DATA PROCESSING AGREEMENT

This agreement reflects the parties' agreement with respect to the Processing of Personal Data by MemberVault, LLC (hereafter, "Processor", "MemberVault") and you (hereafter, "You", "Controller", "Customer", "Permitted Affiliates") in connection with the provisions and use of MemberVault's online business platform.

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 business platform to which the Controller has agreed to and accepted to be bound when Controller created their account on MemberVault's platform. In case of any conflict or inconsistency, this DPA will take precedence over the terms of the Terms and Conditions or Privacy Policy to the extent of such conflict or inconsistency.

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 a 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 your 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.

2. DEFINITIONS UNDER GDPR

Data Protection Laws - all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA (California Civil Code Sec. 1798.100 et seq. also known as the California Consumer Privacy Act of 2018), the data protection and privacy laws of Australia and Singapore, and the UK GDPR as retained in UK domestic law; in each case as amended, repealed, consolidated or replaced from time to time.

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.

UK GDPR - The EU GDPR as retained in UK law by the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and as further amended from time to time. References to EU GDPR in this Agreement shall, where the context requires, be read to include UK GDPR.

Permitted Affiliates - any of your Affiliates that (i) are permitted to use the MemberVault's online business platform pursuant to the Agreement, but have not signed their own separate agreement with us and are not a "Customer" as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws or UK GDPR.

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.

Personal Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the online business platform. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

Processing - any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

Processor - a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

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.

Sub-Processor - means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the online business platform. Sub-Processors may include third parties or our Affiliates but will exclude any MemberVault employee or consultant.

3. 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.

4. THE RESPONSIBILITIES AND OBLIGATIONS OF BOTH CONTROLLER AND PROCESSOR

The Controller agrees:

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

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of customer data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Controller for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of this Agreement; (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through MemberVault's online business platform.

You will inform us without undue delay if you are not able to comply with your responsibilities under this agreement or applicable Data Protection Laws.

(b) the Agreement (including this DPA), together with your use of the online business platform in accordance with the Agreement, constitute your complete Instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the subscription term that are consistent with the Agreement, the nature and lawful use of the online business platform.

(c) independently determine whether the data security provided for in the Subscription Service adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including protecting the security of Personal Data in transit to and from the Subscription Service (including to securely backup or encrypt any such Personal Data).

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. If Processor becomes aware that Personal Data cannot be processed in accordance with your instructions or the Terms and Conditions of this DPA due to a legal requirement under any applicable law, MemberVault will (i) promptly notify Controller of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Controller issues new Instructions with which Processor is able to comply. If this provision is invoked, MemberVault will not be liable to Controller under the Agreement for any failure to perform the applicable services until such time as Controller issues new lawful Instructions to the Processor.

(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 (whether a contractual or statutory duty);

(c) inform the Controller if a data breach takes place 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 further outlined below in this agreement to the Controller.

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

(e) 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;

(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, including but not limited to the right of access, right to erasure, right to rectification, right to restriction of processing, right to data portability, and right to object to processing. Processor will respond to any such requests within a reasonable timeframe and will notify Controller without undue delay upon receiving a data subject rights request that relates to Personal Data processed on Controller's behalf.

(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.

5. 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 DPA, they will remain in effect until either all the Customer Data has been deleted.

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.

6. DATA PROCESSING LOCATION

MemberVault processes and stores Personal Data on infrastructure hosted by Amazon Web Services (AWS) in the us-east-1 region (US East, N. Virginia), United States.

Controllers whose Personal Data originates from the European Union or United Kingdom should be aware that this constitutes an international transfer of Personal Data outside the EU/EEA and UK respectively. MemberVault takes all necessary steps to ensure such transfers are carried out in accordance with applicable Data Protection Legislation.

For transfers of Personal Data from the European Union, MemberVault relies on the Standard Contractual Clauses as annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, as incorporated into this Agreement.

For transfers of Personal Data from the United Kingdom, MemberVault relies on the UK Addendum to the EU Standard Contractual Clauses as issued by the UK Information Commissioner's Office, which is available to UK Controllers upon request by contacting hello@membervault.co.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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: 6/25/2026

MemberVault, LLC - Processor's Signature: 

Name: Mike Kelly, Chief Technical Officer

Name of Business: _____

Controller's Signature: _____

Controller's Name: _____

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

"Standard Contractual Clauses" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, as may be amended, superseded or replaced. The Processor agrees to remain compliant with the Standard Contractual Clauses.

For transfers of Personal Data originating from the United Kingdom, the UK Addendum to these Standard Contractual Clauses (as issued by the UK Information Commissioner's Office) shall apply in

addition to and form part of these Standard Contractual Clauses. UK Controllers may request a copy of the UK Addendum by contacting hello@membervault.co.

Appendix 1 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):

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 ("DPA") 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 defense and settlement of the claim.