



**DATA PROCESSING EXHIBIT**

This Data Processing Exhibit (“DPE”) is an exhibit to the Master Subscription Agreement or the Professional Services Agreement (as the case may be, the “Agreement”), and sets forth the obligations of the parties with regard to the Processing of Personal Data pursuant to such Agreement.

**Designated Data Center Location:** European Economic Area

**1. Definitions**

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Master Subscription Agreement and/or exhibits thereto.

“**Additional Products**” means products, services and applications (whether made available by Workday or a third party) that are not part of the Service.

“**Customer Audit Program**” means Workday’s optional, fee-based customer audit program as described in the Order Form for Audit Program.

“**Customer Data**” has the meaning given in the Master Subscription Agreement.

“**Data Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Data Processor**” means the entity which Processes Personal Data on behalf of the Data Controller.

“**EU Data Protection Laws**” means: (i) up to 25 May 2018, the Data Protection Directive 95/46/EC; and (ii) from 25 May 2018 onwards, the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”).

“**Data Protection Laws**” means all data protection laws applicable to the Processing of Personal Data under this DPE, including local, state, national and/or foreign laws, treaties, and/or regulations, EU Data Protection Laws, and implementations of EU Data Protection Laws into national law.

“**Data Subject**” means the person to whom the Personal Data relates.

“**EEA**” means the European Economic Area.

“**Master Subscription Agreement**” means any agreement between the parties for the provision of the Service.

“**Personal Data**” means any Customer Data that relates to (i) an identified or identifiable natural person or, (ii) an identified or identifiable legal entity, where such information is protected similarly as personal data under applicable Data Protection Laws.

“**Personal Data Breach**” means (i) a ‘personal data breach’ as defined in the GDPR affecting Personal Data, and (ii) any Security Breach affecting Personal Data.

“**Processing or Process**” means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

“**Service**” means Workday’s software-as-a-service applications provided under the Master Subscription Agreement.

“**Standard Contractual Clauses**” means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Commission Decision (2010/87/EU), as set out in Addendum A to this DPE.

“**Subprocessor**” means a Workday Affiliate or third-party entity engaged by Workday or a Workday Affiliate as a Data Processor under this DPE.

“**Valid Transfer Mechanism**” means a data transfer mechanism permitted by EU Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside the EEA.



## DATA PROCESSING EXHIBIT

### 2. Processing Personal Data

**2.1 Scope and Role of the Parties.** This DPE applies to the Processing of Personal Data by Workday in the course of providing the Service. For the purposes of this DPE, Customer and its Affiliates are the Data Controller(s) and Workday is the Data Processor.

**2.2 Instructions for Processing.** Workday shall Process Personal Data in accordance with Customer's documented instructions. Customer instructs Workday to Process Personal Data to provide the Service in accordance with the Agreement (including this DPE). Customer may provide additional instructions to Workday to Process Personal Data, however Workday shall be obligated to perform such additional instructions only if they are consistent with the terms and scope of the Agreement and this DPE.

**2.3 Compliance with Laws.** Workday shall comply with all Data Protection Laws applicable to Workday in its role as a Data Processor Processing Personal Data. For the avoidance of doubt, Workday is not responsible for complying with Data Protection Laws applicable to Customer or Customer's industry such as those not generally applicable to online service providers. Customer shall comply with all Data Protection Laws applicable to Customer as a Data Controller.

### 3. Subprocessors

**3.1 Use of Subprocessors.** Customer agrees that Workday and Workday Affiliates may engage Subprocessors. Workday or the relevant Workday Affiliate shall ensure that such Subprocessor has entered into a written agreement that is no less protective than this DPE. Workday shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts or omissions were performed by Workday.

**3.2 Notification of New Subprocessors.** Workday shall make available to Customer through Workday's customer website (currently located at <https://community.workday.com>) a list of Subprocessors authorized to Process Personal Data ("Subprocessor List") and provide Customer with a mechanism to obtain notice of any updates to the Subprocessor List. At least thirty (30) days prior to authorizing any new Subprocessor to Process Personal Data, Workday shall provide notice to Customer by updating the Subprocessor List.

**3.3 Subprocessor Objection Right.** This Section 3.3 shall apply only where and to the extent that Customer is established within the EEA or Switzerland or where otherwise required by Data Protection Laws applicable to Customer. In such event, if Customer objects on reasonable grounds relating to data protection to Workday's use of a new Subprocessor then Customer shall promptly, and within fourteen (14) days following Workday's notification pursuant to Section 3.2 above, provide written notice of such objection to Workday. Should Workday choose to retain the objected-to Subprocessor, Workday will notify the Customer at least fourteen (14) days before authorizing the Subprocessor to Process Personal Data and the Customer may immediately discontinue using the relevant portion(s) of the Service and may terminate the relevant portion(s) of the Service within thirty (30) days. Upon any termination by Customer pursuant to this Section, Workday shall refund Customer any prepaid fees for the terminated portion(s) of the Service that were to be provided after the effective date of termination.

### 4. Data Center Location and Data Transfers

**4.1 Storage of Personal Data.** Personal Data will be housed in data centers located in the Designated Data Center Location set forth herein unless the parties otherwise expressly agree in writing.

**4.2 Access to Personal Data.** Notwithstanding Section 4.1, in order to provide the Service Workday and its Subprocessors will only access Personal Data from (i) countries in the EEA, (ii) countries or territories formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries") and (iii) the United States provided, in this case, that Workday makes available to Customer a Valid Transfer Mechanism. When Workday or its Subprocessors access Personal Data from outside the Designated Data Center Location for the purposes set forth above, Customer agrees that Personal Data may be temporarily stored in that country.

**4.3 Privacy Shield.** Workday, Inc. is self-certified under the EU-U.S. and the Swiss-U.S. Privacy Shield Frameworks maintained by the U.S. Department of Commerce ("Privacy Shield") and complies with their requirements for handling, collecting and transferring Personal Data from the EEA and Switzerland to the United States in connection with the Service. Workday will remain certified for the term of the Agreement provided that the Privacy Shield is recognized as a Valid Transfer Mechanism.



**DATA PROCESSING EXHIBIT**

**4.4 Standard Contractual Clauses.** Customer may choose to transfer EEA/Swiss Personal Data to Workday, Inc. in reliance on the Standard Contractual Clauses. Where Customer elects to rely on the Standard Contractual Clauses, all transfers of Personal Data out of the EEA and Switzerland shall be governed by the Standard Contractual Clauses which shall apply between Customer and the Customer Affiliates established within the EEA and Switzerland (each as “data exporter”) and Workday, Inc. (as “data importer”), subject to the requirements of Section 14.

**5. Rights of Data Subjects**

**5.1 Correction, Deletion or Restriction.** Workday will, at its election and as necessary to enable Customer to meet its obligations under applicable Data Protection Laws, either (i) provide Customer the ability within the Service to correct or delete Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Customer’s behalf if such functionality is not available within the Service.

**5.2 Access to Personal Data.** To the extent a Data Subject’s Personal Data is not accessible to Customer through the Service, Workday will, as necessary to enable Customer to meet its obligations under applicable Data Protection Laws, provide reasonable assistance to make such Personal Data available to Customer.

**5.3 Handling of Data Subject Requests.** For the avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, deletion or restriction of that person’s Personal Data (“**Data Subject Request**”). If Workday receives a Data Subject Request, Workday will promptly redirect the Data Subject to submit its request to Customer.

**5.4 Data Portability.** During the term of the Agreement, Customer may extract Personal Data from the Service in accordance with the Documentation and the relevant provisions of the Agreement, including so that Customer can provide the Personal Data to an individual who makes a data portability request under EU Data Protection Laws.

**6. Government Access Requests**

Unless prohibited by applicable law or a legally-binding request of law enforcement, Workday shall promptly notify Customer of any request by government agency or law enforcement authority for access to or seizure of Personal Data.

**7. Workday Personnel**

Workday shall take reasonable steps to require screening of its personnel who may have access to Personal Data, and shall require such personnel (i) to Process Personal Data in accordance with Customer’s instructions as set forth in this DPE, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which shall survive the termination of employment.

**8. Personal Data Breach**

In the event Workday becomes aware of a Personal Data Breach it shall without undue delay notify Customer in accordance with the Security Breach provisions of the Agreement. To the extent Customer requires additional information from Workday to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, Workday shall provide reasonable assistance to provide such information to Customer taking into account the nature of Processing and the information available to Workday.

**9. Security Program**

Workday shall implement appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as set forth in the Security Exhibit.

**10. Audit**

Customer agrees that Workday’s then-current SOC 1 and SOC 2 audit reports (or comparable industry-standard successor reports) and/or Workday’s ISO 27001 and ISO 27018 Certifications will be used to satisfy any audit or inspection requests by or on behalf of Customer, and Workday shall make such reports available to Customer. In the event that Customer, a regulator, or supervisory authority requires additional information, including information necessary to demonstrate



**DATA PROCESSING EXHIBIT**

compliance with this DPE, or an audit related to the Service, such information and/or audit shall be made available in accordance with Workday's Customer Audit Program.

**11. Return and Deletion of Personal Data**

Upon termination of the Service, Workday shall return and delete Personal Data in accordance with the relevant provisions of the Agreement.

**12. Additional Products**

Customer acknowledges that if it installs, uses, or enables Additional Products that interoperate with the Service but are not part of the Service itself, then by such actions Customer is instructing Workday to cause the Service to allow such Additional Products to access Personal Data as required for the interoperation of those Additional Products with the Service. Such separate Additional Products are not required to use the Service and may be restricted for use as determined by Customer's system administrator. This DPE does not apply to the Processing of Personal Data by Additional Products which are not part of the Service.

**13. Additional European Terms**

**13.1 Subject-Matter, Nature, Purpose and Duration of Data Processing.** Workday will Process Personal Data to provide the Service (operation and maintenance of a software-as-a-service application). The duration of Processing Personal Data shall be for the term of the Agreement.

**13.2 Types of Personal Data and Categories of Data Subjects.** The types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to the Standard Contractual Clauses, which is hereby incorporated into this DPE by this reference and shall be binding as if it was set forth in this DPE in its entirety.

**13.3 Data Protection Impact Assessments and Prior Consultations.** Customer agrees that Workday's then-current SOC 1 and SOC 2 audit reports (or comparable industry-standard successor reports) and/or Workday's ISO 27001 and ISO 27018 Certifications will be used to carry out Customer's data protection impact assessments and prior consultations, and Workday shall make such reports available to Customer. To the extent Customer requires additional assistance to meet its obligations under Article 35 and 36 of the GDPR to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Service, Workday will, taking into account the nature of Processing and the information available to Workday, provide reasonable assistance to Customer through the Customer Audit Program.

**14. Clarifications to the Standard Contractual Clauses**

If Customer executes the Standard Contractual Clauses with Workday, Inc., the terms in this Section will apply.

**14.1 Audits.** For the purposes of Clause 5 (f) of the Standard Contractual Clauses, Data Importer agrees to make its then-current SOC 1 and SOC 2 audit report (or comparable industry-standard successor report) and/or ISO 27001 and ISO 27018 Certificate available to Data Exporter to satisfy any audit or inspection requests by or on behalf of Data Exporter. In the event that Data Exporter, a regulator, or supervisory authority requires additional information or an audit related to the Service, such information and/or audit shall be made available in accordance with Workday's Customer Audit Program.

**14.2 Subprocessors.** For the purposes of Clause 11 of the Standard Contractual Clauses, Customer consents to Workday appointing Subprocessors in accordance with Section 3 of this DPE.

**14.3 Return and Deletion of Personal Data.** For purposes of Clause 12 (1) of the Standard Contractual Clauses, Workday shall return and delete Data Exporter's data in accordance with the relevant provisions of the Agreement.

**14.4 Conflict.** For the avoidance of doubt, the parties agree that the terms of this Section are not intended to amend or modify the Standard Contractual Clauses. These provisions provide clarity in terms of Workday's business processes for complying with the Standard Contractual Clauses. In the event of any conflict between the terms of this DPE and the provisions of the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.



**DATA PROCESSING EXHIBIT**

**15. Professional Services**

Notwithstanding any provision to the contrary in this DPE, this Section 15 shall control with respect to Professional Services. For purposes of interpreting the DPE terms for the Professional Services, “Agreement” means Professional Services Agreement, and “Service” means Professional Services.

**15.1 Definitions**

The following definitions apply to Professional Services.

**“Professional Services Agreement”** means any agreement between the parties for the provision of consulting or professional services, including but not limited to the following agreements or terms: the Foundation Tenant Service Terms, the Professional Services Agreement, the Delivery Assurance terms, the Professional Services Addendum, and/or the Consulting and Training Addendum and Amendment.

**“Professional Services”** means the professional or consulting services provided to Customer under a Professional Services Agreement.

**“Professional Services Data”** means electronic data or information that is provided to Workday under a Professional Services Agreement for the purpose of being input into the Workday Service, or Customer Data accessed within or extracted from the Customer’s tenant to perform the Professional Services.

**“Personal Data”** means any Professional Services Data that is related to an identified or identifiable person.

**“SOW”** means any separate statement of work or other document under which Workday agrees to provide Professional Services, that has been fully executed by the parties and is subject to a Professional Services Agreement.

**“SFTP Server”** means a secure file transfer protocol server or its successor provided and controlled by Workday that may be used to transfer the Professional Services Data between Customer and Workday for implementation purposes.

**15.2 Notification of New Subprocessors.**

*This Section supersedes Section 3.2 “Notification of New Subprocessors” regarding Professional Services. For the avoidance of doubt, Section 3.2 continues to apply to Workday’s use of its Affiliates on the Subprocessor List as Subprocessors for Professional Services:*

**Notification of New Subprocessors.** Workday shall make available to Customer on Workday Community (<https://community.workday.com>) a list of additional Subprocessors authorized to Process Personal Data (“**Professional Services Subprocessor List**”) and provide Customer with a mechanism to obtain notice of any updates to the Professional Services Subprocessor List. At least thirty (30) days prior to authorizing any new Subprocessor to Process Personal Data, Workday shall provide notice to Customer by updating the Professional Services Subprocessor List.

**15.3 Subprocessor Objection Right.**

*This Section supersedes Section 3.3 “Subprocessor Objection Right” regarding Professional Services. For the avoidance of doubt, Section 3.3 continues to apply to Workday’s use of its Affiliates on the Subprocessor List as Subprocessors for Professional Services:*

**Subprocessor Objection Right.** This Section 15.3 shall apply only where and to the extent that Customer is established within the EEA or Switzerland or where otherwise required by Data Protection Laws applicable to Customer. Provided the Customer has reasonable grounds relating to data protection, Customer may object to Workday’s use of a third-party Subprocessor in two ways: (i) Prior to executing an SOW, Customer may review the then-published Professional Services Subprocessor List and note any objections in the applicable SOW; or (ii) For a new Subprocessor added to the Professional Services Subprocessor List, within fourteen (14) days following Workday’s notification pursuant to Section 15.2 above, Customer may object by providing written notice of such objection to Workday pursuant to the Agreement.

**15.4 SFTP Server Location.**

*This Section supersedes Section 4.1 “Storage of Personal Data” regarding Professional Services:*





**DATA PROCESSING EXHIBIT**

**SFTP Server Location.** The SFTP Server will be housed in data centers located in the Designated Data Center Location unless the parties otherwise expressly agree in writing.

**15.5 Processing Professional Services Data.**

*This Section supersedes Section 4.2 “Access to Personal Data” regarding Professional Services:*

**Processing Professional Services Data.** To provide the Professional Services, Workday and its Subprocessors will only Process Personal Data in (i) countries in the EEA, (ii) countries formally recognized by the European Commission as providing an adequate level of data protection (“**Adequate Countries**”), and provided Workday makes available to Customer a Valid Transfer Mechanism, (iii) the United States, (iv) other countries where Customer and/or its Affiliates are located and (v) other countries as agreed by the parties in writing.

**15.6 Correction, Deletion or Restriction.**

*This Section Supersedes Section 5.1 “Correction, Deletion or Restriction” regarding Professional Services:*

**Correction, Deletion or Restriction.** Workday will, at its election and as necessary to enable Customer to meet its obligations under applicable Data Protection Laws, either (i) provide Customer the ability on the SFTP Server to correct or delete Personal Data or restrict its Processing; or (ii) make such corrections, deletions, or restrictions on Customer’s behalf if such functionality is not available on the SFTP Server.

**15.7 Access to Personal Data**

*This Section supersedes Section 5.2 “Access to Personal Data” regarding Professional Services:*

**Access to Personal Data.** To the extent a Data Subject’s Personal Data is not accessible to Customer through the SFTP Server, Workday will, as necessary to enable Customer to meet its obligations under applicable Data Protection Laws, provide reasonable assistance to make such Personal Data available to Customer.

**15.8 Data Portability**

*Section 5.4 “Data Portability” shall not apply to Professional Services.*

**15.9 Audit**

*This Section supersedes Section 10 “Audit” regarding Professional Services:*

**Audit.** In the event that Customer, a regulator, or data protection authority requires an inspection or audit relating to the Professional Services that Customer cannot obtain through its own access to the SFTP Server or Professional Services Data, such inspection and/or audit shall be made available in accordance with Workday’s Customer Audit Program.

**15.10 Deletion of Professional Services Data**

*This Section supersedes Section 11 “Return and Deletion of Personal Data” regarding Professional Services:*

**Deletion of Professional Services Data.** Subject to the Customer’s prior written request, Workday will delete the Professional Services Data by deletion of Customer’s files on the SFTP Server; provided, however, that Workday will not be required to remove copies of the Professional Services Data from its backup media and servers until such time as the backup copies are scheduled to be deleted, provided further that in all cases Workday will continue to protect the Professional Services Data in accordance with this DPE.

**15.11 Data Protection Impact Assessments and Prior Consultations**

*This Section supersedes Section 13.3 “Data Protection Impact Assessments and Prior Consultations” regarding Professional Services:*

**Data Protection Impact Assessments and Prior Consultations.** In the event that Customer requires additional assistance to meet its obligations under Article 35 and 36 of the GDPR to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer’s use of the Professional Services that Customer cannot obtain through its own access to the SFTP Server or Professional Services Data, Workday will, taking into account



**DATA PROCESSING EXHIBIT**

the nature of Processing and the information available to Workday, provide reasonable assistance to Customer through the Customer Audit Program.

**16. General Provisions**

**16.1 Customer Affiliates.** Customer is responsible for coordinating all communication with Workday on behalf of its Affiliates with regard to this DPE. Customer represents that it is authorized to issue instructions as well as make and receive any communications or notifications in relation to this DPE on behalf of its Affiliates. If required for a Customer Affiliate established within the EEA and/or Switzerland to comply with applicable Data Protection Laws, the Affiliate, subject to the terms of Section 14, may sign the Standard Contractual Clauses as a data exporter by way of an amendment to the Master Subscription Agreement.

**16.2 Disclosure of DPE Terms.** Customer or its Affiliates may only disclose the terms of this DPE to a regulator or supervisory authority to the extent required by law or such regulator or supervisory authority, such as for the purpose of notifications or approvals. Furthermore, Customer shall take reasonable endeavors to ensure that such regulator or supervisory authority do not make this DPE public, including: (i) marking copies of this DPE as “Confidential and Commercially Sensitive”; (ii) requesting return of this DPE once the regulatory notification has been completed or approval granted; and (iii) requesting prior notice and consultation before any disclosure of this DPE by the regulator or supervisory authority.

**16.3 Termination.** The term of this DPE will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Personal Data is deleted from Workday’s systems.

**16.4 Conflict.** This DPE is subject to the non-conflicting terms of the Agreement. With regard to the subject matter of this DPE, in the event of inconsistencies between the provisions of this DPE and the Agreement, the provisions of this DPE shall prevail with regard to the parties’ data protection obligations.

**16.5 Customer Affiliate Enforcement.** Customer’s Affiliates may enforce the terms of this DPE directly against Workday, subject to the following provisions:

- i. the Customer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an “**Affiliate Claim**”) directly against Workday on behalf of such Affiliate, except where the Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim; and
- ii. for the purpose of any Affiliate Claim brought directly against Workday by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

**16.6 Remedies.** Customer’s remedies (including those of its Affiliates) with respect to any breach by Workday or its Affiliates of the terms of this DPE (including the Standard Contractual Clauses), and the overall aggregate liability of Workday and its Affiliates arising out of, or in connection with the Agreement (including this DPE) will be subject to any aggregate limitation of liability that has been agreed between the parties under the Agreement (the “**Liability Cap**”). For the avoidance of doubt, the parties intend and agree that the overall aggregate liability of Workday and its Affiliates arising out of, or in connection with the Agreement (including this DPE) shall in no event exceed the Liability Cap.

**16.7 Miscellaneous.** The section headings contained in this DPE are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPE.



**DATA PROCESSING EXHIBIT**

**ADDENDUM A**

This Addendum A is part of and subject to the terms of the DPE.

**Standard Contractual Clauses (processors)**

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

Name of the data exporting organisation:

Address:

Telephone:

Fax:

Email:

Other information needed to identify the organisation:

For itself and/or on behalf of any Customer Affiliates established in the EEA or Switzerland  
(each a 'data exporter')

And

Name of the data importing organisation: Workday, Inc.

Address: 6110 Stoneridge Mall Road, Pleasanton, CA 94588, USA

Telephone: 925.951.9225

Email: privacy@workday.com

Other information needed to identify the organisation: n/a

(the 'data importer')

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

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

*Clause 1*  
**Definitions**

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who



**DATA PROCESSING EXHIBIT**

is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2****Details of the transfer***

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

*Clause 3****Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4****Obligations of the data exporter***

The data exporter agrees and warrants:

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

**DATA PROCESSING EXHIBIT**

- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5****Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

**DATA PROCESSING EXHIBIT**

- (ii) any accidental or unauthorised access, and
- (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6****Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

*Clause 7****Mediation and jurisdiction***

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

**DATA PROCESSING EXHIBIT**

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8****Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9****Governing Law***

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

*Clause 10****Variation of the contract***

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

*Clause 11****Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.



**DATA PROCESSING EXHIBIT**

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

*Clause 12*

***Obligation after the termination of personal data processing services***

- 1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- 2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Printed Name: \_\_\_\_\_

Position: \_\_\_\_\_

Address: See cover page above.

Signature: \_\_\_\_\_

**On behalf of the data importer (Workday, Inc.):**

Printed Name: \_\_\_\_\_

Position: \_\_\_\_\_

Address: See cover page above.

Signature: \_\_\_\_\_

**DATA PROCESSING EXHIBIT****APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

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

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

**Data exporter**

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

A customer of Workday's enterprise software-as-a-service applications.

**Data importer**

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

Workday, Inc. is a provider of enterprise software-as-a-service applications. The data importer processes Personal Data on behalf of and according to the instructions of data exporter.

**Data subjects**

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

Prospective, current and former employees and other workers, as well as related persons.

**Categories of data**

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

- **Prospective, current and former employee data:** Such employee data as is necessary for human resources and benefits processing, including name; contact information (including home and work address; home and work telephone numbers; mobile telephone numbers; web address data; instant messenger data; home and work email address); marital status; ethnicity; citizenship information; visa information; national and governmental identification information; drivers' license information; passport information; banking details; military service information; religion information; birth date and birth place; gender; disability information; employee identification information; education, language(s) and special competencies; certification information; probation period and employment duration information; job or position title; business title; job type or code; business site; company, supervisory, cost center and region affiliation; work schedule and status (full-time or part-time, regular or temporary); compensation and related information (including pay type and information regarding raises and salary adjustments); payroll information; allowance, bonus, commission and stock plan information; leave of absence information; employment history; work experience information; information on internal project appointments; accomplishment information; training and development information; award information; membership information.
- **Related person's data:** Name and contact information of dependents or beneficiaries (including home address; home and work telephone numbers; mobile telephone numbers); date of birth; gender; emergency contacts; beneficiary information; dependent information).

**Special categories of data (if appropriate)**

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

Ethnicity; religious beliefs; disability information; trade union membership information.

**Processing operations**

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

Basic processing activities involve storing Personal Data and processing necessary to operate and maintain the enterprise software-as-a-service applications and implement data exporter's instructions when using the software-as-a-service applications (e.g. storage, use, retrieval or erasure of Personal Data).





**DATA PROCESSING EXHIBIT**

**DATA EXPORTER**

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

**DATA IMPORTER (Workday, Inc.)**

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_



**DATA PROCESSING EXHIBIT**

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

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

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

Data importer shall implement appropriate technical and organisational measures, designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data as set forth in Section 9.

The technical and organisational measures, internal controls, and information security routines set forth in the Security Exhibit are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

**DATA EXPORTER**

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

**DATA IMPORTER (Workday, Inc.)**

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_