sign here

Client Data Processing Agreement

This Data Processing Agreement, including Schedules 1, 2, 3, 4, and 5, attached hereto and hereby incorporated by this reference (together, this "**DPA**") is entered into effective as of (the "**Effective Date**"), by and between Pantheon Systems, Inc., a Delaware corporation ("**Pantheon**") with its principal place of business at 717 California Street, 3rd Floor, San Francisco, California and [Client Name], a [state of business] corporation with its principal place of business at [business address] ("Customer"). Pantheon and Customer are sometimes referred to herein each as a "**Party**" and together as the "**Parties.**"

In consideration of the mutual promises, covenants, and conditions hereinafter set forth, the receipt and sufficiency of which is hereby acknowledged, the Parties hereto further agree as follows:

1. Definitions. When used in this DPA, the terms set forth below and those defined throughout the DPA when initially capitalized shall have the meanings ascribed to them.

1.1 "Business Purpose" means use of Personal Information for Pantheon's or Customer's operational purposes as set out in the existing arrangement(s) entered separately between the Parties ("**Agreement**") or other notified purposes, provided that the use of Personal Information is reasonably necessary and proportionate to achieve the operational purpose for which the Personal Information was collected or processed or for another operational purpose that is compatible with the context in which the Personal Information was collected. The Business Purpose may be as further listed in **Schedule 1**.

1.2 "California Consumer Privacy Act of 2018" or **"CCPA"** means the California Consumer Privacy Act of 2018, as amended from time to time (Cal. Civ. Code §§ 1798.100 to 1798.199).

1.3 "Commercial Purpose" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

1.4 "Controller" means the entity that determines the purposes and means of the Processing of Personal Data. In this DPA, Customer is the Controller. Under the CCPA, Controller is referred to as "**Business**."

1.5 "Customer Data" means information and data, including Personal Data, acquired from or provided by Customer. Customer Data does not include Pantheon Data.

1.6 "Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Economic Area (the "**EEA**"), Switzerland, the United Kingdom (the "**UK**"), and the United

States of America (the "**U.S.A.**") applicable to the Processing of Personal Data for Business Purpose, including GDPR and CCPA, and to the extent applicable, the data protection or privacy laws of any other country.

1.7 "Data Subject" means (i) an identified or identifiable natural person who is in the EEA, the Switzerland, the UK, or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA.

1.8 "GDPR" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9 "Pantheon Data" means all information and data Pantheon has acquired from a source other than Customer.

1.10 "Personal Data" or "**Personal Information**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

1.11 "Processing" or **"Process"** mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, storage, retrieval, use, organization, recording, adaptation, alternation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.12 "Processor" means the entity which Processes Personal Data on behalf of the Controller. In this DPA, Pantheon is the Processor.

1.13 "Restricted Transfers" means either (i) a transfer of Personal Data from Customer to Pantheon; or (ii) an onward transfer of Personal Data from Pantheon to a Sub-Processor; in each case, where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the Standard Contractual Clauses or other transfer mechanism permitted by applicable Data Protection Laws and Regulations.

1.14 "Services" mean services that Pantheon provides to Customer in accordance with the Business Purpose.

1.15 "Service Provider" is as defined in CCPA Section 1798.140(v).

1.16 "Standard Contractual Clauses" or "**SCC**" mean the agreement for the transfer of Personal Data to processors established in third countries that do not ensure an adequate level of data protection, attached hereto as **Schedule 4,** pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses.

1.17 "Sub-Processor" or "**Sub-Service Provider**" means an entity engaged by a Processor who agrees to receive from the Processor Personal Data exclusively intended for the processing activities to be carried out as part of the services.

1.18 "Supervisory Authority" means an independent public authority which is established by an EU Member

State pursuant to the GDPR.

2. Data Processing

2.1 Roles of the Parties. For purposes of this DPA, Customer is the Controller (or Business). Pantheon shall be a Processor or Service Provider of Customer or a Sub-Processor or Sub-Service Provider of Customer in such cases where Customer is a Processor for its customers. Where Pantheon acts as a Processor, Pantheon is obligated contractually and/or under Data Protection Laws and Regulations to flow down certain data protection related obligations to its appointed Sub-processors.

2.2 Customer's Processing of Personal Data. Customer shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations.

2.3 Pantheon's Processing of Customer Data. Pantheon shall Process Customer Data in accordance with the requirements of Data Protection Laws and Regulations. Pantheon shall treat Customer Data as confidential, and shall only Process Customer Data on behalf of and in accordance with Customer's instructions for the following purposes: (i) Processing in accordance with the Business Purpose; and (ii) Processing to comply with written instructions provided by Customer that are consistent with the Business Purpose.

2.4 Details of the Processing

The subject matter of Processing of Customer Data by Pantheon is the performance of the Services consistent with the Business Purpose. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in **Schedule 2** (Details of the Processing) to this DPA.

Pantheon shall certify that Customer Data has been processed in accordance with the CCPA, in the form provided in **Schedule 3**.

2.5 Obligations under CCPA. Customer discloses Customer Data that includes Personal Data to Pantheon solely for the Business Purpose. Pantheon will only retain, use and disclose Customer Data in a manner permitted under this DPA. Pantheon is prohibited from selling Personal Data and will refrain from taking any action that would cause a transfer of Customer's Data to qualify as a "sale" of personal information under the CCPA.

3. Rights of Data Subjects. To the extent legally permitted, Pantheon shall promptly notify Customer if Pantheon receives a request from a Data Subject to exercise a right of the Data Subject under GDPR or CCPA. The rights under GDPR include the following: right of access, right to rectification, erasure ("right to be forgotten"), restriction of Processing, data portability, right to object to the Processing, or right not to be subject to an automated individual decision-making, including profiling ("**GDPR Data Subject Request**"). The rights under CCPA include the following: right to notice, right to access, right to opt-out, right to deletion, and

right to equal services and prices ("**CCPA Data Subject Request**"). Taking into account the nature of the Processing, Pantheon shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to the appropriate data subject request (GDPR Data Subject Request or CCPA Data Subject Request) under Data Protection Laws and Regulations.

4. Customer Personnel

4.1 Confidentiality. Without prejudice to any existing contractual arrangements between the Parties, Pantheon shall treat all Customer Data as confidential and shall ensure that its employees, agents or contractors engaged in the Processing of Customer Data are informed of the confidential nature of Customer's Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

4.2 Reliability. Pantheon shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Customer who may have access to Customer Data.

4.3 Limitation of Access to Customer Data including Personal Data. Pantheon shall take reasonable steps to ensure that access to Customer Data is limited to those individuals who need to know or need to access the relevant Customer Data, as reasonably necessary for Business Purpose, and to comply with applicable Data Protection Laws and Regulations.

5. Sub-Processing

5.1 Appointment of Sub-Processors. Customer acknowledges and agrees that Pantheon may engage third-party Sub-Processors only in accordance with this DPA. Further, Pantheon shall maintain adequate written data protection agreement(s) with each Sub-Processor and should include terms that meet the requirements of Article 28(3) of the GDPR and applicable provisions under CCPA, to the extent applicable to the Business Purpose.

5.2 List of Current Sub-Processors. Pantheon shall maintain and make available to Customer the current list of Sub-Processors as set out at https://pantheon.io/gdpr/sub-processors.

5.3 Notification of New Sub-Processors. Pantheon may engage a new Sub-Processor only upon giving Customer prior written notice of the appointment of the new Sub-Processor including details of the Processing to be undertaken by the Sub-Processor, and provide Customer a reasonable opportunity to object to the appointment of the new Sub-Processor.

5.4 Approving Sub-Processors. If Customer reasonably believes that Pantheon's new Sub-Processor will violate Data Protection Laws and Regulations, Customer may provide a detailed objection to Pantheon's use of a Sub-Processor by notifying Pantheon within thirty (30) days after notice is provided. In the event Customer objects to a Sub-Processor, Vendor shall work with Pantheon in good faith to resolve the objection. If the parties are unable to come to a resolution, Pantheon may suspend or terminate those services which cannot be provided without use of the objected-to Sub-Processor.

5.5 Sub-Processor Compliance. Pantheon shall ensure that each Sub-Processor performs the obligations under Sections 2 (Data Processing), 3 (Rights of Data Subjects), 4 (Customer Personnel), 6 (Security), 7 (Return and Deletion of Customer Data) and 8 (Data Protection Impact Assessment), as they apply to Processing of Personal Data carried out by that Sub-Processor, as if it were party to this DPA in place of Pantheon. Subject to the limitations set out in this DPA and the applicable Agreement(s), Pantheon agrees to indemnify, defend, and hold Customer and its directors, officers, employees, lawyers, successors, assigns, agents, and affiliates against any and all claims, demands, actions, causes of action, lawsuits, judgments, costs, expenses, attorney and expert witness fees, and other liabilities of every nature, arising out of or related to Sub-Processor's act, error, or omission in complying with this DPA.

6. Security

6.1 Controls for the Protection of Pantheon Data. Taking into account the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, Pantheon shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to Customer Data); confidentiality; and integrity of Customer Data. Pantheon shall regularly monitor compliance with these measures.

6.2 Audits. Pantheon maintains an audit and compliance program. At Customer's written request and under reasonable confidentiality restrictions, Pantheon shall make available to Customer at least annually the results of third party audits.

6.3 Security Incident Management and Notification. Pantheon shall have in place an appropriate written security policy with respect to the Processing of Personal Data. Pantheon shall notify Customer without undue delay of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored, or otherwise Processed by Pantheon, or its Sub-Processors (a "**Security Incident**"). Pantheon shall keep Customer informed of all material developments in connection with the Security Incident, and cooperate with Customer and shall take such reasonable and necessary steps as are directed by Customer to assist in the investigation, mitigation and remediation of each Security Incident.

6.4 Notifications. To the extent permitted and required under applicable Data Protection Laws and Regulations, any notification to Customer of a Security Incident pursuant to Section 6.3 may, to the extent known at the time such notice is provided, at a minimum contains:

a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

the name and contact details of Pantheon's data protection officer where more information can be

obtained;

a description of the known consequences of the Security Incident; and

a description of the measures taken or proposed to be taken by Pantheon to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

7. Return and Deletion of Customer Data

7.1 Pantheon's and Sub-Processor's Return and Deletion of Customer Data. Upon termination or expiration of the Agreement, Pantheon shall delete or destroy Customer Data and securely destroy any existing copies in its possession or control in accordance with terms of the Agreement, this DPA and applicable Data Protection Laws and Regulations. Pantheon shall ensure that all such third parties securely destroy Customer Data in accordance with terms in this DPA.

7.2 Pantheon's Retention of Personal Data. Pantheon and its Sub-Processors may retain certain Personal Data to the extent required by applicable Data Protection Laws and Regulations, provided the confidentiality of all such Personal Data is adequately protected.

7.3 Written Certification. Pantheon shall provide to Customer written certification that Pantheon has fully complied with this Section 7 within fifteen (15) calendar days of Customer's written request.

8. Data Protection Impact Assessment. Upon Customer's request, Pantheon shall provide Customer reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's Personal Data Processing under this DPA. Pantheon shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 8, to the extent required under the GDPR.

9. Assistance to Pantheon. Pantheon shall make available to Customer all information reasonably necessary to demonstrate compliance with Customer's obligations under Article 28 of the GDPR.

10. Restricted Transfers. Pantheon participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework ("**Privacy Shield Framework**") for the transfer of Personal Data from the EEA and Switzerland to the U.S. Further, Pantheon uses the Standard Contractual Clauses, a form is set forth in **Schedule 5** to this DPA, as the transfer mechanism when Personal Data is transferred from the EEA to a "third country" (as mentioned in GDPR) other than the U.S. Customer will comply with the appropriate transfer mechanism to transfer Personal Data out of the EEA and Switzerland.

11. General Terms

11.1 Interpretation. This DPA sets forth the entire agreement and understanding of the Parties, and merges and supersedes all prior agreements, writings, commitments, discussions and understandings between them, relating to the specific subject matter herein. No modification, amendment, or any waiver of any rights regarding this DPA shall be effective unless in writing signed by both Parties. No provision in any written order, purchase order or similar document submitted by Customer hereunder shall in any way

modify or append this DPA. All capitalized terms not defined herein shall have the meaning set forth in the applicable Data Protection Laws and Regulations. If any portion of this DPA is declared invalid or unenforceable for any reason, such portion is deemed severable herefrom and the remainder of this DPA shall be deemed to be, and shall remain, fully valid and enforceable and shall not affect any other term or provision. This DPA shall be interpreted and construed as if such invalid, illegal or unenforceable term had never been contained herein. When necessary for appropriate meaning, a plural shall be deemed to be the singular, a singular shall be deemed to be the plural, and a gender-neutral term shall be deemed feminine or masculine. Section headings are for convenience only and shall not be deemed to govern, limit, modify or in any other manner affect the scope, meaning or intent of the provisions of this DPA or any part thereof nor shall such captions otherwise be given any legal effect. This DPA shall be construed within its fair meaning and no inference shall be drawn against the drafting Party in interpreting this DPA. When used in this DPA, "**including**" shall mean "including, but not limited to." This DPA shall be binding upon and inure to the benefit of the Parties, and their respective heirs, permitted assigns, successors-in-interest, and legal representatives. This DPA may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. The Parties agree that electronic signatures of the Parties shall have the same force and effect as original signatures. Delivery of a copy of this DPA by facsimile, electronic mail as an attached file (e.g. .pdf), or by any other electronic means (e.g. DocuSign) shall be acceptable to bind the Parties and shall not in any way affect this DPA's validity.

11.2 Modifications due to changes in Data Protection Laws. Either Party may give the other Party at least thirty (30) calendar days' written notice to propose variations to this DPA that such Party reasonably considers to be necessary to address the requirements of any Data Protection Laws and Regulations. The Parties shall negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the notice as soon as is reasonably practicable.

11.4 Governing Law and Venue. Without prejudice to clauses 7 (Mediation and Jurisdictions) and 9 (Governing Law) of the Standard Contractual Clauses, this DPA shall be exclusively interpreted, construed and enforced under California (U.S.A.) law without reference to its choice of law rules and, if any federal right violation is alleged, the laws of the United States of America. Venue for any court action arising out of or relating to this Agreement shall be exclusively brought in the appropriate state court in the California Superior Court located in the City and County of San Francisco or any federal court in the Northern District of California and the Parties irrevocably consent to the jurisdiction of such courts for any permitted court action on any obligation hereunder, unless otherwise required by applicable Data Protections Laws and Regulations.

11.5 Assignment. Neither Party may assign, sublicense or otherwise transfer (by operation of law or otherwise) this DPA, or any of a Party's rights or obligations under this DPA, to any third party without the other Party's prior written consent, which consent must not be unreasonably withheld, delayed or conditioned; provided, however, that either Party may assign or otherwise transfer this DPA to a successor-

in-interest in connection with a merger, acquisition, reorganization, a sale of most or all of its assets, or other change of control. Any purported assignment or other transfer in violation of the DPA is void. Subject to the terms of this DPA, the DPA will bind and inure to the benefit of the Parties and their respective permitted successors and transferees.

11.6 Order of Precedence. If there is a conflict between this DPA related to the GDPR and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

By signing below, each Party acknowledges that it has read, understood and agrees to be bound by the terms and conditions of this DPA and that the person signing is duly authorized to do so.

PANTHEON SYSTEMS, INC. **"PANTHEON "** By: Name: Title: Date:	**CUSTOMER** Customer Legal Name: By: Name: Title: Date:

SCHEDULE 1

Business Purpose

Pantheon provides a centralized WebOps platform designed to increase productivity across collaborative teams supporting a website. Customer may provide Pantheon and its Sub-Processors with certain content for the foregoing purpose in accordance with and subject to the limitations of the underlying Agreement(s).

SCHEDULE 2

Details of the Processing

Nature and Purpose of Processing:

Pantheon will Process Personal Data as necessary to perform the Services pursuant to the Agreement(s).

Duration of Processing:

Pantheon will Process Customer Data for the duration of the Agreement, unless otherwise agreed upon in writing by the parties.

Categories of Data Subjects:

The Personal Data transferred concern the following categories of data subjects:

- Employees, agents, advisors, contractors, and freelancers of Customer, who are natural persons.
- Customers, business partners, Customers and subcontractors of Customer, who are natural persons.
- Employees or contact persons of Customer's customers, business partners, Customers and subcontractors.

Type of Personal Data:

The Personal Data transferred concern the following types of data:

- Name (first, last, middle, nickname etc.)
- Contact information (email, phone, physical address)
- **[INCLUDE ADDITIONAL CATEGORIES OF DATA PROCESSED]**

In all such cases of information processed by Pantheon on behalf of Customer and in accordance with and subject to the limitations set out in the Agreement(s), Personal Data processing is restricted by Pantheon where such processing would require Pantheon to apply a standard of protection more stringent or specific than reasonable technical, physical, and procedural safeguards against its unauthorized processing or disclosure.

SCHEDULE 3

Certification Of Compliance With Data Processing Agreement

(CCPA)

Pantheon Systems, Inc., a Delaware corporation, with its principal place of business at **717 California Street in San Francisco, CA 94108** ("Customer" or "**Service Provider**") hereby certifies as follows:

1. Customer and Pantheon Systems, Inc. ("**Pantheon**") executed a Data Processing Agreement ("**DPA**") on [date signed]
2. In accordance with Section 1798.140(w)(2)(B) of the California Consumer Privacy Act ("CCPA"), Service Provider certifies that it will comply with the terms and conditions of this DPA. Service Provider specifically represents and warrants that:
    a. It will retain, use, and disclose Customer Data in the manner permitted by the DPA, Agreement, and Data Protection Laws and Regulations and
    b. It is prohibited from selling Customer's Personal Information and will refrain from taking any action that would cause a transfer of Customer's Personal Information to qualify as a "sale" of personal information under the CCPA.

AS WITNESS the hands of the Parties the day and year first above written:

_____

"Customer" or "SERVICE PROVIDER"

By:

Name:

Date:

SCHEDULE 4

Standard Contractual Clauses

(Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel._____; fax _____; e-mail: _____

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organization: Pantheon Systems, Inc.

Address: 717 California Street, San Francisco, CA 94108

Tel. 855-927-9387; fax N/A; e-mail: legal@pantheon.io

Other information needed to identify the organisation: Not applicable.

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-

processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by

operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of 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 sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

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

(ii) any accidental or unauthorised access; and

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

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

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

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

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim 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.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the

data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses . Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred

to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature

(stamp of organisation)

Other information necessary in order for the contract to be binding (if any):

On behalf of the data importer:

Name (written out in full): **Ronak Ray**

Position: **General Counsel**

Address: 717 California Street, Second Floor, San Francisco, CA 94108

Other information necessary in order for the contract to be binding (if any):

Signature

(stamp of organisation)

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 (as defined above)

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

processes certain personal information in relation to its activities with providing a website.

Data importer (as defined above)

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

Data importer is a provider of website operations solution which Processes Personal Data upon the instruction of the data exporter in accordance with the terms of this Agreement.

Data subjects

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

- Employees, agents, advisors, contractors, and freelancers of Customer, who are natural persons.
- Customers, business partners, Customers and subcontractors of Customer, who are natural persons.
- Employees or contact persons of Customer's customers, business partners, Customers and subcontractors.

Categories of data

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

- Name (first, last, middle, nickname etc.)
- Contact information (email, phone, physical address)
- [INCLUDE ADDITIONAL CATEGORIES OF DATA PROCESSED]

Special categories of data (if appropriate)

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

For avoidance of doubt, the following are not prohibited by the underlying agreement between data exporter and data importer: Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data genetic data, concerning health, a natural person's sex life or sexual orientation. Further, in all such cases of information processed by data importer on behalf of data exporter and in accordance with and subject to the limitations set out in the Agreement(s), Personal Data processing is restricted by data importer where such processing would require data importer to apply a standard of protection more stringent or specific than reasonable technical, physical, and procedural safeguards against its unauthorized processing or disclosure.

Processing operations

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

The objective of Processing Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER **[CUSTOMER PLEASE SIGN]**
Name:
Authorized Signature

DATA IMPORTER
Name: **Ronak Ray**
Authorized 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 organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

For purposes solely of this Appendix, the terms “Data Controller” also means “data exporter” and “Data Processor” also means “data importer”.

This information security overview applies to Data Processor corporate controls for safeguarding personal data which is processed for, and transferred from, the data exporter. This Appendix enables the workforce to understand their responsibilities. Pantheon’s privacy practices are set out at https://pantheon.io/privacy including Pantheon’s compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, “Privacy Shield”). Some customer solutions may have alternate safeguards outlined under separate legal arrangements between data exporter and data importer. Without limiting the generality of the forgoing, Data Processor’s security program shall contain the following principles.

1. **Information Security Management.** Pantheon has a dedicated information security team consisting of a Director of Information Security, a team of Security Engineers responsible for the management of information security throughout the organization, and cross-functional executive leadership responsible for maintaining security and compliance throughout the organization. Pantheon’s Information Security Compliance Committee (ISCC) meets at least quarterly to review changes in the requirements for information security arising from changes in law, contractual requirements and the underlying business at Pantheon. The ISCC reviews and makes any necessary corresponding adjustments to policies, governance and program administration at least annually. Pantheon has further developed a body of written policies to establish a common understanding of rules and procedures governing the development, deployment, operation and management of the Pantheon WebOps offering to its customers.
2. **Business Continuity and Backups.** Pantheon applies a consistent unified framework for the

adoption, documentation and maintenance of business continuity plans. Pantheon's business continuity plans are designed to address priorities for testing and maintenance of Pantheon's business and information security requirements. Business continuity procedures are reviewed by the ISCC for potential or identified threats and tested annually with any findings assigned to information security professionals responsible for implementing additional safeguards. Regarding Pantheon's provision of services to Data Controller, website data in Pantheon systems is backed up daily to Pantheon's subprocessor and encrypted at rest. These backups are available to Data Controller for download, export or self-service rollback and recovery. Pantheon further applies regular database backups for production web development services backup data. Secondary sites are kept in a warm stated, ready to be failed over to, as configured by Data Controller. Pantheon performs a test restore of backup data on an annual basis to validate the business continuity program.

3. **Access Controls.** Pantheon applies measures designed to provide access to systems and data to only those individuals who have a specific authorized purpose for such use and with specific controls that protect personal data from being read, copied, modified or removed without authorization during processing or use and after storage to the extent required under the applicable customer agreement(s):

    a. **Platform Access Controls.** Pantheon will encrypt Data Controller Personal Data not intended for public or unauthenticated viewing when transferring Data Controller Personal Data over public networks. Pantheon will make available to Data Controller such tools as may be necessary and available to Pantheon to support further application of cryptographic protocol, such as TLS or SSH, for the secure transfer of Data Controller Personal Data to and from the Services over public networks. Pantheon applies standard encryption technologies to protect Data Controller data both at rest and in transit where appropriate. Pantheon establishes sessions to the Pantheon web servers utilizing Hypertext Transfer Protocol Secure (HTTPS) and automates adding and renewing Transport Layer Security (TLS) certificates for custom domains added to customer websites. Pantheon users authenticate to production servers over secure shell (SSH) encryption protocol using a uniquely assigned SSH key-pair in which the private key is enabled only with the internal user's unique username and SSH key stored in a hardware token. Pantheon will monitor use of privileged access and maintain security information an event management measures designed to i) identify unauthorized access and activity, ii) facilitate an appropriate response, and iii) to enable internal and independent third-party audits of compliance with documented Pantheon Risk Management and Information Security policy. Logs, in which privileged access and activity are recorded, will be retained in compliance with Pantheon's records retention standards. Pantheon will maintain measures designed to protect against unauthorized access, modification and accidental or deliberate destruction of such logs.

b. **Systems Access Controls.** In respect of any systems used to access Pantheon platform information containing Data Controller data, this paragraph shall apply. Access to system information is protected by multiple authentication and authorization mechanisms. Pantheon leverages SAML to manage access to corporate resources. Pantheon's vulnerability assessment consists of scanning server resources, identifying vulnerabilities, assessment of the vulnerabilities, and remediation. Vulnerability scans are performed periodically. To the extent supported by native device or operating system functionality, Data Processor will maintain computing protections for systems containing Data Controller Personal Data and all end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based antivirus and malware detection and removal that shall i) be regularly updated by central infrastructure and ii) logged to a central location, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements. In accordance with Pantheon's IT policies, all computers must either have antivirus software installed or alternative means to validate system integrity. Updates are pushed automatically and managed by the IT department.

c. **Physical Security**. The platform environment is administered remotely and all access must be performed through connections secured by strong authentication with applicable subprocessors (cf., Platform Access Controls above). Accordingly, Pantheon's subprocessors are required to maintain physical security at data center locations related to the services Pantheon provides to Data Controller. In lieu of any Data Processor or Data Controller audit access, each subprocessor provides industry standard reports which Pantheon will reasonably demand and assist Data Controller is gathering upon request. At a minimum, such physical access controls at all Pantheon and subprocessor locations shall consist of physical entry controls, such as barriers, card or digitally controlled entry points, surveillance cameras, and added security during non-working hours, to protect against unauthorized entry.

4. **Audit and Compliance**. Pantheon participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework ("Privacy Shield Framework") for the transfer of Personal Data from the EEA and Switzerland to the U.S. Pantheon will maintain a AICPA Service Organization Control 2, Type 2 report (the "SOC 2 Audit Report") in each case for the security and availability related controls of the information systems (including procedures, people, software, data, and infrastructure) that are used by Pantheon when processing Data Controller personal data. Security and legal professionals coordinate to develop appropriate compliance initiatives to ensure we identify, monitor, and take appropriate steps towards laws and regulations.

DATA EXPORTER **[CUSTOMER PLEASE SIGN]**

Name:

Authorized Signature

DATA IMPORTER
Name: **Ronak Ray**
Authorized Signature