Vendor 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 effect as of the signature date below (the "**Effective Date**"), between Pantheon Systems, Inc., a Delaware corporation ("**Pantheon**") with its principal place of business at 717 California Street, 3rd Floor, San Francisco, California and the "**Vendor**" with legal name and principal place of business as stated in the signature field. Pantheon and Vendor 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 "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).

1.2 "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.

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

1.4 "Business Purpose" means use of Personal Information for Pantheon's or Vendor's operational purposes, 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. Business Purpose may be stated in the agreement entered into by the Parties for Vendor's services ("**Agreement**") or may be listed in **Schedule 1**.

1.5 "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.

1.6 "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.

1.7 "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).

1.8 "Pantheon Data" means information and data, including Personal Data, (i) acquired from or provided by Pantheon; or (ii) otherwise acquired by Vendor in the course of Vendor's performance of the services for Pantheon. Pantheon Data does not include Vendor Data.

1.9 "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.

1.10 "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.

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

1.12 "Restricted Transfers" means either (i) a transfer of Personal Data from Pantheon to Vendor; or (ii) an onward transfer of Personal Data from Vendor to a Sub-Processor, or between two establishments of Vendor or of 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.

1.13 "Services" mean services that Vendor provides to Pantheon in accordance with the Business Purpose.

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

1.15 "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 5,** pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses.

1.16 "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.

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

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

2. Data Processing

2.1 Roles of the Parties. For purposes of this DPA, Pantheon may act as a Controller (or Business) or it may act as a Processor (or Service Provider) of one of its customers. Vendor therefore acknowledges that it may act as a Processor or Service Provider of Pantheon or a Sub-Processor or Sub-Service Provider of Pantheon. 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. Therefore all obligations placed on Processors in this DPA shall apply to Vendor regardless of whether Vendor acts as a Processor or Sub-Processor.

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

2.3 Vendor's Processing of Pantheon Data. Vendor shall Process Pantheon Data in accordance with the requirements of Data Protection Laws and Regulations. Vendor shall treat Pantheon Data confidentially, and shall only Process Pantheon Data on behalf of and in accordance with Pantheon's instructions for the following purposes: (i) Processing in accordance with the Business Purpose; and (ii) Processing to comply with other reasonable instructions provided by Pantheon (e.g., via email) where such instructions are consistent with the Business Purpose.

2.4 Details of the Processing

a.   The subject matter of Processing of Pantheon Data by Vendor 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.

b.   Annually, Vendor will certify to Pantheon that Vendor has Processed Personal Data and Pantheon Data received from Pantheon in accordance with the CCPA, in the form provided in **Schedule 4**.

2.5 Vendor obligations under CCPA. Pantheon discloses Pantheon Data that includes Personal Data to Vendor solely for the Business Purpose. Vendor is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a Commercial Purpose other than providing Services under Business Purpose; and (iii) retaining, using, or disclosing the Personal Data outside of the Business Purpose. Vendor understands the restrictions and prohibitions underlined in this Section 2.5.

3. Rights of Data Subjects. To the extent legally permitted, Vendor shall promptly notify Pantheon if Vendor 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, Vendor shall assist Pantheon by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Pantheon'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. Vendor Personnel

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

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

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

5. Sub-Processing

5.1 Appointment of Sub-Processors. Pantheon acknowledges and agrees that Vendor may engage third-party Sub-Processors only in accordance with this DPA. Further, Vendor must ensure that it has a written data protection agreement about Processing Pantheon Data with each Sub-Processor, which should be no less protective than this DPA 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. Vendor shall make available to Pantheon the current list of Sub-Processors that will process Personal Data for the Business Purpose in the form attached hereto as **Schedule 3**. Vendor shall keep this list updated. Pantheon reserves the right to object to any current Sub-Processors, and Vendor shall promptly replace such current Sub-Processors in consultation with Pantheon.

5.3 Notification of New Sub-Processors. Vendor may engage a new Sub-Processor only upon giving Pantheon 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 Pantheon an opportunity to object to the appointment of the new Sub-Processor. If Vendor fails to inform Pantheon about the appointment of the new Sub-Processor within ninety (90) days, Pantheon reserves the right to terminate the underlying Agreement, if any, and this DPA without prejudice to any fees incurred by Pantheon from the date of appointment of the new Sub-Processor.

5.4 Approving Sub-Processors. Pantheon may object to Vendor's use of a Sub-Processor by notifying Vendor. In the event Pantheon objects to a Sub-Processor, Vendor shall work with Pantheon in good faith to make available a commercially reasonable change in the provision of the Services which avoids the Processing of Personal Data by the objected-to Sub-Processor. If Vendor is unable to find a suitable Sub-Processor, Pantheon may suspend or terminate the underlying Agreement, if any, and this DPA without prejudice to any fees incurred by Pantheon prior to suspension or termination.

5.5 Sub-Processor Compliance. Vendor shall ensure that each Sub-Processor performs the obligations under Sections 2 (Data Processing), 3 (Rights of Data Subjects), 4 (Vendor Personnel), 6 (Security), 7 (Return and Deletion of Pantheon 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 Vendor. Vendor agrees to indemnify, defend, and hold Pantheon 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 applicable data processing agreement/addendum.

6. Security

6.1 Controls for the Protection of Pantheon Data. Taking into account the state of the art, 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, Vendor 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 Pantheon Data); confidentiality; and integrity of Pantheon Data. Vendor shall regularly monitor compliance with these measures. Vendor will not materially decrease the overall security of the Services as long as the Vendor is Processing Personal Data.

6.2 Audits. At Pantheon's written request, Vendor: (a) shall annually conduct regular audits of its security through independent third party auditors, and (b) subject to the confidentiality provisions set forth in this DPA, make available to Pantheon (or Pantheon's independent third-party auditor) information regarding its compliance with the obligations set forth in this Section 6, including results of the security audit, at Vendor's cost.

6.3 Security Incident Management and Notification. Vendor shall have in place an appropriate written security policy with respect to the Processing of Personal Data. Vendor shall notify Pantheon without undue delay, which shall under any circumstances not exceed twenty-four (24) hours of becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Pantheon Data, including Personal Data, transmitted, stored, or otherwise Processed by Vendor, or its Sub-Processors, of which Vendor becomes aware (a "**Security Incident**"). Vendor shall keep Pantheon informed of all material developments in connection with the Security Incident, and cooperate with Pantheon and shall take such reasonable and necessary steps as are directed by Pantheon to assist in the investigation, mitigation and remediation of each Security Incident.

6.4 Notifications. Any notification to Pantheon pursuant to Section 6.3 shall at a minimum contain:

a. 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;

b. the name and contact details of Vendor's data protection officer or another contact point where more information can be obtained;

c. a description of the likely consequences of the Security Incident; and

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

7. Return and Deletion of Pantheon Data

7.1 Vendor's and Sub-Processor's Return and Deletion of Pantheon Data. At the discretion of Pantheon, upon termination of this DPA and/or the Agreement, upon Pantheon's written request, or upon fulfillment of all purposes agreed to in the context of the Services whereby no further Processing is required, Vendor shall either delete, destroy or return all Pantheon Data to Pantheon and securely destroy or return any existing copies. Vendor shall notify its Sub-Processors of the termination of the DPA or cessation of Processing and shall ensure that all such third parties shall either securely destroy Pantheon Data or return the Pantheon Data to Pantheon, at the discretion of Pantheon.

7.2 Vendor's Retention of Personal Data. Vendor may retain certain Personal Data to the extent required by applicable Data Protection Laws and Regulations, provided Vendor shall ensure the confidentiality of all such Personal Data, and provided Vendor shall ensure that such Personal Data is only processed as

necessary for the purpose(s) specified in the Data Protection Laws and Regulations requiring its storage, and for no other purpose.

7.3 Written Certification. Vendor shall provide to Pantheon written certification that Vendor has fully complied with this Section 7 within fifteen (15) calendar days of termination of or fulfillment of the Business Purpose.

8. Data Protection Impact Assessment. Upon Pantheon's request, Vendor shall provide Pantheon with reasonable cooperation and assistance needed to fulfill Pantheon's obligation under the GDPR to carry out a data protection impact assessment related to Pantheon's use of the Services, to the extent that Pantheon does not otherwise have access to relevant information and to the extent such information is available to Vendor. Vendor shall provide reasonable assistance to Pantheon 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. Vendor shall make available to Pantheon all information necessary to demonstrate compliance with Vendor's obligations under Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Pantheon or another auditor mandated by Pantheon.

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. Vendor 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 Vendor 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 Liability and Indemnity. Vendor shall indemnify and hold Pantheon harmless against all claims, actions, third party claims, losses, damages and expenses incurred by Pantheon and arising directly or

indirectly out of or in connection with a breach of this DPA and/or the Applicable Data Law by Vendor or its Sub-Processor (as mentioned in Section 5.5).

11.3 Modifications due to changes in Data Protection Laws. Pantheon may give Vendor at least thirty (30) calendar days' written notice to propose variations to this DPA that Pantheon reasonably considers to be necessary to address the requirements of any Data Protection Laws and Regulations. Upon receiving such notice, Vendor shall promptly discuss the proposed variations with Pantheon. 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. This DPA and the respective rights and obligations arising out of it shall not be assigned or transferred by Vendor, or to or by any third party under any circumstances, including by court order, operation of law, statute, regulation, ordinance, or otherwise, without Pantheon's prior express written consent. Vendor shall notify Pantheon H promptly in writing of any change of ownership of Vendor or of any sale of all or substantially all of Vendor's assets. Vendor acknowledges that any change of ownership, sale of all or substantially all of Vendor's assets, or attempted assignment by Vendor of this Agreement, or any part thereof, without Pantheon's prior written consent is expressly prohibited, shall be null and void from the beginning and may result in immediate termination of this Agreement by Pantheon. Pantheon may assign or otherwise transfer its rights and obligations to successors-in-interest (whether by purchase of stock or assets, merger, operation of law, or otherwise) of that portion of its business related to the subject matter hereof. Subject to the foregoing restrictions on assignment, this Agreement is binding upon, inures to the benefit of, and is enforceable by the Parties and their respective successors and assigns.

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.	VENDOR
"Pantheon"	Vendor Legal Name:
DocuSigned by: *Ronak Ray*	
By: _____ 4CCDEC117F2E4AA...	By:
Name: Ronak Ray	Name:
Title: General Counsel	Title:
Date: 2020-05-12 | 09:40:11 PDT	Date:

SCHEDULE 1

Business Purpose

SCHEDULE 2

Details of the Processing

Nature and Purpose of Processing:
Vendor will Process Personal Data as necessary to perform the Services pursuant to the Agreement and applicable order form(s), or Schedule 1, as applicable, and as further instructed by Pantheon in its use of the Services.

Duration of Processing:
Vendor will Process Pantheon 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 Vendor, who are natural persons.
- Vendors, business partners, vendors and subcontractors of Vendor, who are natural persons.
- Employees or contact persons of Vendor's customers, business partners, vendors 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 BELOW**]

SCHEDULE 3

List of Current Sub-Processors

SCHEDULE 4

Certification Of Compliance With Data Processing Agreement
(CCPA)

The **"Vendor"** with its principal place of business as provided in the signature field below hereby certifies as follows:
1. Vendor and Pantheon Systems, Inc. ("**Pantheon**") executed a Data Processing Agreement ("**DPA**") on the signature date below
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 the Addendum. Service Provider specifically represents and warrants that:
    a. comply with the applicable CCPA provisions, as amended from time to time, in the Processing of Personal Information;
    b. Process Personal Information only on behalf of Pantheon and pursuant to Pantheon's instruction for the specific purpose of performing the Services in the Agreement;
    c. shall not retain, use, or disclose Personal Information for any other purpose other than for the specific purpose of performing the services specific in the Agreement; including for a Business Purpose;
    d. shall not further Collect, Sell, or use Personal Information without Pantheon's prior express written consent, and only as necessary to perform the Business Purpose.
3. Service Provider represents and warrants that it shall immediately notify the Pantheon in writing, if it:
    a. determines or reasonably suspects its inability to comply with its obligation set forth in the Data Processing Agreement;
    b. cannot ensure compliance with the Pantheon's instructions for use of Personal Information.
    c. Upon any such notice to the Pantheon, Service Provider shall immediately cease all use of Personal Information hereunder, and Pantheon is entitled to suspend to terminate the Data Processing Agreement.

 "VENDOR" or "SERVICE PROVIDER"
Vendor Legal Name:
Signature:

Signatory Name:
Address:
Date:

SCHEDULE 5

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. __847-772-5446__ ; fax __N/A__ ; e-mail : __ronak.ray@pantheon.io__
Other information needed to identify the organisation:
(the data **exporter**)

And

Name of the data importing organization:
Address:
Tel. _____; fax_____ ; e-mail :_____
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 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.

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[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 …
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): **Ronak Ray**
[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.
Position: **General Counsel**
Address: **717 California Street, San Francisco, CA 94115**

Signature

Ronak Ray

─4CCDEC117F2E4AA...
(stamp of organisation)

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

On behalf of the data importer: [VENDOR, PLEASE COMPLETE]
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):
Signature

(stamp of organisation)

PANTHEON
The WebOps Platform Built for Agility

SCHEDULE 5

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 (please specify briefly your activities relevant to the transfer):
[description of services].
Limited to the scope, duration and purpose solely as authorized in the underlying written agreement between data exporter and data importer.
Data importer [VENDOR, PLEASE COMPLETE]
The data importer is (please specify briefly activities relevant to the transfer):

"**Vendor**" (with details and signature appear below) is a provider of _____which Processes 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 Vendor, who are natural persons.
- Vendors, business partners, vendors and subcontractors of Vendor, who are natural persons.
- Employees or contact persons of Vendor's customers, business partners, vendors 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)
- Health and medical information
- [**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):

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.

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. Specifically, [please specify as appropriate].

DATA EXPORTER [**PANTHEON PLEASE SIGN**]
Name: **Ronak Ray**
Authorized Signature

DocuSigned by:

Ronak Ray

4CCDEC117F2E4AA...

DATA IMPORTER [**VENDOR PLEASE SIGN**]
Name:
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):

[VENDOR, PLEASE PROVIDE EXAMPLES OF THE PHYSICAL, ADMINISTRATIVE AND TECHNICAL SECURITY CONTROLS THAT ARE IN PLACE HERE.]

DATA EXPORTER [**PANTHEON PLEASE SIGN**]
Name: **Ronak Ray**
Authorized Signature

DocuSigned by:

Ronak Ray

4CCDEC117F2E4AA...

DATA IMPORTER [**VENDOR PLEASE SIGN**]
Name:
Authorized Signature

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Certificate Of Completion

Envelope Id: F56851C3AD9C4B16B07EF915EC94E4CA
Subject: Please DocuSign: Vendor Data Processing Agreement.docx
Source Envelope:

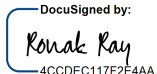|		
Document Pages: 19	Signatures: 4	Envelope Originator:
Certificate Pages: 1	Initials: 0	Celine Josol
AutoNav: Enabled		717 California St.
EnvelopeId Stamping: Enabled		FL 3
Time Zone: (UTC-08:00) Pacific Time (US & Canada)		San Francisco, CA 94108
		celine.josol@pantheon.io
		IP Address: 61.9.108.95

Status: Completed

Record Tracking

Status: Original	Holder: Celine Josol	Location: DocuSign
5/11/2020 7:39:32 PM	celine.josol@pantheon.io	

Signer Events	Signature	Timestamp
Ronak Ray ronak.ray@pantheon.io General Counsel Pantheon Security Level: Email, Account Authentication (None)	DocuSigned by: *Ronak Ray* 4CCDEC117F2E4AA... Signature Adoption: Pre-selected Style Using IP Address: 73.70.99.209	Sent: 5/11/2020 8:30:34 PM Viewed: 5/12/2020 9:39:06 AM Signed: 5/12/2020 9:40:11 AM

Electronic Record and Signature Disclosure:
   Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/11/2020 8:30:35 PM
Certified Delivered	Security Checked	5/12/2020 9:39:07 AM
Signing Complete	Security Checked	5/12/2020 9:40:11 AM
Completed	Security Checked	5/12/2020 9:40:11 AM

Payment Events	Status	Timestamps