DATA PROCESSING AGREEMENT

This agreement is between _____, a business formed under the laws of _____ with its registered address at _____ (hereafter, "Controller"); and MemberVault, LLC., a company formed under the laws of the State of Washington (hereafter, "Processor", “MemberVault”).

1. GENERAL

This data processing agreement (the "Processing Agreement", “DPA”) sets out the terms and conditions for the processing of Personal Data as it is defined below. The processing of personal data is carried out in accordance with the Terms and Conditions and our Privacy Policy with respect to the provisions and use of MemberVault’s online course creation platform to which the Controller has agreed to and accepted to be bound when Controller created their account on MemberVault’s platform.

You, as the Controller, determine the purpose and methods that we can process Personal Data under. Therefore, you control the process of Personal Data processing. The Processor, in this case MemberVault, processes Personal Data on behalf of the Controller. Any Personal Data processing will take place strictly in accordance with this Processing Agreement.

The purpose of this Processing Agreement is to comply with the obligations and regulations set forth in the Data Protection Legislation (as defined below), according to which whenever Personal Data is processed by a Processor on behalf of a Controller, it must be affirmed by a written agreement.

This Data Processing Addendum (hereafter “DPA” or “Agreement”) between MemberVault LLC (hereafter “MemberVault”) and You supplements, and if necessary, amends our Privacy Policy and Terms and Condition.

MemberVault is a Software as a Service (“SAAS”) business, and as such, is both a data controller and data processor. To carry out its business, at times MemberVault will share personal data with third-party companies. All the necessary protocols and precautions will

be maintained to ensure that both MemberVault and You are complying with the General Data Protection Regulation ("GDPR").

Before MemberVault will enter into a business arrangement with You, You need to accept this DPA. You can accept it on your behalf or on behalf of a Customer.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have read and understand what the terms in this Data Processing Addendum mean, (b) that you have full legal authority to accept on behalf of Customer and that you acceptance binds Customer to this DPA terms; and (c) you accept these DPA terms on behalf of Customer. In the event that you do not have full legal authority to accept on behalf of Customer and bind Customer to this Agreement, please refrain from accepting.

1. **DEFINITIONS UNDER GDPR**

EU GDPR — European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons regarding the processing of personal data and movement of such data. This Regulation repealed the Directive 95/46/EC.

European Data Protection Legislation — this is in reference to either (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

Personal data — any information that will make the individual directly or indirectly identifiable. Information such as the individual's name, last name, phone number, date of birth, social security number are all considered personal data because they can easily identify the individual in question. Other information, such as geographic location, IP address, web cookies, can also be considered personal data if they can help to identify the individual either by themselves or as part of a whole. Moreover, even data that is pseudonymous can be considered personal data if identifying the person is relatively easy.

Data controller — Data controller is the person or individual who makes decisions about the collected data-specifically how and why the personal data will be processed. MemberVault is a SAAS business, and as such is both a data controller and a data processor.

Data processor —Data processor is a third-party individual or business that actually processes the collected personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. Data processors can be email service providers, cloud based storage softwares or services, and many others.

Data subject — The person whose data is processed. Our data subjects are our customers and clients, website visitors, and potential clients who visit membervault.co or /*.vipmembervault.com.

2. **PROCESSING UNDER THE AUTHORITY OF THE CONTROLLER OR PROCESSOR**

As the data processor or any person who is acting under the authority of Membervault who has access to personal data, must only process that data under the authority

3. **THE RESPONSIBILITIES AND OBLIGATIONS OF BOTH CONTROLLER AND PROCESSOR**

The Controller agrees to:

(a) process Personal Data according to the Data Protection Legislation and any related ordinances, regulations and guidelines that are issued by relevant and competent authorities; and

(b) provide a written, documented instruction on the processing of Personal Data to the Processor when required.

The Processor agrees to:

(a) only process Personal Data as per Controller’s specific documented instructions based on the Terms and Conditions and this DPA. When it comes to processing Personal Data, the Processor will not do anything that is not specifically instructed by the Controller. The only exception to this is if the Processor is required to comply with a Legislation that Processor is subject to. And even in such a case, the Processor is obligated to notify the Controller of that circumstance before Personal Data is processed.

(b) keep all Personal Data strictly confidential and take measures to ensure that any person authorized to process Personal Data has agreed to comply with confidentiality obligations regarding Personal Data;

(c) only process Personal Data in accordance with Data Protection Legislation and any related ordinances and regulations that are issued by competent and valid authorities;

(d) comply with all the decisions and judgments, including settlements agreements, that were entered by a competent authority, court, or even an arbitration tribunal regarding Personal Data;

(e) notify the Controller immediately if a Controller's instruction violates the Data Protection Legislation or infringes any other applicable data protection regulation.

(f) whenever Processor has access to the relevant Personal Data, if possible and necessary, Processor will aid the Controller to ensure that Controller is legally compliant with the Data Protection Legislation. Such aid can be technical and organizational security measures to make sure the Controller is following the Data Protection Legislation in all instances, including when the Data Subject exercises their rights under the Data Protection Legislation.

(g) keep a written record of all data processing activities relating to Personal Data in accordance with the Data Protection Legislation requirements; and

(h) provide the Controller with information and documentation showing that Processor is fulfilling its obligations under this DPA, if Controller requests such information.

4. TERM AND TERMINATION OF DPA

The terms in this Data Processing Agreement will go into effect as of the Effective Date located on the bottom of this Processing Agreement and will remain in effect for as long as the Processor processes Personal Data on behalf of the Controller, notwithstanding expiration of the Terms, they will remain in effect until either all the customer data has been deleted, the terms automatically expire.

If the Processor, for whatever reason, stops processing Personal Data on behalf of the

Controller, then the Processor must promptly either return or if requested, delete and obliterate all personal information and data, unless legislation requires that such data be stored.

5. **DATA PROTECTION**

If the data subject is within the EU area, that subject's personal data will be controlled and processed by MemberVault located in the United States. All the GDPR guidelines will be followed, and the data subject will have the same rights and privileges that GDPR grants them.

6. **DATA SECURITY MATTERS**

The Processor understands and agrees that it must maintain appropriate technical and organizational measures to protect Personal Data against any unauthorized or unlawful processing, or unintentional, intentional, unauthorized or unlawful deletion, destruction, loss or disclosure taking into account the nature of the processing. All these security measures must at least maintain the level of security set forth in Data Protection Legislation and any related ordinances and regulations.

Only the people who need access in order for the Processor to meet its obligations and be able to process Personal Data will have access to that Personal Data. The Processor will ensure that those people who have access to the Personal Data are complying with the Data Protection Legislation.

If a data breach takes place, the Processor must inform the Controller about that breach without undue delay. Moreover, if requested by the Controller and if the Processor actually has access to, the Processor must provide certain information that is outlined below to the Controller.

7. **INFORMATION THE PROCESSOR MUST PROVIDE TO THE CONTROLLER IF REQUESTED IN CASE OF PERSONAL DATA BREACH**

The Processor must provide to the Controller details about the data breach such as what

kind of data was compromised, how many data subjects were affected. Furthermore, the Processor must state as best as it can the consequences that will likely happen as a result of this data breach. Lastly, the Processor must inform the Controller about any steps that the Processor took or will take to address and fix the data breach, and what, if any steps are going to be taken to address and alleviate the harm that was caused to the data subjects of the personal data breach.

If the Processor cannot provide the entire information stated above to the Controller at the same time, the Processor may provide the information in phases without undue delay. The Controller must be given contact information for the person responsible for handling relevant Personal Data Breach.

8. TRANSFERRING PERSONAL DATA

The Processor is a Software as a Service (SAAS) business and may transfer Personal Data to a country outside the European Union ("EU"). However, the Processor must comply with the provisions and regulations under the Data Protection Legislation and agrees to take all the necessary and required steps to ensure that the Controller will also be able to comply with those provisions.

Processor also has the authority to enter into an agreement with any and as many sub-processors as need be to process Personal Data on behalf of the Controller given that Processor will make sure that all the sub-processors are complying with the Data Protection Legislation and any relevant provisions.

9. ADDITIONAL MISCELLANEOUS CLAUSES

If at any point any of the provisions or clauses under this Processing Agreement become invalid or unenforceable, all the other remaining parts under this DPA are valid and will continue in full force and the DPA will continue to be enforceable and valid. The Controller and the Processor must do their best to agree upon any necessary and reasonable adjustments and amendments of this DPA in order to protect the interests of both the Controller and the Processor and the main objectives of this DPA at the time of execution.

10. NO ASSIGNMENTS UNDER THIS DPA

This DPA is only between the Processor and the Controller. Without a prior written permission, this DPA cannot be assigned to any other parties that are not part of this DPA at the time of its execution. The duties and obligations laid out in this Processing Agreement are binding on the parties and not transferable or assignable, unless approved previously by a separate written agreement.

11. MODIFICATIONS AND AMENDMENTS TO THE PROCESSING AGREEMENT

Any amendment, change or alteration of this Processing Agreement must be made in writing and duly signed by both Parties in order to become valid and effective.

If there is a discrepancy between this Processing Agreement and the Terms and Conditions, then this DPA will prevail when it comes to processing of Personal Data.

12. GOVERNING LAW AND DISPUTE RESOLUTION

This Data Processing Agreement shall be governed by the substantive laws of the State of Washington. If there are any disputes, controversies or claims that rise out of or are connected with this DPA, it's potential breach, termination or any other clauses in the Processing Agreement then those shall be settled by an arbitration that will be submitted to the American Arbitration Association. The arbitrator shall follow any applicable federal law and Washington State Law in making a decision as to the award, decision, settlement and all arbitral proceedings shall be in English. Judgment on the award may be entered in any court having jurisdiction. Both the Controller and the Processor accept, acknowledge and agree that the arbitrators' decision will be final and binding to the fullest extent permitted by law and enforceable by any court having jurisdiction.

This Data Processing Agreement can be signed in part and both Controller and Processor can have a signed copy, and this entire Agreement will be enforceable in full.

Effective Date: 07/21/2020

MemberVault, LLC

Processor's Signature:

Name: Mike Kelly, Chief Technical Officer

Name of Business:

_____

Controller's Signature: _____

Controller's Name: _____

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. Read this Standard Contractual Clauses in their entirety online.

Name of the data exporting organisation:
Address: _____
_____
E-mail: _____
(the data exporter);

And

Name of the data importing organisation: **MemberVault, LLC**
Address: 1037 NE 65th St. #80675, Seattle, Washington, 98115, United States
E-mail: hello@membervault.com
(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.

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;

(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.

2. Details of the transfer

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

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 subprocessor 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.

4. Obligations of the data exporter

The data exporter agrees and warrants:

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

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

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and
against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

5. Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:

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

(ii) any accidental or unauthorised access; and

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

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

advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security
measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

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 of 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.

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.

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).

9. Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely *(enter the name of the state/country where the data exporter is established)* .

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.

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 (1). 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 *(enter the name of the state/country where the data exporter is established)*
.

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

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: _____

Position: _____

Address: _____

_____

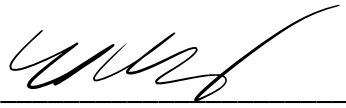
Signature: _____

On behalf of the data importer:

Name: **Mike Kelly**

Position: Chief Technology Officer, CTO

Address: 1037 NE 65th St. #80675, Seattle, Washington, 98115, United States

Signature: 

Appendix 1 to the Standard Contractual Clauses

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

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

Data exporter

The data exporter is *(briefly specify your activities relevant to this transfer)* .

Data importer

The data importer is an online Software as a Service ("SAAS") platform that enables its users/account holders to create online courses, one-on-one offerings, online memberships, and more. The SAAS platform enables delivery of said online creations to its students where students get connected to MemberVault account holders who are the instructors and teachers of the above described online creations.

Data subjects

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

Users (MemberVault account owners and students) using the MemberVault platform.

Categories of data

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

First name, last name (optional), email address, what email service provider the user uses (optional), IP address, credit card information (although this information is not stored by MembeVault).

Special categories of data (if appropriate)

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

Not applicable for this process.

Processing operations

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

Registering both the account holder and the students to MemberVault accounts and are processed to log into their accounts.

Personal data is also processed to provide technical support to both account holders and students if necessary.

The student and account holder data is processed to communicate with them via email in case of failed payments.

Personal data is also processed for usage trends such as registering the last time a user has been active on the account, the specific products they have looked at, and for overall improvement of the MemberVault platform as it serves its customers.

On behalf of the data exporter:

Name: _____
Position: _____
Address: _____
_____

Signature: _____

On behalf of the data importer:

Name: **Mike Kelly**
Position: Chief Technology Officer, CTO
Address: 1037 NE 65th St. #80675, Seattle, Washington, 98115, United States

Signature: 

Appendix 2 to the Standard Contractual Clauses

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

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

The Data Importer, in this case MemberVault, LLC will implement all the technical and organizational security measures, and will carry out its obligations and responsibilities as set forth in its Data Processing Agreement ("DAP") that parties must sign.

Indemnification Clause

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim