

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is made by and between CampusLogic, Inc., a Delaware corporation (“**CampusLogic**”) and the Customer identified on any applicable Subscription Order Form (“**Customer**”).

This DPA, including its Schedules and Appendices forms part of and is subject to the terms of the CampusLogic Terms and Conditions or other written or electronic agreement between CampusLogics and Customer for the purchase of services from CampusLogic (identified either as “Services” or otherwise in the applicable agreement, and hereinafter defined as “**Services**”) (the “**Agreement**”) to reflect the parties’ agreement with regard to the Processing of Personal Data. This DPA shall be effective for the term of the Agreement.

1. Definitions

1.1. For the purposes of the DPA:

1.1.1. “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data;

1.1.2. “**Customer Personal Data**” means the Personal Data described under Schedule 1 of this DPA that is subject to Data Protection Legislation, in respect of which Customer is the Controller;

1.1.3. “**CCPA**” means the California Consumer Privacy Act;

1.1.4. “**Data Protection Legislation**” means all applicable legislation relating to data protection and privacy including without limitation the CCPA and the European Data Protection Laws;

1.1.5. “**European Data Protection Laws**” means the GDPR, together with any applicable national implementing laws in any Member State of the European Economic Area (EEA), and the United Kingdom (UK) Data Protection Act 2018, each as amended, repealed, consolidated or replaced from time to time;

1.1.6. “**GDPR**” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**EU GDPR**”) and the EU GDPR in such form as incorporated into the laws of the UK (“**UK GDPR**”), each as amended or replaced from time to time;

1.1.7. “**Personal Data**”, “**Data Subject**”, “**Personal Data Breach**” and “**Processing**” will each have the meaning given to them in the European Data Protection Laws;

1.1.8. “**Processor**” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, including as applicable any “service provider” as defined under the CCPA; and

1.1.9. “**Standard Contractual Clauses**” means Standard Contractual Clauses approved by the European Commission with Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, supplemented, updated or replaced from time to time.

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Processing of Customer Personal Data

- 2.1. Each of Customer and CampusLogic will comply with their respective obligations under the Data Protection Legislation. Customer shall ensure that Customer has provided any required notice to Data Subjects and has obtained (or will obtain) all rights and consents (if required) which are necessary for CampusLogic to Process Customer Personal Data in accordance with this DPA.
- 2.2. The provisions in this Section 2.2 shall apply to the extent CampusLogic's processing of Customer Personal Data is subject to the European Data Protection Laws.
 - 2.2.1. The parties acknowledge and agree that Customer is the Controller and CampusLogic is the Processor of Customer Personal Data. CampusLogic will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions, including with respect to transfers of Customer Personal Data. CampusLogic is hereby instructed to Process Customer Personal Data to the extent necessary to enable CampusLogic to provide the Services in accordance with the Agreement.
 - 2.2.2. If CampusLogic cannot process Customer Personal Data in accordance with Customer's instructions due to a legal requirement under any applicable law of the European Union, European Union member states or the UK, CampusLogic will (i) promptly notify Customer of such inability, providing a reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law; and (ii) cease all Processing of the affected Customer Personal Data (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as Customer issues new instructions with which CampusLogic is able to comply. If this provision is invoked, CampusLogic will not be liable to Customer under the Agreement for failure to perform the Services until such time as Customer issues new instructions.
 - 2.2.3. CampusLogic will provide Customer with reasonable assistance to facilitate conducting data protection impact assessments and consultation with data protection authorities, if Customer is required by the European Data Protection Legislation to engage in such activities, and solely to the extent that such assistance is necessary and relates to the Processing by CampusLogic of Customer Personal Data, taking into account the nature of the Processing and the information available to CampusLogic.
 - 2.2.4. CampusLogic will notify Customer without undue delay after it becomes aware of any Personal Data Breach affecting any Customer Personal Data. At Customer's request CampusLogic will promptly provide Customer with all reasonable assistance necessary to enable Customer to notify relevant security breaches to the competent data protection authorities and/or affected Data Subjects, if Customer is required to do so under the European Data Protection Legislation. Customer is solely responsible for complying with Personal Data Breach notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breach.
 - 2.2.5. CampusLogic will, at Customer's request, provide Customer with all information necessary to enable Customer to demonstrate compliance with its obligations under the European Data Protection Laws, and allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, to the extent that such information is within CampusLogic's control and CampusLogic is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party, and provided that such audits shall be carried out with reasonable notice during regular business hours not more often than once per year. CampusLogic will immediately inform Customer if, in its opinion, an instruction from Customer infringes the European Data Protection Legislation.

- 2.3. To the extent CampusLogic's Processing of Customer Personal Data is subject to the CCPA, CampusLogic shall not (1) retain, use, or disclose Customer Personal Data other than as provided for in the Agreement, as needed to perform the Services, to build or improve the quality of the Services to detect security incidents, to protect against fraudulent or illegal activity, to retain sub-Processors in compliance with Section 6, or as otherwise permitted by the CCPA; or (2) sell Customer Personal Data.

3. Cross-border Transfers

- 3.1. If the Processing of Customer Personal Data involves transfers of Customer Personal Data from the EEA, Switzerland or the UK to any third country that does not ensure an adequate level of protection under the Data Protection Legislation, then the parties agree to be bound by the terms of the Standard Contractual Clauses and their Module Two (Controller to Processor transfers) attached to this DPA as Schedule 2, which form part of, and are incorporated into, this DPA. Each of CampusLogic's and the Customer's entering into this DPA shall be treated as, respectively, CampusLogic's and the Customer's signature of Annex I, Section A, of the Standard Contractual Clauses as of the date this DPA becomes binding on the parties thereto.
- 3.2. Insofar as the transfer of Personal Data is subject to, respectively, the Data Protection Legislation of Switzerland ("**Swiss Data Protection Laws**") and the Data Protection Legislation of the United Kingdom ("**UK Data Protection Laws**"), the following provisions apply: (a) the Swiss Federal Data Protection and Information Commissioner and the Information Commissioner will be the competent supervisory authorities for, respectively, transfers of Personal Data from Switzerland and transfers of Personal Data from the United Kingdom under Clause 13 of the Standard Contractual Clauses; (b) the parties agree to abide by the EU GDPR standard in relation to all Processing of Personal Data that is governed by Swiss Data Protection Laws and by the UK Data Protection Laws standard in relation to all Processing of Personal Data that is governed by UK Data Protection Laws; (c) the term 'Member State' in the Standard Contractual Clauses will not be interpreted in such a way as to exclude Data Subjects in Switzerland and the UK from the possibility of suing for their rights in their place of habitual residence (Switzerland or the UK, as applicable) in accordance with Clause 18(c) of the Standard Contractual Clauses; (d) references to the 'GDPR' and its provisions in the Standard Contractual Clauses will be understood as references to Swiss Data Protection Laws or, as applicable, UK Data Protection Laws; (e) all references to the "European Economic Area" or the "European Union" in the Standard Contractual Clauses shall be deemed to refer to, respectively, Switzerland and the UK, (f) for transfers of Personal Data governed by UK Data Protection Laws, Clause 17 of the Standard Contractual Clauses is replaced to provide that the Standard Contractual Clauses are governed by the laws of England and Wales, and for transfers of Personal Data governed by Swiss Data Protection Laws, Clause 17 of the Standard Contractual Clauses is replaced to provide that the Standard Contractual Clauses are governed by the laws of Switzerland; and (g) for transfers of Personal Data governed by UK Data Protection Laws, the courts under Clause 18 of the Standard Contractual Clauses shall be the courts of England and Wales, and for transfers of Personal Data governed by Swiss Data Protection Laws, the courts under Clause 18 of the Standard Contractual Clauses shall be the competent courts of Switzerland. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

4. Confidentiality

- 4.1. CampusLogic will ensure that any person whom CampusLogic authorizes to Process Customer Personal Data on its behalf is subject to confidentiality obligations in respect of that Customer Personal Data.

5. Security Measures

- 5.1. CampusLogic will implement appropriate technical and organisational measures to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data.
- 5.2. CampusLogic will provide Customer with reasonable assistance as necessary for the fulfilment of Customer's obligation to keep Customer Personal Data secure.

6. Sub-Processing

- 6.1. Customer authorizes CampusLogic to appoint sub-Processors to perform specific services on CampusLogic's behalf which may require such sub-Processors to Process Customer Personal Data. CampusLogic will inform Customer of any intended changes concerning the addition or replacement of any sub-Processors and Customer will have an opportunity to object to such changes on reasonable grounds within fifteen (15) business days after being notified. If the parties are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.
- 6.2. CampusLogic will enter into an agreement with the sub-Processor that imposes on the sub-Processor substantially the same obligations that apply to CampusLogic under this DPA. Where any of its sub-Processors fails to fulfil its data protection obligations, CampusLogic will be liable to Customer for the performance of its sub-Processors' obligations.

7. Data Subject Rights

- 7.1. CampusLogic will provide Customer with assistance necessary for the fulfilment of Customer's obligation to respond to requests for the exercise of Data Subjects' rights relating to Customer Personal Data. Except as required by law, CampusLogic shall not respond to such requests without Customer's prior written consent and written instructions and Customer shall be solely responsible for responding to such requests.

8. Return or Deletion of Customer Personal Data

- 8.1. CampusLogic will return or delete, at Customer's choice, Customer Personal Data to Customer after the end of the provision of Services relating to the Processing, and delete existing copies unless the applicable law of the European Union, European Union member state or UK law requires storage of the data.

9. Liability

- 9.1. Each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.
- 9.2. Customer acknowledges that CampusLogic is reliant on Customer for direction as to the extent to which CampusLogic is entitled to Process Customer Personal Data on behalf of Customer in performance of the Services. Consequently CampusLogic will not be liable under the Agreement for any claim brought by a Data Subject arising from any action or omission by CampusLogic, to the extent that such action or omission resulted from Customer's instructions or from Customer's failure to comply with its obligations under Data Protection Legislation.

10. General Provisions

- 10.1. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail.

SCHEDULE 1

Decription of Processing

- **Categories of Data Subjects:** Customer's students, parents and other individuals whose data may be included in Customer Data provided to CampusLogic in connection with the Services by Customer, and third parties on behalf of or pertaining to Customer.
- **Types of Personal Data:** Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, such as names, email address, IP address, social security numbers, contact details, non-public education records related to financial aid.
- **Subject-Matter and Nature of the Processing.** The subject-matter of Processing of Customer Personal Data by CampusLogic is the provision of the Services to Customer that involves the Processing of Customer Personal Data. Customer Personal Data will be subject to those Processing activities which CampusLogic needs to perform in order to provide the Services pursuant to the Agreement or as otherwise authorized in the Agreement.
- **Purpose of the Processing.** Customer Personal Data will be Processed by CampusLogic for purposes of providing the Services set out into the Agreement or as otherwise authorized in the Agreement.
- **Duration of the Processing.** Customer Personal Data will be Processed for the duration of the Agreement, subject to Section 8 of this DPA.
- **Rights and Obligations of the Controller:** As described in the DPA.

SCHEDULE 2
STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
- (c) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (d) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

To the Standard Contractual Clauses

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:	As provided on any applicable Subscription Order Form
Address:	As provided on any applicable Subscription Order Form
Contact person's name, position and contact details:	As provided on any applicable Subscription Order Form
Activities relevant to the data transferred under these Clauses:	A customer of the data importer.
Signature and date:	Signature _____ Name _____ Title _____ Date Signed _____
Role (controller/processor):	Controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:	CampusLogic, Inc.
Address:	1340 S. Spectrum Blvd., Suite 200, Chandler, AZ 85256, United States
Contact person's name, position and contact details:	Chris Chumley, President & COO chris.chumley@campuslogic.com
Activities relevant to the data transferred under these Clauses:	Provider of a higher education financial aid software-as-a-service
Signature and date:	Signature _____ Name _____ Title _____

	Date Signed _____
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The categories of data subjects described in Schedule 1 to the DPA to which these Clauses are attached.

Categories of personal data transferred:

The categories of personal data described in Schedule 1 to the DPA to which these Clauses are attached.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

As described in Schedule 1 to the DPA to which these Clauses are attached.

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis):

The frequency of the transfer is continuous (for as long as the Customer uses the Services).

Nature of the processing:

As described in Schedule 1 to the DPA to which these Clauses are attached.

Purpose(s) of the data transfer and further processing:

As described in Schedule 1 to the DPA to which these Clauses are attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The duration specified in Clause 8.5 of the Standard Contractual Clauses and in the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The competent supervisory authority communicated by Customer to CampusLogic.

ANNEX II
To the Standard Contractual Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.