DATA PROCESSING AGREEMENT

This Data Processing AGREEMENT (this **"DPA"**) forms a part of the Business Terms of Use.

1. **Definitions.** Unless otherwise defined below, capitalized terms used in this DPA are defined in the Agreement, and are used herein as defined therein.

"**Adequate Country**" means a country or territory that is recognized under EU Data Protection Laws from time to time as providing adequate protection for personal data;

"**Customer Data**" means Personal Data provided to Pluralsight by Customer in order for Pluralsight to perform its obligations under the Agreement;

"**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a data subject to the processing of the data subject's Personal Data;

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including (where applicable) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and the California Consumer Privacy Act (CCPA);

"**Personal Data**" means any information relating to an identified or identifiable natural person;

"**Pluralsight Group**" means Pluralsight and any corporate entities which are from time to time Affiliates of Pluralsight.

"**processing**", "**data controller**", "**data subject**", "**supervisory authority**" and "**data processor**" shall have the meanings ascribed to them in the GDPR. For purposes of this DPA, the term "**data subject**" includes a "**consumer**" as that term is defined in the CCPA;

"**Security Breach**" means an actual incident of unauthorized or accidental disclosure of or access to any Customer Data by any of its staff, sub-processors or any other identified or unidentified third party. "Pings" and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents are not included within the meaning of Security Breach.

2. Data Processing

2.1. **Scope and Roles of the Parties.** This DPA applies when Customer Data is processed by Pluralsight. In this context, Customer and its Affiliates are the data controller(s) and Pluralsight is the data processor, processing Customer Data on Customer's and its Affiliates' behalf. The parties hereby acknowledge and agree that Pluralsight is the data controller with respect to the Personal Data provided to Pluralsight by an individual user of the Platform, excluding and distinct from the Customer Data.

2.2. **Subject-Matter, Nature, Purpose and Duration of Data Processing.** Pluralsight processes Customer Data to provide access to and functionality on the Platform. The duration of the processing shall be for the term of the Agreement.

2.3. **Categories of Data Subjects and Types of Personal Data.** Pluralsight processes Customer data for Customer's employees and other persons authorized by Customer to access the Platform. The types of Customer Data processed pursuant to this DPA are first name, last name, corporate email address, and last login IP address of data subjects.

2.4. **Compliance with Laws.** Customer and Pluralsight each will comply with the Data Protection Laws in its role as data controller or data processor, respectively. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data.

2.5. **Customer Instructions.** The parties agree that this DPA and the Agreement constitute Customer's documented instructions to Pluralsight for the processing of Customer Data ("**Documented Instructions**").

Pluralsight will process Customer Data only in accordance with Documented Instructions, and will not sell, nor retain, use or disclose Customer Data for any other purpose. Additional instructions outside the scope of the Documented Instructions (if any) require the parties' prior written agreement, including agreement on any additional fees payable by Customer to Pluralsight for carrying out such additional instructions. Pluralsight shall notify the Customer promptly (unless prohibited from so doing by applicable law) in the event that applicable law requires Pluralsight to process Customer Data other than pursuant to Documented Instructions or if, in Pluralsight's opinion, any Documented Instruction violates applicable law.

3. Security of Customer Data.

3.1. **Security Program.** Pluralsight has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data as set out in the Security Measures attached hereto as Annex 2.

3.2. **Pluralsight Personnel.** Pluralsight shall take reasonable steps to ensure that only authorised personnel have access to such Customer Data and that any persons whom it authorises to have access to the Customer Data are (i) appropriately trained regarding the handling and safeguarding of Customer Data; and (ii) are under obligations of confidentiality.

3.3. **Return or Deletion of Customer Data.** Upon receipt of Customer's written election at the termination or expiry of the Agreement, and unless prohibited by applicable law, Pluralsight shall promptly delete (as specified by Customer) all Customer Data (including copies thereof) processed by Pluralsight.

3.4. **Government Access Requests.** If Pluralsight receives a demand from a governmental body for Customer Data, Pluralsight will attempt to redirect the governmental body to request that data directly from Customer. If compelled to disclose Customer Data to a governmental body, and unless prohibited by applicable law, Pluralsight will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy

4. **Security Breaches**. If Pluralsight becomes aware of a Security Breach, it shall, without undue delay, notify Customer of the Security Breach. Pluralsight's notice shall include, if known, (i) the possible cause and consequences of the Security Breach; (ii) the categories of Customer Data involved; (iii) a summary of the possible consequences for the relevant data subjects; (iv) a summary of the unauthorised recipients of the Customer Data; and (v) the measures taken by Pluralsight to mitigate any damage. Unless required by applicable law, Pluralsight shall not make any announcement about a Security Breach (a "**Breach Notice**") without the prior written consent of Customer of the content, media and timing of the Breach Notice.

5. **Data Subject Rights**

5.1. **Access, Correction, Deletion or Restriction.** Pluralsight will assist Customer in meeting its obligations under applicable Data Protection Laws, by either (i) providing Customer the ability within the Platform to access, correct or delete Customer Data or restrict its processing; or (ii) if such functionality is not available within the Platform, make Customer Data available to Customer, or as applicable, make such corrections, deletions, or restrictions on Customer's behalf.

5.2. **Handling of Data Subject Requests.** Customer is solely responsible for responding to Data Subject Requests. Unless otherwise required by law, if Pluralsight receives a Data Subject Request, it shall promptly redirect the data subject to Customer.

5.3. **Data Portability.** During the term of the Agreement, Customer may extract Customer Data from the Platform, including so that Customer can provide Personal Data to an individual who makes a data portability request under Data Protection Laws.

6. Sub-Processing

6.1. **Notification of New Sub-processors and Objection Right.** Pluralsight will maintain a list of sub- processors at the following URL: http://www.pluralsight.com/sub-processors, will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Customer Data, and shall provide a mechanism (e.g. RSS Feed) to allow Customer to receive notices of updates to the list. If Customer has a reasonable objection relating to data protection to any new or replacement sub-processor, it shall notify Pluralsight of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matterin good faith. If Pluralsight is able to provide the Platform to Customer in accordance with the Agreement without using the sub-processor and decides in its discretion to do so, then Customer will have no further rights under this clause 6.1 with respect to the proposed use of the sub-processor. If Pluralsight requires to use the sub-processor and is unable to satisfy Customer as to 1) the suitability of the sub-processor, or 2) the documentation and protections in place between Pluralsight and the sub-processor within sixty (60) days from Customer's notification of objection, Customer may, within thirty (30) days of the end of the sixty (60) day period referred to above, terminate the Agreement by providing written notice to Pluralsight having effect thirty (30) days after receipt by Pluralsight. Pluralsight may use a new or replacement sub-processor whilst the objection procedure in this clause is in process.

6.2. **General Authorization.** Customer grants a general authorization (a) to Pluralsight to appoint other members of the Pluralsight Group as sub-processors and (b) to Pluralsight and other members of the Pluralsight Group to appoint third party data center operators, and outsourced support providers as sub-processors to support the performance of the Platform.

6.3. **Engagement.** Pluralsight will ensure that any sub-processor it engages on its behalf in connection with the Agreement does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Customer Data than those imposed on Pluralsight in this DPA (the "**Relevant Terms**"). Pluralsight shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms.

7. Audits and Impact Assessments

7.1. **Audits.** Customer agrees that an audit report not older than 18 months by a registered and independent external auditor demonstrating that Pluralsight's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard (such as ISO 27001 or SSAE 16 II SOC1 and SOC2) will be used to satisfy any audit or inspection requests by or on behalf of Customer, and Pluralsight shall make such reports available to Customer upon request. In the event that a regulator, or supervisory authority requires additional information, including information necessary to demonstrate compliance with this DPA, or an audit related to the security of Customer Data, Pluralsight shall allow no more than once in any twelve-month period inspection of its facilities and provide additional information in Pluralsight's possession or control.

7.2. **Data Protection Impact Assessments and Prior Consultations**. If, after receipt of an accepted industry standard audit report as further outlined in Section 7.1 above, Customer requires additional assistance to meet its obligations under Data Protection Laws to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Platform, Pluralsight will, taking into account the nature of processing and the information available to Pluralsight, provide reasonable assistance to Customer.

8. Data Center Location and Data Transfers

8.1. **Location of Customer Data.** Customer Data will be located in data centers within the United States or Canada unless the parties otherwise expressly agree in writing or as necessary to comply with the law or binding order of a governmental body.

8.2. **Application of Standard Contractual Clauses.** The Standard Contractual Clauses (SCCs) as set out in Annex 1 hereto will apply to Customer Data that is transferred outside the European Economic Area (EEA), either directly or via onward transfer, to any country not recognized by the European Commission as an Adequate Country. The SCCs will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Pluralsight adopts Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

8.3. **Clarifications to the SCCs.** The following terms set forth how the Parties comply with certain terms of the SCCs:

a. Customer may exercise its right of audit under clause 5.1(f) of the SCCs as set out in, and subject to the requirements of, clause 7.1 of this DPA; and

b. Pluralsight may appoint sub-processors as set out, and subject to the requirements of, clause 6 of this DPA.

9. General

9.1. **Conflicts.** This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this

DPA shall prevail so far as the subject matter concerns the processing of Customer Data.

9.2. **Remedies.** Customer's remedies (including those of its Affiliates) with respect to any breach by Pluralsight or the Pluralsight Group of the terms of this DPA, and the overall aggregate liability of Pluralsight and the Pluralsight Group arising out of, or in connection with the Agreement (including this DPA and the SCCs) shall not under any circumstances exceed the maximum aggregate liability of Pluralsight to Customer as set out in the Agreement. Nothing in this DPA will limit Pluralsight's liability in respect of personal injury or death in negligence or for any other liability or loss which may not be limited by agreement under applicable law.

9.3. A person who is not a party to this DPA shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this DPA.

Annex 1

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

----

INTRODUCTION

Both 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.

AGREED TERMS

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**' shall have the same meaning as in EU Data Protection Laws 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 entity 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 EU Data Protection Laws 95/46/EC;

d. 'the **sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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; and

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 4.1(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 sub-processor 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 sub- processor shall 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 EU Data Protection Laws 95/46/EC;

g. to forward any notification received from the data importer or any sub-processor 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 sub- processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor 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 shall 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 agreement with the supervisory authority;

g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub- processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i. that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j. to send promptly a copy of any sub-processor agreement 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall 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
Co-operation 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 sub-processor, 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 shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9
Governing law

The Clauses shall 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
Sub-processing

1. The data importer shall 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 shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub- processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall 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 sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall 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 sub-processor 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.

Appendix 1
To the Standard Contractual Clauses

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

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is a customer of, and subject to a subscription licensing agreement with the data importer.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer provides an online library of training courses to IT and software developer professionals.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data subjects are employees of the data exporter receiving online training.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data importer stores first name, last name, corporate email address, and last login IP address in a user table that is maintained persistently and backed up regularly.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

No transfer of special categories is anticipated.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data importer uses the data to validate that users attempting to access the data importer’s online training platform are authorized to do so.

Appendix 2
To the Standard Contractual Clauses

This Appendix forms part of the Clauses and is agreed to upon acceptance of the Terms of Use.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Security Measures are attached as Annex 2 to the DPA.

Annex 2 Security Measures

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Data are processed, include:

- Establishing secure areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Data in accordance with their access rights, and that Customer Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Customer Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;

- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Customer Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Data are disclosed, include:

- Encryption/tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Customer Data are processed solely in accordance with the instructions of the Controller include:

- Unambiguous wording of the contract;
- Criteria for selecting subprocessor(s).

7. Availability control

Technical and organizational measures to ensure that Customer Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Customer Data collected for different purposes can be processed separately include:

- Separation of databases;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes