

# 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 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 "Customer" with legal name and principal place of business as stated in the signature field. 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 as amended 27 June 2021.

**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. Pantheon 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 Pantheon 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. If retention is legally required, Pantheon continues to adequately protect the confidentiality of all such Personal Data..

**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.** For the transfer of Personal Data from the EEA and Switzerland to the U.S., or any other "third country" as noted in the GDPR, Pantheon adheres to the Standard Contractual Clauses, a form is set forth in Schedule 5 to this DPA, as well as the application of physical, organizational and technological controls, as the transfer mechanism. 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, including when applicable, Addendum I - International Data Transfer Addendum and/ or Addendum II - CPRA Data Processing Addendum, 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.

**11.3 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.

**11.4 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.

**11.5 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** ("**Service Provider**") hereby certifies as follows:

1. Customer and Pantheon Systems, Inc. ("**Pantheon**") executed a Data Processing Agreement ("**DPA**"), signed and dated as indicated 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 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:

**"SERVICE PROVIDER"**

By:

Name:

Date:

**SCHEDULE 4**

EUROPEAN COMMISSION

Brussels, 4.6.2021

C(2021) 3972 final

**ANNEX**

*to the*

**COMMISSION IMPLEMENTING DECISION**

**on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

## ANNEX

### Standard Contractual Clauses

#### SECTION 1

##### *Clause 1*

##### **Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) <sup>[1]</sup> for the transfer of personal data to a third country.

(b) The Parties:

- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")
- have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

##### *Clause 2*

##### **Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider

contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### *Clause 3*

#### **Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

#### **Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### *Clause 5*

#### **Hierarchy**

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

### *Clause 6*

## **Description of the transfer(s)**

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

### *Clause 7 - Optional*

#### **Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### *Clause 8*

#### **Data protection safeguards**

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

##### **8.1 Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

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

##### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as

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

#### 8.4 Accuracy

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

#### 8.5 Duration of processing and erasure or return of data

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

#### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation,

the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular, to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

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

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>[2]</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

#### 8.9 Documentation and compliance

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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

#### *Clause 9*

#### **Use of sub-processors**

- (a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the



engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

### *Clause 10*

#### **Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this

regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### *Clause 11*

#### **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>[4]</sup> at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

### *Clause 12*

#### **Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these

Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### *Clause 13*

#### **Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these

Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

*Clause 14*

**Local laws and practices affecting compliance with the Clauses**

*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>[5]</sup>;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these

Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

### *Clause 15*

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

##### 15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply

with these Clauses.

## 15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### *Clause 16*

#### ***Non-compliance with the Clauses and termination***

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance.

Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

#### **Governing law**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of



\_\_\_\_\_ (*specify Member State*).

[OPTION 2 : These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify Member State*).

*Clause 18*

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of \_\_\_\_\_ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX

### EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

### ANNEX I

#### **A. LIST OF PARTIES**

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

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor): **Controller**

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

Name: **Pantheon Systems, Inc.**

Address: **717 California Street, San Francisco, CA 94108**

Contact person's name, position and contact details: **Kha Nguyen, VP, General Counsel,  
privacy@pantheon.io**

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor): **Processor**

## **B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

*Categories of personal data transferred*

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

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

*Nature of the processing*

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

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

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

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authorities in accordance with Clause 13*

## ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers*

*from a processor to a sub-processor, to the data exporter.*

## ANNEX III – LIST OF SUB-PROCESSORS

### EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: Amazon

Address: 410 Terry Ave. North, Seattle WA 98109-5210

Contact person's name, position and contact details: General Counsel, Amazon, 410 Terry Ave. North, Seattle WA 98109-5210

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Amazon provides DNS and legacy backup storage for Subscriber sites hosted on the Pantheon platform.

2. Name: Fastly

Address: P.O. Box 78266, San Francisco, CA 94107

Contact person's name, position and contact details: General Counsel, Fastly, P.O. Box 78266, San Francisco, CA 94107

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Fastly provides a CDN and edge cache for Subscriber sites hosted on the Pantheon platform.

3. Name: Google Cloud Platform

Address: Google, LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043

Contact person's name, position and contact details: General Counsel, Google, LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): GCP provides database, file hosting and storage of backups.

4. Name: LogzIO

Address: HaArba'a Street, 28 Tel Aviv – Yafo Israel

Contact person's name, position and contact details: General Counsel, LogzIO, HaArba'a Street, 28 Tel Aviv – Yafo Israel

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): LogzIO provides log aggregation and search capability for Subscriber websites.

5. Name: New Relic

Address: 188 Spear Street, San Francisco, CA 94105



Contact person's name, position and contact details: General Counsel, New Relic, 188 Spear Street, San Francisco, CA 94105

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): New Relic provides site performance analytics with regard to Subscriber websites.

6. Name: Pingdom

Address: Jakobsbergsgan 22 11th Floor, 114 44 Stockholm, Sweden

Contact person's name, position and contact details: General Counsel, Pingdom, Jakobsbergsgan 22 11th Floor, 114 44 Stockholm, Sweden

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised):

7. Name: Rackspace

Address: 1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218

Contact person's name, position and contact details: General Counsel, Mail Stop US 109-2301, Rackspace US, Inc., 1 Fanatical Place, City of Windcrest, San Antonio, Texas 78218

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Rackspace provides detection, prevention and resolution of security and technical issues as provided under the applicable Subscriber agreement for Services.

8. Name: Sentry

Address: 132 Hawthorne Street, San Francisco, CA 94107

Contact person's name, position and contact details: General Counsel, Sentry, 132 Hawthorne Street, San Francisco, CA 94107

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Sentry provides services enabling logging of requests for Subscriber to receive technical support.

9. Name: Tesorio

Address: 831 Mitten Road, Burlingame, CA 94010

Contact person's name, position and contact details: General Counsel, Tesorio, 831 Mitten Road, Burlingame, CA 94010

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Tesorio provides a workflow tool for accounts receivable.

10. Name: Cloudflare

Address: 101 Townsend Street, San Francisco, CA 94107

Contact person's name, position and contact details: General Counsel, 101 Townsend Street, San Francisco, CA 94107

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Cloudflare provides a CDN and edge cache for Subscriber sites hosted on the Pantheon platform.

11. Name: Splunk, Inc.

Address: 270 Brannan St., San Francisco, CA 94107

Contact person's name, position and contact details: Elizabeth Davies, Splunk Global Data Protection Officer; [DPO@splunk.com](mailto:DPO@splunk.com)

Description of processing (including a clear delimitation of responsibility in case several sub-processors are authorised): Splunk provides security log collection activities for the Pantheon enterprise services.

## ADDENDUM I - INTERNATIONAL DATA TRANSFER ADDENDUM

*International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (**only** applicable to Customers based in the United Kingdom or collecting data from UK individuals)*

*VERSION B1.0. in force 21 March 2022*

*This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.*

### PART 1 TABLES

Table 1: Parties

Start Date	The Start date for this Addendum shall coincide with the start data of each Agreement between the Parties.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
	The Exporter is the Customer as identified in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	The Importer is PANTHEON
Parties Details	Exporters' details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	Importer's details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Key Contact	Exporters' Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	Importer's Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Signature	The Parties agree that their signatures affixed to the DPA or the EU SCCs in Annex I.A. of Addendum I shall serve to legally bind the Parties to this Addendum.	

Table 2: Selected SCCs. Modules and Selected Clauses

<p>Addendum EU SCCs</p> <p>The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information</p> <p>Date:</p> <p>Reference:</p> <p>Other Identifier (if any):</p> <p>Or</p> <p>the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:</p>						
Module	Module in Operation	Clause 7 Docking Clause	Clause 11 (Option)	Clause 9 a (Prior Authorisation / General Authorisation)	Clause 9 a (Time Period)	Is personal data received from the Importer combined with personal data collected by the Exporter
1	No					
2	Yes	No	No	Yes	10 business days	
3	No					
4	No					

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

--	--

Annex 1A: List of Parties:	Parties are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Annex 1B: Description of Transfer:	Description of Transfer is as set forth in Annex I.B. of the EU SCCs found in Addendum I to the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	TOMs are as set forth in Annex II to the EU SCCs found in Addendum I to the DPA.
Annex III: List of Sub processors (Modules 2 and 3 only):	Sub processors are as set forth in Section III.O. of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes.	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input checked="" type="checkbox"/> Neither Party. Clause 18 will apply in the event the Approved Addendum changes in accordance therewith.</p>
----------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## PART 2: MANDATORY CLAUSES

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the

Approved EU SCCs and any part of the Approved EU SCCs.

## Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Add incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is append as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Ar 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 20 it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, priv and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that



transfer.”;

d. Not applicable. Intentionally left blank;

e. Clause 8.8(i) of Module 2 is replaced with:

“the onward transfer is to a country befitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. Not applicable. Intentionally left blank;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer

before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. Makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and / or

b. Reflects changes to the UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate, and demonstrable increase in:

a. Its direct costs of performing its obligations under the Addendum; and / or

b. Its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum,

but any changes must be made in accordance with its terms.

## Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
-------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# Addendum II - CPRA Data Processing Addendum

This CPRA Data Processing Addendum (“CDPA”) applicable **only** to Customers based in the United States of America, amends, when applicable, the terms and forms part of the Terms of Use or other agreement governing our provision of Services to you (“Services”) (collectively, the “Agreement”) by and between you (the “Customer”) and Pantheon, Inc. (“PANTHEON”). This CDPA shall apply to “Personal Information” of a “Consumer” as those terms are defined under the California Privacy Rights Act of 2020 (“CPRA”) (referred to hereafter as “Customer Data”), that Pantheon processes in the course of providing Customer the Services under the Agreement.

This CDPA shall be effective the date Pantheon receives a complete and executed Agreement, from the Customer (the “Effective Date”)

## **1 Effectiveness**

1.1 This CDPA will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this CDPA.

## **2 Data Processing**

2.1 **Customer’s Role.** The Customer is a Business (as such term is defined under the CPRA), and as such Customer determines the purpose and means of processing Customer Data. Customer will provide Customer Data to Pantheon solely for the purpose of Pantheon performing the Services.

2.2 **Pantheon’s Role.** Pantheon is a Service Provider (as such term is defined under the CPRA), and as such Pantheon shall provide the Services and process any Customer Data in accordance with the Agreement. Pantheon may not retain, use, or disclose Customer Data for any other purpose other than for providing the Services and in performance of the Agreement.

2.3 **Data Processing, Transfers and Sales.** Pantheon will process Customer Data only as necessary to perform the Services, and will not, under any circumstances, collect, combine, share, use, retain, access, share, transfer, or otherwise process Customer Data for any purpose not related to providing such Services. Pantheon will refrain from taking any action that would cause any transfers of Customer Data to or from Pantheon to qualify as “selling personal information” as that term is defined under the CPRA.

2.4 **Sub-Service Providers.** Notwithstanding the restrictions in Section 2.3, Customer agrees that Pantheon may engage other Service Providers (as defined under the CPRA), to assist in providing the Services to Customer (“Sub-Service Providers”). A list of Pantheon’s Sub-Service Providers can be found at <https://pantheon.io/gdpr/sub-processors> provided always that such

engagement shall be subject to a written contract binding each such Sub-Service Provider to terms no less onerous than those contained within this CDPA. Pantheon shall be responsible for all acts or omissions of its Sub-Service Providers as if they were the acts or omissions of Pantheon.

**2.5 Security.** Pantheon will use commercially reasonable security procedures that are reasonably designed to maintain an industry-standard level of security, prevent unauthorized access to and/or disclosure of Customer Data. An outline of Pantheon's minimum security standards can be found at Annex I to this Addendum.

**2.6 Retention.** Pantheon will retain Customer Data only for as long as the Customer deems it necessary for the permitted purpose, or as required by applicable laws. At the termination of this CDPA, or upon Customer's written request, Pantheon will either destroy or return Customer Data to the Customer, unless legal obligations require storage of the Customer Data.

**2.7 Consumer Rights Requests.** Pantheon provides Customer with tools to enable Customer to respond to a Consumer Rights' requests to exercise their rights under the Data Protection Laws. See <https://privacyportal.onetrust.com/webform/fa6fb68e-f740-462d-904a-2646fdf07448/0ddaa1e6-701b-4bbd-9ced-56e8b08aec82> To the extent Customer is unable to respond to Data Subject's request using these tools, Pantheon will provide reasonable assistance to the Customer in responding to the request.

**2.8 Assistance with Consumers' Rights Requests.** If Pantheon, directly or indirectly, receives a request submitted by a Consumer to exercise a right it has under the CPRA in relation to that Consumer's Customer Data, it will provide a copy of the request to the Customer. The Customer will be responsible for handling and communicating with Consumers in relation to such requests.

### **3 Assessments & Third-Party Certifications**

**3.1 Impact Assessment Assistance.** Taking into account the nature of the Processing and the information available, Pantheon will provide assistance to Customer in complying with its obligations under Applicable Law (inclusive) (which address obligations with regard to security, breach notifications, data risk assessments, and prior consultation). Upon request, Pantheon will provide Customer a list of processing operations.

**3.2 Certification/SOC Report.** In addition to the information contained in this CDPA, upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement place, Pantheon will make available the following documents and information regarding the System and Organization Controls (SOC) 2 Report (or the reports or other documentation describing the controls implemented by Pantheon that replace or are substantially equivalent to the SOC 2), so that Customer can reasonably verify Pantheon's compliance with its obligations under this CDPA.

3.3 If Customer has reasonable cause to suspect that Pantheon is not providing the platform in a manner consistent with CPRA and allowing unauthorized use of personal information, Customer may (i) submit an inquiry to [privacy@employinc.com](mailto:privacy@employinc.com), (ii) cease use of their license until they are able to confirm Pantheon's compliance, or (iii) with evidence of non-compliance of CPRA terminate the Agreement between the parties. Pantheon will provide notice if it believes it can no longer meet its obligations under this CDPA.

#### **4 Enforceability**

4.1 Any provision of this CDPA that is prohibited or unenforceable shall be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall then incorporate such substitute provision into this CDPA.

#### **5 Liability**

5.1 To the extent permitted by applicable laws, liability arising from claims under this CDPA will be subject to the terms of the Agreement.

## ANNEX I - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

*Pantheon provides technical and organizational measures in compliance with certification to SOC 2, Type II requirements, including:*

#### 1. **Physical access control**

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- Pantheon employees do not have physical access to the processing environment.
- Pantheon reviews its sub-processors to ensure they have adequate physical security controls for the processing environment, including:
  - Badge access to the physical data center
  - Video surveillance for the physical data center
  - Visitor procedures for the physical data center

#### 2. **Authorization control**

- Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage. Pantheon logs all user activity in the processing environment.
- Pantheon restricts access to the processing environment to those personnel with a business need.
- Pantheon requires each personnel with access to the processing to have unique usernames specific to each personnel.
- Pantheon reviews personnel access rights on a quarterly basis

### **3. Logical access control**

Measures suitable for preventing data processing systems from being used by unauthorized persons.

- Pantheon requires authentication for access to the processing environment.
- Pantheon requires username and complex password plus an additional second factor to authenticate to its systems.
- Pantheon requires secure protocols (https and SSH) for access to the processing environment.

### **4. Confidentiality control**

- The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures. Pantheon encrypts data at rest and in transit.
- Pantheon publishes an Information Classification and Handling Policy to all employees with requirements for the treatment of data at various classifications, including requirements for encryption usage.
- Pantheon provides Security Awareness Training to all employees upon hire and annually thereafter.

### **5. Input control**

- Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application). Pantheon logs all user activity in the processing environment.
- Pantheon provides customers the capability to log activities by their personnel associated with their sites.
- Pantheon performs penetration testing of the processing environment on an annual basis.

### **6. Availability control**

- Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.). Pantheon performs regular backups of its



systems.

- Pantheon provides customers with the capability to backup and restore their sites.
- Pantheon reviews its sub-processors to ensure they have adequate physical security controls for the processing environment, including:
  - Fire suppression systems in the physical data center
  - Video surveillance for the physical data center
  - Environmental controls for the physical data center
- Pantheon has a documented Business Continuity Plan that is exercised on an annual basis

## **7. Separation control**

- Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data. Pantheon ensure the separation of its corporate, development, and production environments.
- Pantheon logically separates each customer's data from that of other customers

## **8. Resilience control**

- Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident. Pantheon has a documented incident response processes that are tested at least annually.
- Pantheon has a documented Disaster Recovery Plan to ensure the recovery of systems in accordance with agreed upon RTO and RPO requirements.
- Pantheon performs regular backups of its systems.
- Pantheon provides customers with the capability to backup and restore their sites.

## **9. Integrity control**

- Measures capable of ensuring that personal data remains intact, complete, and current. Pantheon performs regular backups of its systems.
- Pantheon provides customers with the capability to backup and restore their sites.
- Pantheon performs penetration testing of the processing environment on an annual basis.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

- Pantheon has Data Processing Agreements with its processors and sub-processors to ensure that Pantheon can provide assistance to the Controller.
- Pantheon reviews all of its Processors before usage.
- Pantheon has processes in place to ensure that the Controller is aware of any changes to its processors used to provide the services.