

## ZENLER DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) forms a part of the Customer Terms of Service found at <https://zenler.com/terms-of-use>.

By signing the DPA, Customer(Controller) enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer(Controller) and Controller Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services under the Agreement, Zenler may Process certain Personal Data (such terms defined below) on behalf of Customer and where Zenler processes such Personal Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

### **How to Execute this DPA:**

1. This DPA consists of two parts: the main body of the DPA, and Exhibit A, B and C (including Appendices 1 and 2).
2. This DPA has been pre-signed on behalf of Zenler. The Standard Contractual Clauses in Exhibit C have been pre-signed by Zenler Ltd as the data importer.
3. To complete this DPA, Customer must complete information and signatures on pages 11,16, 25, 27, 28.
4. Send the completed and signed DPA to Zenler by email, indicating Customer’s Site/Schol URL(s) (as set out on the applicable signup Form), to [support@zenler.com](mailto:support@zenler.com). Upon receipt of the validly completed DPA by Zenler at this email address, this DPA will become legally binding.

### **How this DPA Applies to Customer and its Affiliates**

If the Customer signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Zenler entity that is party to the Agreement is party to this DPA. If the Customer signing this DPA has executed an Signup/Order form with Zenler or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Signup/order form and applicable renewal Order Forms, and the Zenler entity that is party to such Order Form is party to this DPA. If the Customer entity signing this DPA is neither a party to an Signup/Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer who is a party to the Agreement executes this DPA.

Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and

processors.

**Agreed Terms:**

**1. Definitions and Interpretation**

The following definitions and rules of interpretation apply in this Agreement.

**1.1 Definitions:**

**Data Protection Legislation:** all applicable data protection laws including GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

**Data Subject:** an individual who is the subject of Personal Data.

**GDPR:** General Data Protection Regulation ((EU) 2016/679).

**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.

**Controller:** means the entity which determines the purposes and means of the Processing of Personal Data. "Controller **Controller Affiliate:** means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Zenler, but have not signed their own signup/Order Form and are not a "Customer" as defined under the Agreement, (b) if and to the extent Zenler processes Personal Data for which such Affiliate(s) qualify as the Controller.

**Personal Data:** means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

**Processing:** 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

making available, alignment or combination, restriction, erasure or destruction.

**Processor:** means the entity which Processes Personal Data on behalf of the Controller.

**Zenler:** means the Zenler entity which is a party to this DPA, as specified in the section “How this DPA Applies” above, being Zenler Ltd, a company constituted under the laws of UK, as applicable. “Zenler Group” means Zenler and its Affiliates engaged in the Processing of Personal Data. “Standard Contractual Clauses” means the agreement executed by and between Customer and Zenler Ltd. and attached hereto as Exhibit C pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

**Sub-processor** means any entity engaged by Zenler or a member of the Zenler Group to Process Personal Data in connection with the Services. “Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

**Supervisory Authority:** means an independent public authority which is established by an EU Member State pursuant to the GDPR.

## 2.1 Roles of the Parties

The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Zenler is the Processor and that Zenler or members of the Zenler Group will engage Sub-processors pursuant to the requirements set forth in list of Zenler sub processors below.

## 2.2 Customer’s Processing of Personal Data.

Customer shall, in its use of the Services and provision of instructions, process Personal Data in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

**2.3 Zenler’s Processing of Personal Data.** As Customer’s Processor, Zenler shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Signup / Order Form(s); (ii) Processing initiated by Authorized Students in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the “Purpose”). Zenler acts on behalf of and on the instructions of Customer in carrying out the Purpose.

## 2.4 Details of the Processing.

The subject-matter of Processing of Personal Data by Zenler is as described in the Purpose in Section 2.3. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit B (Description of Processing Activities)

to this DPA.

### **3. Rights Of Data Subjects**

#### **3.1 Data Subject Requests.**

Zenler shall, to the extent legally permitted, promptly notify Customer if Zenler receives any requests from a Data Subject to exercise the following Data Subject rights in relation to Personal Data: access, rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a “Data Subject Request”). Taking into account the nature of the Processing, Zenler shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under applicable Data Protection Legislation. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Zenler shall, upon Customer’s request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Zenler is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Zenler’s provision of such assistance, including any fees associated with provision of additional functionality.

### **4. Sub Processors**

#### **4.1 Appointment of Sub-processors.**

Customer acknowledges and agrees that (a) Zenler’s Affiliates may be retained as Sub-processors through written agreement with Zenler and (b) Zenler and Zenler’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Personal Data, Zenler or a Zenler Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Customer acknowledges that Zenler Ltd is located in the UK and is involved in providing the Services to Customer either directly or through sub processors who may be outside the EU. In either case, Customer agrees to enter into the Standard Contractual Clauses set out in Exhibit C and acknowledges that Sub-processors may be appointed by Zenler in accordance with Clause 11 of Exhibit C.

**4.2 List of Current Sub-processors and Notification of New Sub-processors.** A current list of Sub processors for the Services, including the identities of those Sub-processors is provided below

#### **Company - Sub Processing Activity - Country**

##### **Infrastructure Sub Processors:**

Amazon - Infrastructure Cloud Provider - US

**Other Sub Processors:**

Vimeo - Cloud Based Video Hosting - US

FileStack - Cloud Based File management Provider - US

SendGrid - Cloud based Email provider - US

Zendesk - Cloud based Support software - US

Intercom - Cloud based Support software - US

**Zenler Affiliates:**

Zenler LLC - Zenler Development/Sales/Support team - US

Zenler India - Development/Support team, India

Customer may receive notifications of new Sub-processors by e-mailing support@zenler.com with the subject "Update me about new Sub Processors ", and if a Customer contact subscribes, Zenler shall provide the subscriber with notification of new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

**4.3 Objection Right for New Sub-processors.**

Customer may reasonably object to Zenler's use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Zenler promptly in writing within ten (10) business days after receipt of Zenler's notice in accordance with the mechanism set out in Section 4.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Zenler will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Zenler is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Signup/Order Form(s) with respect only to those Services which cannot be provided by Zenler without the use of the objected-to new Sub-processor by providing written notice to Zenler. Zenler will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

**4.4 Liability.**

Zenler shall be liable for the acts and omissions of its Sub-processors to the same extent Zenler would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

## 5. Security

**5.1 Controls for the Protection of Personal Data.** Zenler shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data. Zenler regularly monitors compliance with these measures. Zenler will not materially decrease the overall security of the Services during a subscription term.

### 5.1 Confidentiality

We place strict controls over our employees' access to the data you and your users make available via the Zenler services, as more specifically defined in your agreement with Zenler covering the use of the Zenler services ("Student Data"), and are committed to ensuring that Student Data is not seen by anyone who should not have access to it. The operation of the Zenler services requires that some employees have access to the systems which store and process Student Data. For example, in order to diagnose a problem you are having with the Zenler services, we may need to access your Student Data. These employees are prohibited from using these permissions to view Student Data unless it is necessary to do so. We have technical controls and audit policies in place to ensure that any access to Student Data is logged.

All of our employees and contract personnel are bound to our policies regarding Student Data and we treat these issues as matters of the highest importance within our company.

### 5.2 Personnel Practices

Zenler conducts background checks on all employees before employment, and employees receive privacy and security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our comprehensive information security policy covering the security, availability, and confidentiality of the Zenler services.

### 5.3 Compliance

The environment that hosts the Zenler services maintains multiple certifications for its data centers, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, please visit the AWS Security website <https://aws.amazon.com/security/> and the AWS Compliance website <https://aws.amazon.com/compliance/>.

### 5.4 Availability

We understand that you rely on the Zenler services to work. We're committed to making Zenler a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers or even entire data centers.

### **5.5 Disaster Recovery**

Student Data is stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. Student Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system.

### **5.6 Network Protection**

In addition to sophisticated system monitoring and logging, we have implemented two-factor authentication for all server access across our production environment. Firewalls are configured according to industry best practices and unnecessary ports are blocked by configuration with AWS Security Groups.

### **5.7 Logging**

Zenler maintains an extensive, centralized logging environment in its production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about the Zenler services. These logs are analyzed for security events via automated monitoring software, overseen by the security team.

### **5.8 Incident Management & Response**

In the event of a security breach, Zenler will promptly notify you of any unauthorized access to your Student Data. Zenler has incident management policies and procedures in place to handle such an event.

### **5.9 Audits.**

Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Zenler shall make available to Customer (or Customer's independent, third-party auditor) information regarding the Zenler Group's compliance with the obligations set forth in this DPA. Customer may contact Zenler in accordance with the "Notices" Section of the Agreement to request an on-site audit of Zenler's procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Legislations. Customer shall reimburse Zenler for any time expended for any such on-site audit at the Zenler Group's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Zenler shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Zenler. Customer shall promptly notify Zenler with information regarding any non-compliance discovered during the course of an audit, and Zenler shall use commercially reasonable efforts to address any confirmed non-compliance.

## **6. Personal Data Incident Management and Notification**

Zenler shall notify Customer without undue delay of any breach relating to Personal Data (within the meaning of

applicable Data Protection Legislation) of which Zenler becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law or which Zenler is required to notify to Customer under applicable Data Protection Legislation (a “Personal Data Incident”). Zenler shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Zenler’s control. Except as required by applicable Data Protection Legislations, the obligations herein shall not apply to incidents that are caused by Customer, Students and/or any Non Zenler Products.

## **7. Return and Deletion of Personal Data**

Upon termination of the Services for which Zenler is Processing Personal Data, Zenler shall, upon Customer’s request return all Personal Data in Zenler’s possession to Customer or securely destroy such Personal Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data. For clarification, depending on the Service plan purchased by Customer, access to export functionality may incur additional charge(s) and/or require purchase of a Service upgrade.

## **8. Controller Affiliates**

**8.1 Contractual Relationship.** The parties acknowledge and agree that, by executing the DPA in accordance with “How to Execute this DPA”, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Zenler and each such Controller Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Customer.

### **8.2 Communication.**

The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Zenler under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

### **8.3 Rights of Controller Affiliates.**

If a Controller Affiliate becomes a party to the DPA with Zenler, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1 Except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or

seek any remedy under this DPA against Zenler directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

8.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, if carrying out an on-site audit of the Zenler procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Zenler by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

## **9. Limitation Of Liability**

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and Zenler, whether in contract or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Zenler's and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

## **10. European Specific Provisions**

### **10.1 GDPR**

With effect from 25 May 2018, Zenler will Process Personal Data in accordance with the GDPR requirements directly applicable to Zenler's provisioning of the Services.

#### **10.1.1 Data Protection Impact Assessment**

Upon Customer's request, Zenler shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Zenler. Zenler shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

## **10.2 Transfer Mechanisms**

For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Legislations:

1. Zenler's Sub Processors who are Privacy Shield Framework self-certified.
2. The Standard Contractual Clauses set forth in Exhibit C to this DPA apply, subject to Exhibit A.

## **11. Parties to this DPA**

The Section "How this DPA applies" specifies which Zenler entity is party to this DPA. In addition, Zenler Affiliates are a party to the Standard Contractual Clauses in Exhibit C. Notwithstanding the signatures below of any other Zenler entity, such other Zenler entities are not a party to this DPA or the Standard Contractual Clauses.

## **12. Legal Effect**

This DPA shall only become legally binding between Customer and Zenler when the formalities steps set out in the Section "How to Execute this DPA" above have been fully completed.

## **13. Governing Law**

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of UK.

## **List of Exhibits**

Exhibit A: Additional Data Transfer Terms

Exhibit B: Description of Processing Activities

Exhibit C: Standard Contractual Clauses

The parties' authorized signatories have duly executed this DPA:

On behalf of Customer: Name (written out in full): \_\_\_\_\_

Position: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

On behalf of Zenler Ltd.:

Name: Rakesh Vallil

Position: Director, Zenler Ltd, Tech

Address, Zenler Ltd, Techhub, 101 Finsbury Pavement, London EC2A 1RS, UK

Signature:  \_\_\_\_\_

24/05/2018 03:21:51 PDT

## **EXHIBIT A**

### **Additional Data Transfer Terms**

#### **1. Additional Terms to Standard Contractual Clauses**

##### **1.1. Customers covered by the Standard Contractual Clauses**

The Standard Contractual Clauses and the additional terms specified in this Exhibit A apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Controller Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Services. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed “data exporters”.

##### **1.2. Instructions**

This DPA and the Agreement are Customer’s complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Authorized Students in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) where such instructions are consistent with the terms of the Agreement.

##### **1.3. Appointment of new Sub-processors and List of current Sub-processors.**

Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) Zenler’s Affiliates may be retained as Sub-processors; and (b) Zenler and Zenler’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Zenler shall make available to Customer the current list of Sub-processors in accordance with Section 4.2 of this DPA.

##### **1.4. Notification of New Sub-processors and Objection Right for new Sub-processors**

Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Zenler may engage new Sub-processors as described in Sections 4.2 and 4.3 of the DPA.

##### **1.5. Copies of Sub-processor Agreements.**

The parties agree that the copies of the Sub-processor agreements that must be provided by Zenler to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Zenler beforehand; and, that such

copies will be provided by Zenler, in a manner to be determined in its discretion, only upon request by Customer.

**1.6. Audits** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Zenler shall make available to Customer (or Customer's independent, third-party auditor) information regarding the Zenler Group's compliance with the audit obligations set forth in this DPA. Customer may contact Zenler in accordance with the "Notices" Section of the Agreement to request an on-site audit of Zenler's procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Legislation. Customer shall reimburse Zenler for any time expended for any such on-site audit at the Zenler Group's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Zenler shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Zenler. Customer shall promptly notify Zenler with information regarding any non-compliance discovered during the course of an audit, and Zenler shall use commercially reasonable efforts to address any confirmed non-compliance.

**1.7. Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Zenler to Customer only upon Customer's request.

**1.8. Conflict**

In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Exhibit C, the Standard Contractual Clauses shall prevail.

## EXHIBIT B

### Description of Processing Activities

Data subjects Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Students and Leads of Customer
- Consultants and Contractors of Customer
- Affiliates and agents of Customer; and/or
- Third parties with which Customer conducts business.

### Categories of data

The personal data transferred concern the following categories of data: Any personal data comprised in Student Data, as defined in the Agreement.

Sensitive personal data below will **not** be submitted by Customer to Zenler through the Services as per the Zenler terms of service:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic or biometric data
- Health and
- Sex life

### Processing operations

The personal data transferred will be processed in accordance with the Agreement and any Signup or Order Form and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain, and update the Services provided to Customer;

- To provide customer and technical support to Customer; and
- Disclosures in accordance with the Agreement, as compelled by law.

**EXHIBIT C**

**Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller to processor transfers)**

**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 or person : \_\_\_\_\_

Address: \_\_\_\_\_

Tel. : \_\_\_\_\_

e-mail: \_\_\_\_\_

Other information needed to identify the organisation/person: \_\_\_\_\_  
(the data exporter)

And

Name of the data importing organisation:

Zenler Ltd

Address: Zenler Ltd, TechHub, 101 Finsbury Pavement, London EC2A 1RS, UK

Tel.:+44-020 8144 0587 e-mail: support@zenler.com

Zenler Ltd

Other information needed to identify the organisation: \_\_\_\_\_  
(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.

**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 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<sup>(1)</sup>);
  
- (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;
  
- (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;
  
- (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 Schedule 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 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 Schedule 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;
- (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 Schedule 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 <sup>(2)</sup>**

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 Schedule 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 Schedule 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**

**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 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, namely ...

**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  
(3). Where the sub-processor fails to fulfil 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 law of the Member State in which the data exporter is established, namely ...
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(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.

**On behalf of the Data Exporter:**

Name (written out in full): \_\_\_\_\_

Position: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

**On behalf of the Data Importer:**

Name: Rakesh Vallil

Position: Director

Address: Zenler Ltd, TechHub, 101 Finsbury Pavement, London EC2A 1RS, UK

Signature:  \_\_\_\_\_

24/05/2018 03:21:51 PDT

## Appendix 1

### to the Standard Contractual Clauses

This Schedule 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 Schedule

#### **Data exporter**

The Data Exporter is a customer of the Data Importer's communication and productivity software, services, systems and/or technologies.

#### **Data importer**

The Data Importer is a provider of online course hosting, creation an marketing software, services, systems and/or technologies.

#### **Data subjects**

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Law and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Authorized Students/Users of Data Exporter;
- Consultants and Contractors of the Data Exporter
- Affiliates and agents of the Data Exporter; and/or
- third parties with which the Data Exporter conducts business.

#### **Categories of data**

The personal data transferred concern the following categories of data:

Any personal data comprised in Student Data. "Student Data" means all data and information submitted by Students granted access to a Zenler Site/Service account by a Customer and may include contact details, billing data, course data, messages, files, comments and links, but does not include Zenler Products or the Services.

**Special categories of data**

Data Exporter will **not** submit sensitive personal data to the Data Importer through the Services as per Zenler terms of service.

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic or biometric data
- Health; and
- Sex life.

**Processing operations**

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

The personal data transferred will be processed in accordance with the Agreement and any Order Form and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain and update the Services provided to the Data Exporter
- To provide customer and technical support to the Data Exporter; and
- Disclosures in accordance with the Agreement, as compelled by law.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: Rakesh Vallil

Authorised Signature  .....

**Appendix 2**

**to the Standard Contractual Clauses**

This Schedule 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(d) and 5(c) (or document/legislation attached):**

The Data Importer has implemented and will maintain appropriate technical and organisational measures to protect the personal data against misuse and accidental loss or destruction as set forth in Zenler's Security Practices in the Section 5 of DPA.

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: Rakesh Vallil

Authorised Signature ..... 

24/05/2018 03:21:51 PDT