VERSAL DATA PROCESSING ADDENDUM

This Data Processing Addendum is entered into by and between Versal Group, Inc., 330 Townsend Street; Suite 205, San Francisco, CA 94107, on behalf of itself and its Affiliates (“Versal”) and the customer who has executed this DPA (“the Client”), and takes effect on the later of May 24, 2018 or the date the Client executes this DPA (the “Effective Date”).

This DPA applies to the Processing of Personal Data (both terms defined below) pursuant to the Versal Services and Platform (defined in the Addendum), and is an addendum to and forms a part of the Addendum.

WHO SHOULD EXECUTE THIS DPA:
Clients that have determined that they qualify as a data controller under the GDPR and need a GDPR-compliant data processing addendum (DPA) in place with vendors that process personal data on their behalf.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of the main body of the DPA, and Annexes 1, 2, and 3.

2. This DPA has been pre-signed on behalf of Versal, and includes the EU Standard Contractual Clauses in Annex 3 (including Appendix 1 thereto), which have also been pre-signed by Versal as the data importer.

3. To complete this DPA, Customer must complete the information in the signature boxes and sign on pages 4, 12, 13 and 14.

4. Send the completed and signed DPA to Versal by email, indicating the Client’s Legal Name (as set out on the applicable order form or invoice, if applicable), to sales@versal.com.

Upon receipt of the validly completed DPA by Versal at this email address, this DPA will become legally binding.

1. Certain Definitions

1.1 In this Addendum, the following terms will have the meanings set out below:

(a) “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 direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

(b) “Client Personal Data” means any Personal Data Processed by Versal or a Subprocessor in the provision of the Services to Client, including (but not limited to) any contact information or other personally identifiable information of End Users of Client Events or contained in Client Materials;

(c) “Data Breach” means accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data transmitted, stored or otherwise Processed by Versal or its Subprocessors.

(d) “Data Protection Laws” means any local, national or international laws, rules and regulations related to privacy, security, data protection, and/or the Processing of Personal Data, including EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (on and after May 25, 2018) by the GDPR and laws implementing or supplementing the GDPR;

(e) “Personal Data” is any information relating to an identified or identifiable natural person;

(f) “Process” means any operation or set of operations that is performed upon Client Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and “processed,” or “processing” will be construed accordingly;

(g) “Restricted Transfer” means a transfer of Client Personal Data originating in the EU or collected from the EU transferred to or by Versal and/or a Subprocessor, to a jurisdiction that is not recognized as providing an adequate level of protection for Personal Data by EU Data Protection Laws;

(h) “Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection of data subjects, which have been approved by the European Commission as adding adequate safeguards for Restricted Transfers, or any successor clauses thereto or alternative data transfer mechanisms recognized by the European Commission pursuant to Art. 46 of the GDPR;

(i) “Subprocessor” means any person or entity (including any third party and any Versal Affiliate, but excluding an employee of Versal) appointed by or on behalf of Versal who may Process Client Personal Data;

(j) “Supervisory Authority” means (a) an independent public authority established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws; and

(k) The terms “Data Controller,” “Data Processor,” “Data Subject,” and “Member State” will have the same meaning as in the GDPR.

1.2 All capitalized terms not defined herein shall have the meaning set forth in the Addendum.

2. Processing of Personal Data
2.1 The parties acknowledge and agree Client is the Data Controller, and Versal is the Data Processor. Versal will Process Client Personal Data only on Client’s documented instructions, or where Processing is required by applicable laws.

2.2 Client on its own behalf and as agent for each relevant Client Affiliate instructs Versal (and authorizes Versal to instruct each Subprocessor) to, as reasonably necessary for the provision of the Versal Services (including any additional services used by Client or Client Affiliate, which may subject to supplemental terms): (a) Process Client Personal Data; (b) transfer Client Personal Data to any country or territory provided such complies with Section 7 (Restricted Transfers) below; and (c) engage any Subprocessors, provided such complies with Section 6 (Subprocessing) below.

2.3 Client agrees that (a) Client’s submission of Client Personal Data and instructions for the Processing of Personal Data will comply with Data Protection Laws and Client will at all relevant times remain duly and effectively authorized to give the instruction set out in this Section (Processing of Personal Data) on behalf of each relevant Client Affiliate; (b) Client and any Client Affiliate will, in the use of the Versal Services, Process Personal Data in accordance with the requirements of Data Protection Laws; and (e) Client will provide any required notices to and obtain any required consents from Data Subjects related to the Processing of Client Personal Data as contemplated in these DPA and the Addendum, or as otherwise instructed by Client.

2.4 Client agrees that Versal may de-identify Client Personal Data and other data related to the Versal Services to render it Anonymous Data, which may then be used for the purposes of operating and improving Versal’s services and operations, developing new services and offerings, and other research, analytics and related purposes. Versal may maintain Anonymous Data as part of its own records and information, and such data shall no longer be subject to the Addendum or these DPA. “Anonymous Data” means data that has been de-identified and/or aggregated with other data to such an extent that Client and Client Affiliates are no longer identifiable, and individuals are no longer identified, identifiable, or otherwise ascertainable by reference to or combination with other datasets.

2.5 Annex 1 to these DPA sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, and the categories of Personal Data and Data Subjects, as required by Article 28(3) of the GDPR; Annex 1 does not confer and rights or obligations on either party.

3. Confidentiality and Security

3.1 Personnel. Versal will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Client Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

3.2 Security Controls. Versal will implement appropriate technical and organizational measures, as set forth in Annex 2 (Technical and Organizational Measures), that are designed to provide a level of security appropriate to the risks presented by the Processing of Client Personal Data. In assessing the appropriate level of security, Versal will take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

3.3 Personal Data Breach. Versal will notify the Client without undue delay if it discovers a Personal Data Breach involving the Client Personal Data, and will provide information (as available) to assist the Client to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Versal will co-operate with the Client and take such reasonable steps as are agreed in good faith by the Parties to assist in the investigation, mitigation and remediation of each Personal Data Breach.
4. **Reasonable Assistance to Controller.**

Versal will promptly notify the Client if it receives a request from a Data Subject regarding the Client Personal Data. Upon request of the Client and subject to the nature of the relevant Processing by and information available to Versal, Versal will provide the Client with reasonable assistance as necessary to the Client's fulfillment of its obligations under Data Protection Laws to respond to Data Subject requests relating to Personal Data, and conduct any data protection impact assessments or prior consultations with any Supervisory Authority.

5. **Audit Rights**

Upon the Client’s written request, Versal will make available to the Client information reasonably necessary to demonstrate Versal’s compliance with this Addendum. Where the Client reasonably determines that the information provided is not sufficient to demonstrate Versal’s compliance, Versal will upon reasonable notice, allow for and contribute to inspections by a qualified, independent third-party auditor appointed by the Client to confirm Versal’s compliance with this Addendum, provided such audits or inspections will be conducted within normal business hours no more than once in any calendar year. The Client will reimburse Versal in full for all costs reasonably and properly incurred by Versal performing its obligations under this Section.

6. **Subprocessing**

6.1 Client authorizes Versal to appoint (and permit each Subprocessor appointed in accordance with this Section to appoint) Subprocessors. Client expressly agrees that Versal Affiliates may be engaged as Subprocessors, and that Versal may continue to use those other Subprocessors already engaged by Versal as of the date of these DPA. Versal will provide notice of new Subprocessors prior to authorizing new Subprocessors to Process Personal Data in connection with the Versal Services, by sending an email notification. Client may object to the appointment of a new Subprocessor by sending written notice to Versal at help@versal.com within ten (10) business days of the notice of new Subprocessors; Client’s notice of objection should state the basis for Client’s objection. Client agrees that it will not unreasonably object to the use of a Subprocessor. If Client does not object to the appointment of the Subprocessor within ten (10) business days, the Client shall be deemed to have approved and agreed to such appointment.

6.2 The parties will work in good faith to resolve Client’s objections to the appointment of any Subprocessors. During this time, there may be an impact to the provision of the Versal Services; Client agrees that Versal is not liable for any such impact. If the parties are unable to resolve Client’s objection within 90 days, Client may terminate without penalty the portion of the Addendum pertaining to the Versal Services that Versal states it cannot provide without the use of the objected-to Subprocessor, and Versal will refund Client any prepaid but unused amounts for such portion; otherwise, the Addendum shall remain in full force and effect.

6.3 With respect to each Subprocessor, Versal will include terms in the contract between Versal and each Subprocessor which offer an equivalent level of protection for Client Personal Data as those set out in these DPA, taking into account the nature of the services performed by the Subprocessor. If the arrangement involves a Restricted Transfer, ensure that adequate contractual measures are in place as required by Data Protection Laws, and where the Client Personal Data is from the EEA or Switzerland the Standard Contractual Clauses will be incorporated into the Addendum between Versal and the Subprocessor.

7. **Restricted Transfers**

Versal the (“data importer”) will execute with Client (the “data exporter”) the Standard Contractual Clauses, set forth in Annex 2 herein, which will apply to Client Personal Data transferred from the EU to Versal in the United States.
8. Deletion or Return of Personal Data

Upon the termination or expiration of the Addendum (unless continued Processing is subject to a new or amended Addendum) and to the extent not prohibited by applicable law, Versal will delete the Customer Content three years after the termination of the Addendum (unless the associated account is reactivated), or earlier upon the Customer’s request. The parties agree that Versal is not required to return or delete any Anonymous Data at the conclusion of the Addendum.

9. General Terms

9.1 Liability. The aggregate liability of Versal arising out of or related to these DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability in the Addendum.

9.2 Termination. The parties agree that these DPA and the Standard Contractual Clauses will terminate automatically upon: (a) termination of the Addendum; or (b) expiry or termination of all service contracts entered into by Versal with Client pursuant to the Addendum; or (iii) termination or completion of statements of work, work orders or similar documents, thereunder, whichever is later.

9.3 Changes in Data Protection Laws. If any variation is required to these DPA (including the Standard Contractual Clauses) as a result of a change in Data Protection Law, either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to these DPA to address such changes.

This Addendum is entered into and becomes a binding as of the Effective Date.

Client Legal Name: ____________________________

Signature ____________________________

Name ____________________________

Title ____________________________

Date Signed ____________________________

Versal Group, Inc.

Signature ____________________________

Name ____________________________

Title ____________________________

Date Signed ____________________________
ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Client Personal Data as required by Article 28(3) GDPR.

1. **Subject matter and duration of the Processing of Client Personal Data:**

   The subject matter and duration of the Processing of Client Personal Data are set out in the Addendum and these DPA.

2. **The categories of Data Subject to whom Client Personal Data relates**

   - Actual and prospective users ("End Users") of Client content, courses and other materials ("Client Content") through the Versal Services.
   - Client personnel, agents, affiliates, subsidiaries and others who have been authorized to access, manage and use the Platform on Client’s behalf ("Authorized Users"), and other client personnel

3. **The nature and purpose of the Processing of Client Personal Data:**

   - Collection, storage, and management of registration and other information from End Users
   - Facilitate Client’s creation, management, hosting, delivery, sharing, and distribution of Client Content
   - Facilitate reminders, notices, and other email and other communications (including by email) to End Users
   - Manage Platform access by Authorized Users and prevent unauthorized access
   - Generate and provide reporting and analytics to Client related to Versal Services
   - Support, maintenance, and managed services related to Client’s Use of the Platform and Versal Services

4. **The types of Client Personal Data to be Processed**

   - Name, email, and other contact details
   - Company, position/title, company contact details, and other business information
   - Other information Client chooses to or requests Versal to collect as part of Client Event registration or attendance
   - Video, images, audio, and other content
   - Name, title, company email, and other information requested of Authorized Users
   - Client Event analytics and usage statistics
ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

1. Any Processing of Personal Data will take place on data processing systems for which commercially reasonable technical and organizational measures for protecting Personal Data have been implemented. Versal will maintain reasonable and appropriate technical, physical, and administrative measures to protect Client Personal Data under its possession or control against unauthorized or unlawful Processing or accidental loss, destruction or damage, taking into account the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage, and the sensitivity of the Client Personal Data.

2. Security measures will be designed to:
   (a) deny unauthorized persons access to data-processing equipment used for processing Personal Data (equipment access control);
   (b) prevent the unauthorized reading, copying, modification, or removal of media (data media control);
   (c) prevent the unauthorized input of Personal Data and the unauthorized inspection, modification, or deletion of stored Personal Data (storage control);
   (d) prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
   (e) provide that persons authorized to use an automated data-processing system only have access to the Personal Data covered by their access authorization (data access control);
   (f) enable Versal to verify and establish to which individuals Client Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
   (g) enable identification of which Client Personal Data have been put into automated data-processing systems and when and by whom the input was made (input control);
   (h) prevent the unauthorized reading, copying, modification, or deletion of Client Personal Data during transfers of those data or during transportation of storage media (transport control);
   (i) include commercially reasonable disaster recovery procedures to provide for the continuation of services under the Addendum and backup of Client Personal; and
   (j) include appropriate technical security solutions are implemented and managed to protect the confidentiality, integrity, and availability of Client Personal Data.

3. Where appropriate, data will be encrypted in transmission and at rest, using industry-standard cryptographic techniques and secure management of keys.

4. Versal will take reasonable steps to ensure the reliability of its employees and other personnel having access to Client Personal Data, and will limit access to Client Personal Data to those Personnel who have a business need to have access to such Client Personal Data, and have received reasonable training regarding the handling of Personal Data and Data Protection Laws.

5. On request and subject to written confidentiality obligations, Versal will provide the Company with access
to its relevant data security policies and procedures.

**Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: ____________________________

Address: ____________________________

Other information needed to identify the organisation

........................................................................................................

(the data exporter)

And

Name of the data importing organisation: Versal Group, Inc. for itself and its affiliated entities

Address: 330 Townsend Street; Suite 205, San Francisco, CA 94107

........................................................................................................

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter and data importer have entered into an Addendum pursuant to which the data importer will provide certain claims management services for or on behalf of the data exporter (the “Addendum”). As part of the Addendum the data exporter and data importer have also entered into data processing terms, pursuant to which it is contemplated that services provided by the data importer will involve the transfer of personal data to the data importer (or its affiliates or subsidiaries), located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the data exporter (for itself and its relevant affiliates or subsidiaries) agrees to the provision of such services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

**Definitions**

For the purposes of the Clauses:
(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' will have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.]

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor will be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words “within the meaning of Directive 95/46/EC” are deleted.]

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for
subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which will be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in Addendum with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessiong, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which will be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessiong, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor Addendum it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor will be limited to its own processing operations under the Clauses.
Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer will promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter will be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses will be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.
Clause 11

Subprocessing

1. The data importer will not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it will do so only by way of a written Addendum with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written Addendum the data importer will remain fully liable to the data exporter for the performance of the subprocessor's obligations under such Addendum.

2. The prior written contract between the data importer and the subprocessor will also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor will be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 will be governed by the law of the Member State in which the data exporter is established.

4. The data exporter will keep a list of subprocessing Addendums concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which will be updated at least once a year. The list will be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor will, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or will destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full): 
Position: 

Page 14 of 17
Address:
Other information necessary in order for the contract to be binding (if any):

On behalf of the data importer:
Name (written out in full):  
Position:  
Address: 330 Townsend Street; Suite 205, San Francisco, CA 94107

Signature

Signature
APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

The data exporter is:

A company that has entered into an Addendum to use data importer’s eLearning platform.

Data importer
The data importer is:

A provider of a SaaS-based eLearning Platform and related services.

Data subjects
The personal data transferred concern the following categories of data subjects:

Those set forth in paragraph 3 of Annex 1 to the DPA.

Categories of data
The personal data transferred concern the following categories of data:

Those set forth in paragraph 2 of Annex 1 to the DPA.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:

Those set forth in paragraph 2 of Annex 1 to the DPA.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

Those set forth in paragraph 1 of Annex 1 to the DPA.

<table>
<thead>
<tr>
<th>DATA EXPORTER</th>
<th>DATA IMPORTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name ___________________________</td>
<td>Name Versal Group  ____</td>
</tr>
<tr>
<td>Authorised Signature ____________</td>
<td>Authorised Signature ____________</td>
</tr>
</tbody>
</table>
APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(e) and 5(e):

The parties agree that the data importer will comply with the security requirements set forth in Annex 2 to this Data Processing Terms (Schedule 3 to the Addendum).

DATA EXPORTER
Name
Authorised Signature

DATA IMPORTER
Name
Authorised Signature