7250 Dallas Parkway, Suite 400,
Plano, TX 75024
+1 972 634 3390

DATA PROCESSING ADDENDUM

VERSION DATED: 13 FEBRUARY 2023

THIS DATA PROCESSING ADDENDUM ("**DPA**") to the Agreement is entered into as of the Addendum Effective Date by and between Cypher Learning Pty Ltd. if Customer is located in Australia; Cypher Learning QTSP LLC if Customer is located in Qatar; or Cypher Learning, Inc. if Customer is located in the United States (collectively "**Cypher Learning"** or "**Vendor**"); and the customer identified on the Order Form ("**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 Cypher Learning Subscription 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, where applicable, GDPR, APPs, Qatar Privacy Law and CCPA.

(d) "**APPs**" means the Australian Privacy Principles as implemented by the Privacy Act 1988 (Cth).

(e) "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (the "**CPRA**") and any binding regulations promulgated thereunder.

(f) "**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 Personal Data.

(g) "**Customer Personal Data**" means any Personal Data Processed by Vendor or its Sub-Processor on behalf of Customer to perform the Services under the Agreement (including, for the avoidance of doubt, any such Personal Data comprised within Customer Content).

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

(i) "**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.

(j) "**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.

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

(l) "**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.

(m) "**Personal Data**" means any information provided to Vendor by Customer that is protected as "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws, except that 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).

(n) "**Personal Data Breach**" means a breach of Vendor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised 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 Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

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

(p) "**Process**" and any inflection thereof means any operation or set of operations which is performed on Personal Data or on sets of 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, destruction, dissemination, blocking or anonymization.

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

(r) "**Qatar Privacy Law**" means Qatari Law No. 13 of 2016 (Personal Data Privacy Protection Law).

(s) "**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 "**EU 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.

(t) "**SCCs**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(u) "**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.

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

(w) "**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; (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office; and (iii) in the context of any other Applicable Data Protection Law, means the regulator of such Applicable Data Protection Law in that jurisdiction.

(x) "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "**UK Mandatory Clauses**").

1.2 Unless otherwise defined in this DPA, all capitalized terms in this DPA shall have the meaning given to them in the Agreement.

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 the DPA.

2.3 Annex 2 (European & Australian Annex) to this DPA applies only if and to the extent Vendor's Processing of Customer Personal Data under the Agreement is subject to either or both of the GDPR and the APPs.

2.4 Annex 3 (California 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 CCPA with respect to which Customer is a "business" (as defined in the CCPA).

2.5 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 for Processors under Applicable Data Protection Laws, and in such cases, only in respect of Processing of 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 instructions or as required or permitted by applicable laws and shall be considered a "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. 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 this DPA are integral to the Services and the business relationship between the Parties. Access to 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 take commercially reasonable steps to ascertain the reliability of any Vendor Personnel who Process Customer Personal Data and, where required by applicable laws, shall enter into written confidentiality agreements with all Vendor Personnel who Process Customer Personal Data that are not subject to professional or statutory obligations of confidentiality.

5. **SECURITY**

5.1 Vendor shall implement and maintain technical and organizational measures in relation to Customer Personal Data designed to protect Customer Personal Data against Personal Data Breaches as described in Annex 4 (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 Vendor, taking into account the nature of the Processing of Customer Personal Data, 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 on the written instructions of Customer or as required by Applicable Data Protection Laws.

6.3 Except to the extent prohibited by applicable law, Customer shall be fully responsible for all time spent by Vendor (at Vendor's then-current professional services rates) in Vendor's cooperation and assistance provided to Customer under this Section 6, and shall on demand reimburse Vendor any such costs incurred by Vendor.

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 Personal Data Processed by Vendor) 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 URL specified in Section 8.2.

8.2 Information about Sub-processors, including their functions and locations, is available at: https://www.cypherlearning.com/data-processing-addendum (as may be updated by Vendor from time to time) or such other website address as Vendor may provide to Customer from time to time (the "**Subprocessor 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.

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 Subprocessor 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, 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 Vendor, taking into account the nature of the Processing and the information available to 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 Personal 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, and 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 normal business hours; 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 Upon expiration or earlier termination of the Agreement, Vendor shall 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.

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 Union, 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 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 and permissions have been obtained from, Data Subjects and others as are required, including under Applicable Data Protection Laws, relating to the Processing by Vendor of Customer Personal Data.

11.3 Customer agrees that the Service, 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) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) biometric information; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) any payment card information subject to the Payment Card Industry Data Security Standard; or (i) any other information that falls within any special categories of personal data (as defined in GDPR or any other Applicable Data Protection Law) and/or data relating to criminal convictions and offences or related security measures (together, "**Restricted Data**").

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, 9, and 10.1 of this DPA, beyond providing self service features included as part of the Service.

12. **DEIDENTIFIED, ANONYMIZED, OR AGGREGATED DATA**

12.1 To the extent Vendor processes 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**

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) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the Agreement; **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**

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 Paragraph 2.3 of Annex 2 (European Annex).

15. **INCORPORATION AND PRECEDENCE**

15.1 This DPA is incorporated into and forms a binding and effective part of the Agreement automatically upon the Parties' entry into the Agreement, with effect on and 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.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Annex 1

Data Processing Details

VENDOR / 'DATA IMPORTER' DETAILS

Name:	Cypher Learning
Address:	As set out in the preamble to the DPA
Contact Details for Data Protection:	Role: VP of Engineering Email: rik@cypherlearning.com
Vendor Activities:	CYPHER LEARNING is a company that specializes in providing learning platforms for organizations around the world since 2009. CYPHER has three products: NEO LMS for Schools and Universities, MATRIX LMS for Business, and INDIE LMS for Entrepreneurs. CYPHER LEARNING is currently the only company that offers learning platforms in all major e-learning sectors: academic, corporate, and individuals.
Role:	Processor

CUSTOMER / 'DATA EXPORTER' DETAILS

Name:	As set out in the Order Form
Address:	As set out in the Order Form
Contact Details for Data Protection:	Role: As set out in the Order Form Email: As set out in the Order Form
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

DETAILS OF PROCESSING

Categories of Data Subjects:	Categories of Personal Data:	Sensitive Categories of Data, and associated additional restrictions/safeguards:
Matrix		
• Current, former and prospective students (including, but not limited to, corporate learners) • Teachers/instructors • Administrators	Relevant Personal Data includes: Personal details – for example any information that identifies the Data Subject such as their name, gender, email. Contact details – for example business address, email address, telephone details and other contact information.	Categories of sensitive data: N/A Additional safeguards for sensitive data: N/A
Neo		
• Current, former and prospective students • Teachers/instructors • Administrators • Parents	Relevant Personal Data includes: Personal details – for example any information that identifies the Data Subject such as their name, gender, email. Contact details – for example business address, email address, telephone details and other contact information.	Categories of sensitive data: Data collected from a known child (as per Applicable Data Protection Law) Additional safeguards for sensitive data: N/A
Indie		
• Current, former and prospective students • Teachers/instructors • Administrators	Relevant Personal Data includes: Personal details – for example any information that identifies the Data Subject such as their name, gender, email. Contact details – for example business address, email	Categories of sensitive data: N/A Additional safeguards for sensitive data: N/A

	address, telephone details and other contact information.	

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.
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 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 & Australian Annex

1. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**

1.1 Vendor, taking into account the nature of the Processing and the information available to 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**

EU Restricted Transfers

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

(a) populated in accordance with Part 1 of Attachment 1 to 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 SCCs, which are hereby deemed to be:

(a) 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 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, other than the SCCs,

that enables the lawful transfer of Customer Personal Data 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 0 (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 Attachment 1 to Annex 1 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 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 Three of the 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 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 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 SCCs.

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

3.6 Certification of deletion of Customer Personal Data as described in Clauses 8.5 and 16(d) of the 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 EU Restricted Transfer, the 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 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

1. **SIGNATURE OF THE SCCs:**

Where the SCCs apply in accordance with Paragraph 2.1 of 0 2 (European Annex) to the DPA each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. **MODULES**

The following modules of the SCCs apply in the manner set out below (having regard to the role(s) of Customer set out in Annex 1 to the DPA):

(a) Module Two of the SCCs applies to any EU Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and/or

3. **POPULATION OF THE BODY OF THE SCCs**

3.1 For each Module of the 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 Paragraph 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 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 SCCs shall be governed by the law of Ireland in relation to any EU 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 SCCs in relation to any EU 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 SCCs.

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

4.1 Annex I to the Appendix to the 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 SCCs is populated as below:

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

4.3 Annex II to the Appendix to the 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

1. UK TRANSFER ADDENDUM

1.1 Where relevant in accordance with Paragraph 2.2 of 0 (European Annex) to the DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum 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 1.3 of this Part 2.

Annex 3

California Annex

1. In this Annex, the terms "**business**," "**business purpose**," "**commercial purpose**," "**consumer**," "**sell,**" "**share**," and "**service provider**" shall have the respective meanings given thereto in the CCPA; and "**personal information**" shall mean Customer Personal Data that constitutes "personal information" as defined in and that is subject to the CCPA.

2. The business purposes and services for which Vendor is Processing personal information are for Vendor to provide the services to and on behalf of Customer as set forth in the Agreement, as described in more detail in Annex 1.

3. It is the Parties' intent that with respect to any personal information, Vendor is a service provider. Vendor (a) acknowledges that personal information is disclosed by Customer only for limited and specific purposes described in the Agreement; (b) shall comply with applicable obligations under the CCPA and shall provide the same level of privacy protection to personal information as is required by the CCPA; (c) agrees that Customer has the right to take reasonable and appropriate steps under Section 9 of this DPA to help ensure that Vendor's use of personal information is consistent with Customer's obligations under the CCPA; (d) shall notify Customer in writing of any determination made by Vendor that it can no longer meet its obligations under the CCPA; and (e) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

4. Vendor shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the business purposes specified in the Agreement , including retaining, using, or disclosing the personal information for a commercial purpose other than the business purpose specified in the Agreement, or as otherwise permitted by CCPA; (c) retain, use or disclose the personal information outside of the direct business relationship between Vendor and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Vendor's own interaction with any consumer to whom such personal information pertains.

5. Vendor shall implement reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, Customer, in accordance with Section 5 of the DPA.

6. When Vendor engages any Sub-processor, Vendor shall notify Customer of such Sub-processor engagements in accordance with Section 8 of the DPA.

7. Obligations under this Annex that are neither required to be imposed on Vendor for Vendor to qualify as a service provider under the CCPA nor for the Parties to comply with their obligations under the CCPA in relation to the required terms of contracts, in each case, before the CPRA becomes operative on January 1, 2023, shall apply to Vendor only on and after January 1, 2023.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Annex 4

Security Measures

As from the Addendum Effective Date, Vendor will implement and maintain the Security Measures as set out in this Annex 4.

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

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Vendor's organization, monitoring and maintaining compliance with Vendor's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

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

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

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

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

7. 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.

8. 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.

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

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

11. 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.

12. 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.

13. 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 of the DPA.

[REMAINDER OF PAGE INTENTIONALLY BLANK]