ELLUCIAN PARTNER DATA PROTECTION ADDENDUM (DPA) TERMS

(Version 2: April 1st, 2024)

These Data Protection Addendum ("DPA") Terms form part of the relevant Partner Agreement fully executed between the relevant Ellucian signatory (on behalf of itself and its affiliate companies) (collectively, "**Ellucian**"), and relevant Ellucian partner (the "**Partner**") that references this DPA and incorporates it therein (as amended) ("**Agreement**"). This DPA is effective as of the date of later signature of the Agreement or such other effective date specified in the fully executed Agreement (the "**DPA Effective Date**") The parties agree that this DPA is in addition to and not in lieu of any other provisions of the Agreement. Capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the Agreement and this DPA, the order of precedence shall be as specified in the fully executed Agreement (or, of no order of preference is specified, this DPA shall control).

PART 1: DEFINITIONS

The defined terms have the meaning set forth below whether or not such defined terms begin with capital letters elsewhere in this DPA.

1.1 "Applicable Data Protection Laws" means the relevant data protection and privacy law(s) to which Ellucian and/or the Partner is subject, as applicable, including (without limitation): (i) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("the

GDPR"); (ii) the California Privacy Rights Act and California Consumer Privacy Act; (iii) the Virginia Consumer Data Protection Act; (iv) the Colorado Privacy Act; (v) the Utah Privacy Act; (vi) Senate Bill 6, the Connecticut Data Privacy Act (vii) the UK General Data Protection Regulation (as defined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) (the "UK GDPR"); and, (viii) any other data protection legislation that applies to the parties from time to time.

1.2 "Confidential Information" has the meaning set forth in the Agreement. In addition to any description of Confidential Information in the Agreement, Confidential Information shall include, but not be limted to, (a) Information Systems user authentication secrets or verifiers, such as passwords, cryptographic privacy keys, digital certifications, or user login or application session tokens; or (b information that might otherwise need to be strictly controlled or protected due to its business sensitivity, criticality, or value, or due to associate risk factors that may result in severe risk to Discloser.

1.3 "Discloser" shall be as defined in the Agreement (or, if not defined in the Agreement shall mean the Party providing its Protected Data to the Recipient).

1.4 "Information Systems" means computing hardware, software and media components.

1.5 "Personal Data" means any information relating to an identified or identifiable natural person, or any other information regulated under any Applicable Data Protection Laws.

1.6 "Process" or "Processing" means any operation or set of operations which is performed on Protected Data or on sets of Protected 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 deletion.

1.7 "Protected Data" means Confidential Information and Personal Data, collectively.

1.8 "Recipient" shall be as defined in the Agreement (or, if not defined in the Agreement shall mean the Party receiving Protected Data of the Discloser).

1.9 "Security Incident" means any suspected (with a reasonable degree of certainty) or actual unauthorized access to Discloser's Information Systems; access, unauthorized or unplanned disruption of service due to malicious actor(s); unauthorized modification of systems; or the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed.

1.10 "Controller" and "Processor" shall have the meanings given to them by applicable Data Protection Law.

PART 2: DPA TERMS

2 INTRODUCTION AND STATUS OF THE PARTIES

2.1 The parties acknowledge and agree that any disclosure of Protected Data, will in no way be construed to be an assignment, transfer, or conveyance of title to or ownership rights in such Protected Data.

2.2 The terms of this DPA apply to the parties if and to the extent applicable based on the activities under the Agreement. Each party may be both a "Discloser" (as defined in the Agreement) and a "Recipient" (as defined in the Agreement) of Protected Data (as defined below). In the Processing of Personal Data, the parties acknowledge that the Discloser shall be the Controller of the Personal Data or a Processor of its customers' Personal Data, and the Recipient is the Processor or Subprocessor, respectively.

2.3 Discloser will provide Protected Data to Recipient as reasonably required for Recipient to comply with its responsibilities under the Agreement.

3 PROCESSING REQUIREMENTS

3.1 Details of Processing. The type of Personal Data Processed pursuant to this DPA as well as the subject matter, nature and purpose of the Processing, the Data Subjects involved, location(s) and retention period are as described in the Agreement.

3.2 Instructions. Recipient will Process Personal Data only to the extent required for Recipient to carry out its responsibilities under the Agreement, and Recipient will not retain, use or disclose Personal Data for any purpose other than for the specific purpose of performing the services specified in the Agreement. Recipient shall comply with all lawful instructions provided by Discloser to Recipient during the term of the Agreement regarding Protected Data, and shall only Process Protected Data in accordance with such instructions. Recipient shall also promptly inform Discloser if, in Recipient's reasonable opinion at such time, an instruction infringes any Applicable Data Protection Laws. Recipient shall not retain, use, or disclose the Protected Data other than for the direct business relationship between Recipient and Discloser.

3.3 Restrictions on Use. Recipient will not sell, rent, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to another business or third party for monetary or other valuable consideration. Recipient will not transfer or otherwise make available Personal Data to third parties for cross-context behavioral advertising purposes. Recipient will not re-identify or attempt to re-identify data that has been de-identified, and will take reasonable measures to prevent such re-identification. Recipient will not combine Personal Data with data from other third-party sources.

3.4 Confidentiality. Recipient shall treat all Protected Data as strictly confidential. Recipient shall take appropriate steps so that only authorized personnel who are subject to binding obligations of confidentiality, either contractual or statutory, will have access to the Protected Data. Termination or expiration of this DPA shall not discharge Recipient from its confidentiality obligations.

3.5 Data Subject Rights Requests. Recipient will promptly provide such information and assistance to Discloser in responding to requests from individuals related to Personal Data about them, including but not limited to data subject requests and any subsequent appeals. Recipient shall ensure it implements and maintains appropriate technical tools and organisational meansures to ensure that Discloser is able to comply with its obligations under Applicable Data Protection Laws. In the event that Recipient receives a request from an individual regarding Personal Data provided to Recipient by Discloser, Recipient will promptly notify Discloser of such request and will not respond to such request without the prior written consent of

Discloser's data protection officer (or, if none, Discloser's responsible person), except where required by applicable law.

3.6 Assistance. Recipient will provide such information and assistance as Discloser may reasonable request in order for Discloser to comply with its obligations under Applicable Data Protection Laws including Discloser's obligations to perform data protection impact assessments.

3.7 Return and Destruction. Upon termination of the Services, Recipient will, in accordance with Discloser's instructions, return or destroy all Personal Data.

4 USE OF THIRD PARTIES

4.1 Recipient will limit access to the Personal Data to its employees, agents, and subcontractors (including affiliates) who have a need to access such Personal Data to perform Recipient's obligations under the Agreement. Discloser agrees that Recipient may use subcontractors to fulfill its obligations under this DPA and the Agreement so long as Recipient's relationship with such subcontractors complies with 4.2 below. Ellucian's list of Subprocessors shall include all relevant Ellucian Affiliates and any relevant sub-contractors used by Ellucian from time to time including without limitation its hosting provider(s) and may be more particularly described in a published list of Subprocessors that Ellucian makes available on its website (or via such other accessible location) from time to time and/or may be more particularly described in the Agreement. Unless agreed otherwise, Partner's list of Subprocessors must be referenced in the Agreement. Recipient shall inform Discloser of any changes to the subcontractor list prior to permitting any new Subprocessor to process Personal Data. Discloser will have 30 days from receipt of Recipient's notice to object to such changes. If Discloser fails to object to such changes within the allotted time frame, such changes shall be deemed accepted. If Discloser timely sends Recipient a written objection notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Discloser's objection. In the absence of a resolution, each Party may terminate the portion of the Services which cannot be provided without the subcontractor.

4.2 Recipient will require that its subcontractors who have access to Personal Data agree to abide by substantially similar restrictions and conditions that apply to Recipient with regard to such Personal Data.

4.3 Recipient will remain fully responsible for any subprocessor's failure to fulfil their data protection obligations in accordance with the requirements of this DPA.

5. DATA PRODUCTION REQUESTS. If Recipient or any Approved Sub-Processors receives a mandatory request, order, demand, notice or direction from any parent, holding company or any government department, body or agency, public authority to disclose any Personal Data whether or not in writing or identifying any specific data subject(s) ("Data Production Request"), it shall deal with the Data Production Request in accordance with the following terms:

5.1 No Personal Data shall be disclosed in response to a Data Protection Request unless either the Recipient or the Approved Sub-Processor is under a compelling statutory obligation to make such disclosure, or (having regard to the circumstances and the rights and freedoms of any affected data subjects) there is an imminent risk of serious harm that merits disclosure in any event (for example, to protect individuals' vital interests);

5.2 Where disclosure of the Personal Data is required in response to a Data Production Request, the Recipient shall notify Discloser in writing in advance (setting out all relevant details) and shall, thereafter, provide all reasonable cooperation and assistance, including assistance with any application, injunction, order or request to prevent (or where that is not possible, to delay) the disclosure of any Personal Data;

5.3 Except where the imminent risk of serious harm prohibits prior notification, the Recipient shall notify and consult with the relevant supervisory authority in respect of the Data Production Request, and at all times afterwards cooperate with the supervisory authority and Discloser to deal with the Data Production Request.

6. SECURITY. Recipient will maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as set forth in the Description of Technical and Organizational Measures set forth in Appendix 1.

7. INCIDENT RESPONSE AND NOTIFICATION. Recipient will promptly, and without undue delay, notify the Discloser's designated security contact in writing of any Security Incidents as described below. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. Recipient will promptly respond to requests for information from Ellucian related to any actual or suspected Security Incidents. Recipient shall reasonably cooperate with Discloser in investigating and resolving Security Incidents, including providing access to incident logs, analysis, and staff. Recipient shall notify Discloser immediately of any legal actions or investigations related to Security Incidents affecting Discloser. Recipient will reasonably cooperate with Discloser with regard to any notices required by applicable law to individuals who may be adversely affected by a Security Incident and, if required, to the relevant supervisory authorities. The contact information for Ellucian is securitynotification@ellucian.com and the contact details for the Partner shall be the latest contact details that Ellucian has on file for the Partner from time to time.

8. COMPLIANCE AND RIGHT TO AUDIT.

8.1 Upon reasonable prior written notice from Discloser, Recipient shall make available to Discloser such information as is strictly necessary to demonstrate its compliance with this DPA and Applicable Data Protection Laws and shall, to the extent required by Applicable Data Protection Laws, allow for and contribute to audits, including inspections, conducted by Discloser or another auditor mandated by Discloser. Any costs arising in connection with Recipient's obligations under this clause shall be promptly reimbursed to Recipient by the Discloser upon reasonable request.

8.2 Recipient uses independent third party auditors at its selection and expense to verify the adequacy of its security measures for Cloud Software and Cloud Services. Discloser agrees that Recipient will satisfy Discloser's right of audit and inspection by providing, no more than once per calendar year upon Discloser's written request and subject to Discloser executing a non-disclosure agreement: (i) a copy of the most recent independent security attestation report associated with the provision of Cloud Software or Cloud Services as applicable, and (ii) a copy of Recipient's then-current information security policies and standards that relate to security controls associated with the Cloud Software or Cloud Services as applicable.

8.3 To the extent Discloser's audit requirements under the Data Protection Laws cannot reasonably be satisfied through the security attestation report, documentation or compliance information Recipient makes generally available to its customers, Discloser shall notify Recipient in writing and the Parties will engage in discussions to determine reasonable and appropriate means to satisfy such requirements..

9. **INTERNATIONAL TRANSFER OF PERSONAL DATA.** Except as provided in Appendix 2 to this Agreement or in documented instructions from Discloser, any international transfer of Discloser Personal Data by Recipient (or any Approved Sub-Processors) is prohibited.

10. **AMENDMENTS**. In the event that applicable data protection regulations require additional data protection language to be added to this DPA, Ellucian and Partner agree to negotiate in good faith to update the data protection terms between the parties accordingly.

11. **ACKNOWLEDGMENT.** For the avoidance of doubt, each party is a Controller of its employee data and any/or other data that it collects directly from a data subject (usage data) and/or other data for which it determines the purposes and means of the processing (e.g. in relation to events that the party operates). Each party is a Processor of its customer data. In the event that the Parties rely on the EU Standard Contractual Clauses to process, or permit the processing, of personal data internationally, which Module shall apply shall depend upon which party is the prime contractor and which party is the sub-contractor in each case and the type of personal data that is being processed in each case. Where processing the other party's employee personal data, such as business contact information, for its own business purposes, such as for communication or billing purposes, the party sharing its employees' personal data is a controller and the party receiving the other party's employees personal data is also a controller for those purposes. Where a party is a prime contractor it will either be a Processor (depending on the type of data). Where a party is a sub-contractor it shall be a Processor. The Modules are as follows: Module One (Controller to Controller), Module Two (Controller to Processor), Module Three (Processor to Processor) and Module Four (Processor to Controller).

APPENDIX 1

TECHNICAL AND ORGANIZATIONAL MEASURES

1. Recipient shall promptly report activity that may reasonably lead to physical harm to individuals, loss of information (including, but not limited to Personal Data) or damage to facilities or equipment to Discloser.

2. **INFORMATION SECURITY PROGRAM.**

2.1 Without limiting Recipient's obligation of confidentiality in the Agreement and as further described herein, Recipient will be responsible for establishing and maintaining an information security program that is designed to:

a) ensure the security and confidentiality of Protected Data;

b) protect against any anticipated threats or hazards to the security or integrity of the Protected Data;
c) protect against unauthorized access to or use of the Protected Data;
d) ensure the proper disposal of Protected Data, as further defined herein; and,
e) ensure that all subcontractors of Recipient who have access to Discloser's Protected Data or access to Discloser's Information Systems used to Process Discloser Protected Data, if any, are approved in writing by Discloser and comply with all of the foregoing.

2.2 Recipient will designate an individual to be responsible for the information security program. Such individual will respond to Discloser inquiries regarding computer security and to be responsible for notifying Discloser-designated contact(s) if a Security Incident occurs, as further described herein.

2.3 The information security program will be modeled after the requirements of ISO 27001 or another globally-recognized information security standard and will be compliant with all applicable legal and regulatory requirements for data protection and privacy of Protected Data.

3. DISCLOSER DATA HANDLING PROCEDURES.

3.1 Protected Data must be physically and logically secured when not in use and securely disposed of upon Discloser's request or the termination or expiration of the Agreement. Destruction of Protected Data on electronic media shall be according to Section 4 below.

3.2 Destruction of Protected Data on paper shall be by shredding by Recipient or a third party that provides secure document destruction services. Upon request, Recipient will provide information to Discloser regarding procedures for secure destruction of Protected Data.

4. ERASURE OF INFORMATION AND DESTRUCTION OF ELECTRONIC STORAGE MEDIA. All electronic storage media containing Protected Data must be wiped or degaussed for physical destruction or disposal in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization or other methods authorized by Discloser's Information Security team. Recipient must maintain documented evidence of data erasure and destruction. This evidence must be available for review at the request of Discloser.

5. SYSTEM DEVELOPMENT & MAINTENANCE. The following shall apply if the Recipient is utilizing, developing and/or providing software to Discloser (including as a service).

5.1 Recipient shall not release or provide software (including as a service) to Discloser with newly introduced Critical or High vulnerabilities as defined by the Forum of Incident Response and Security Teams Common Vulnerability Scoring System (FIRST CVSS) qualitative rating scale.

5.2 Where software or software services are developed or provided by the Recipient and utilized by Discloser, the relevant software will be regularly scanned by Recipient for vulnerabilities and the Recipient shall notify Discloser of Critical or High vulnerabilities with a known active exploit.

5.3 The notice shall include a summary of the identified vulnerability and a description of the remediation measures to be taken by the Recipient to remediate or mitigate the identified vulnerability.

5.4 Without prejudice to the foregoing, Recipient shall remediate or mitigate any identified vulnerabilities within a timeframe that is, at a minimum, consistent with an industry standard vulnerability remediation framework and upon request the Recipient shall provide notification of remediation or mitigation for those identified Critical or High vulnerabilities to Discloser.

6. **PERSONNEL SCREENING.** Recipient will verify the suitability of on all Recipient personnel and contractors including temporary and non-employee personnel who will have access to Protected Data or directly support such access or the environment storing or Processing that Protected Data during work they perform for Discloser pursuant to the Agreement that includes verifying at the greater of the past 7 years of employment or the previous 3 employers, verifying the highest level of education attained by an applicant, and validating immigration/right to work status of each individual. Recipient will not assign any person to the Agreement who has not been screened, or whose screening according to these standards has revealed that the person does not meet these standards. Where such checks are prohibited by applicable law, Recipient will notify Discloser in advance that a particular individual has not been screened under this Section prior to that individual performing work for Discloser. If Recipient contracts, for any services, with a third party that needs to be allowed or requires access to Protected Data, the third party will undergo the same screening as performed on Recipient personnel and contractors under this Section.

7. **TRAINING.** Recipient must conduct formal security awareness training for all personnel and contractors as soon as reasonably practicable after the time of hiring or prior to being appointed to work on Personal Data and annually recertified thereafter. Documentation of Security Awareness Training must be retained by Recipient, confirming that this training and subsequent annual recertification have been completed, and available for review by Discloser.

8. **NETWORK AND COMMUNICATIONS SECURITY.**

8.1 All Recipient connectivity to Discloser Information Systems shall be through remote access mechanisms approved by Discloser Global Information Security.

8.2 Recipient will not transmit any unencrypted Protected Data over the internet and will not store any Protected Data on any mobile device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software or other safeguards approved by Discloser. Notwithstanding the foregoing, it is acceptable to transmit the sub-set of Personal Data that consists only of business contact details for individuals involved in the business relationship without using encryption.

8.3 Recipient will not access, and will not permit unauthorized persons or entities to access, Discloser computing systems and/or networks without Discloser's express written authorization and any such actual or attempted access will be consistent with any such authorization.

8.4 Recipient will take appropriate measures to ensure that Recipient's systems connecting to Discloser's systems and anything provided to Discloser through such systems does not contain any malicious code designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment to the operation of Discloser's systems, and Recipient will promptly notify Discloser of any material vulnerabilities that could impact Discloser.

9. PHYSICAL SECURITY. All Protected Data must be contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by Recipient. Protected Data must be encrypted in storage and in transit, provided, however, it is acceptable to transmit the sub-set of Personal Data that consists only of business contact details for individuals involved in the business relationship without using encryption.

10. BUSINESS CONTINUITY

a) Recipient must maintain a formal Business Continuity Plan (BCP), ensuring the continuous secure provisioning of the services and solutions in-scope of this agreement.
b) The BCP must include recovery strategies, recovery time objectives, data backup policies, and communication procedures.
c) Recipient shall periodically test, update, and revise the BCP, at least annually, and provide evidence of such activities, no more than once annually, and only upon request.
d) Any significant changes in Recipient's operations that might impact the BCP must be promptly communicated to Discloser.

11. CHANGE MANAGEMENT

Recipient must maintain a formal change management program for the services and solutions in-scope of this agreement.

a) Changes with potential to impact the services and solutions provided to Discloser must be communicated in advance and in writing (email to an agreed upon address is acceptable).
b) Changes that result in Critical or High risk to the services and solutions provided to Discloser, or the data Discloser entrusts to these services or solutions, must be communicated without undue delay in writing (email to an agreed upon address is acceptable).

12. THIRD PARTY RISK MANAGEMENT

a) Recipient is expected to manage risks associated with their own third-parties (including subcontractors) that may impact the in-scope services and solutions provided to Discloser or to the data Discloser entrusts to these services and solutions.
b) Recipient must evaluate the security risks associated with their third parties (including subcontractors), through security assessments and obtaining satisfactory assurances on data protection and privacy.
c) Recipient must notify Discloser of any changes or identified risks associated with their third-party relationships that might affect the services and solutions provided to Discloser.

13. INFORMATION SECURITY INCIDENT RESPONSE

a) Recipient must maintain a formal Incident Response Plan (IRP) to respond to information security incidents.
b) The IRP must be capable of swiftly isolating and addressing any security incident, potential or known breaches, minimizing damage, and restoring services to normal operation.

14. PENETRATION TESTING.

14.1 During Recipient's performance under the Agreement, Recipient will engage, at its own expense and at least one time per year, a reputable third party vendor that is in the business of performing penetration testing to perform penetration and vulnerability testing ("Penetration Tests") with respect to Recipient's systems containing and/or storing Protected Data. Without prejudice to any other terms of this DPA (including those relating to the identification of Critical and High vulnerabilities affecting any software or

software services that are developed or provided by the Recipient to Discloser and utilized by Discloser), Recipient will make available to Discloser, upon request, a summary of the Penetration Testing results and certify to Discloser the current state of remediation of all identified Critical level and High level security issues.

APPENDIX 2

INTERNATIONAL TRANSFERS

For the purposes of the performance of this DPA, the Recipient may only process, or permit the processing, of Personal Data internationally with prior written consent of Discloser, which has been granted subject to and in accordance with the terms of this DPA and under the following conditions:

1. TRANSFERS FROM THE EUROPEAN ECONOMIC AREA

1.1 The transfer of Personal Data regulated by the EU GDPR outside the European Economic Area ("EEA Personal Data") shall be permissible to any of Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom, and Uruguay pursuant to the European Commission's adequacy decisions for these jurisdictions together with any other countries the subject of subsequent European Commission adequacy decisions ("Adequate Countries").

1.2 The transfer of EEA Personal Data from the EEA to any other country excluding the EEA and Adequate Countries ("**Restricted Country**") shall only be permissible subject to one of the following appropriate safeguards being in place:

a) A legally binding and enforceable instrument between public authorities,
b) Binding corporate rules (BCRs),
c) Standard contractual clauses adopted by the local regulatory authority,
d) Standard contractual clauses adopted by a supervisory authority and approved by the local regulatory authority,
e) An approved code of conduct, or
f) An approved certification mechanism.

1.3 Where the Parties opt to use standard contractual clauses adopted by the local regulatory authority as the appropriate safeguard, the EEA Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and as available here https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914 (the "EEA SCCs") shall be incorporated into this DPA as follows:

a) Where Discloser and Recipient are both Data Controllers of the EEA Personal Data then Module One (Controller to controller transfers) shall apply, where Discloser is the Data Controller of the EEA Personal Data then Module Two (Controller to processor transfers) shall apply, where a Discloser Customer is the Data Controller then either Module 3 (Processor to processor transfers) shall apply (if

Recipient does not exercise controllership over the EEA Personal Data) or Module 4 (Processor to controller transfers) shall apply (if Recipient does exercise controllership over the EEA Personal Data), and, where both Discloser and a Discloser Customer exercise controllership over the EEA Personal Data then Module 2 shall apply but the Discloser Customer shall be entitled to enforce those rights conferred upon data controllers under the EEA SCCs directly against the Recipient as if it were a party to this DPA.

(i) Discloser or the relevant Discloser entity identified shall be the Data Exporter and Recipient shall be the Data Importer.

(ii) The content required for Annex I, II and III of the EEA SCCs shall correspond to the respective content in this DPA.

(iii) Clause 7 (docking clause) shall be omitted.

(iv) Clause 9 (Use of sub-processors): Option 2: General Written Authorization shall be selected, and the Sub-Processors authorized under this DPA have been authorized by Discloser with a notice period for replacement of 45 days;

(v) Clause 11 (Redress): the right to lodge a complaint with an independent dispute resolution body shall be omitted;

(vi) Clause 13 (Supervision): the Irish regulator shall be the competent supervisory authority;

(vii) Clause 17 (Governing Law): The EEA SCCs shall be governed by the laws of Ireland;

(viii) Clause 18 (Choice of Forum and Jurisdiction): disputes relating to the EEA SCCs shall governed by the laws of Ireland.

2. TRANSFERS FROM THE UK

2.1 The transfer of Personal Data regulated by the UK GDPR ("UK Personal Data") to any other country excluding a country or territory which benefits from a UK Adequacy decision ("UK Restricted Country") shall only be permissible under the terms of this clause 2, unless the Partner can evidence other appropriate safeguards deemed suitable under the UK GDPR.

2.2 All transfers of UK Personal Data to a UK Restricted Country shall be subject to the EEA SCCs in conjunction with the UK's International Data Transfer Addendum ("**UK Addendum**") available at https://ico.org.uk/media/for-organisations/documents/4019535/addendum-international-data-transfer.docx (collectively, the "**UK SCCs**"), which are hereby incorporated with the following clarifications:

a) The terms agreed for the EEA SCCs as set out above are agreed for the UK SCCs and deemed to be prepopulated into the UK Addendum.

b) The UK SCCs shall be governed by the laws of England and Wales.

c) The Mandatory Clauses of the UK Addendum shall automatically be incorporated into this DPA.

d) Table 4 of the UK Addendum "Ending this Addendum when the Approved Addendum Changes" shall have "neither party" selected.

3. TRANSFER RISK ASSESSMENTS

3.1 The Parties, in assessing the specific circumstances of the transfers of EEA and/or UK Personal Data to Restricted Countries, shall have due regard to the laws and practices in the countries of destination relevant to such transfer and, in particular, whether such laws and practices may undermine the protections afforded by the SCCs and/or UK SCCs (as applicable).

3.2 Recipient shall provide all information Discloser may reasonably require in connected with the completion of any transfer risk assessments and, in particular, Recipient shall conduct and keep up-to-date a risk assessment to assess the extent to which it (or any of its Approved Sub-Processors) may be subject to a Data Production Request and shall provide to Discloser such risk assessment, promptly following its written request.

3.3 Recipient warrants and represents that all information it provides pursuant to this clause 3 is accurate and complete and shall keep Discloser informed of any changes which may affect the accuracy of that information.