the Agreement and/or this DPA as it reasonably determines are necessary or appropriate to address the requirements of such Data Protection Law(s). Such amendments shall become effective thirty (30) days after such written notice unless Company receives a written response from Vendor prior to such date setting forth (i) its objection to the amendment and (ii) the specific bases for such objection (collectively an "Objection"). In the event of an Objection, the Parties shall promptly discuss the objection and negotiate in good faith with a view to agreeing and implementing alterative amendments to address the requirements of the Data Protection Law(s) as soon as reasonably practicable; provided, however, that in the event the Parties are not able to agree to amendments before the earlier of (x) the effective date of such Data Protection Law(s) or (y) such earlier date as Company reasonably determines is necessary in order for it to find an alternative provider before the effective date of such Data Protection Law(s), Company may terminate the Agreement by written notice (which notice shall specify the termination date) without penalty, and shall receive a refund of all amounts paid for Services not delivered prior to the effective date of such termination.

5. SEVERABILITY

2. If any term of this DPA is determined by a court of competent jurisdiction to be, to any extent, illegal, otherwise invalid, or incapable of being enforced, such a term shall be excluded to the extent of such invalidity or unenforceability; all other terms herein shall remain in full force and effect; and, to the extent permitted and possible, the invalid or unenforceable term shall be deemed replaced by a term that is valid and enforceable and that comes closest to expressing the insertion of such invalid or unenforceable term.

6. SURVIVAL

7. The terms and conditions of this DPA, and Vendor's obligations with respect to Company Personal Data, shall survive the termination or expiration of this DPA for so long as Vendor retains any Company Personal Data.