

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 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.

“**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, the GDPR, and implementations of the GDPR into national law.

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

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

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679.

“**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.

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

“**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 the GDPR as a lawful basis for transferring Personal Data to a recipient outside the EEA.

2. Processing Personal Data

2.1 Scope and Role of the Parties. This DPE applies to the Processing of Personal Data by Workday to provide 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 a list of Subprocessors (currently located at: <https://community.workday.com>) 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.

DATA PROCESSING EXHIBIT

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.

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 the GDPR.

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 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 Addendum 1 hereto.

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. Professional Services. Notwithstanding any provision to the contrary in this DPE, this Section 14 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.

14.1 Definitions. The following definitions apply to Professional Services.

DATA PROCESSING EXHIBIT

“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.

14.2 Notification of New Subprocessors.

This Section supersedes Section 3.2 “Notification of New Subprocessors” regarding Professional Services, except that 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.

14.3 Subprocessor Objection Right.

This Section supersedes Section 3.3 “Subprocessor Objection Right” regarding Professional Services, except that Section 3.3 continues to apply to any objection by Customer of Workday’s use of its Affiliates on the Subprocessor List as Subprocessors for Professional Services:

Subprocessor Objection Right. This Section 14.3 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 14.2 above, Customer may object by providing written notice of such objection to Workday pursuant to the Agreement.

14.4 SFTP Server Location.

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

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.

14.5 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, and (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, and (iv) other countries where Customer and/or its Affiliates are located, and (v) other countries as agreed by the parties in writing.

14.6 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.

14.7 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.

14.8 Data Portability

This Section supersedes Section 5.4 “Data Portability” regarding Professional Services:

Data Portability. Customer may extract Personal Data from the SFTP Server in accordance with the Documentation.

14.9 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.

DATA PROCESSING EXHIBIT

14.10 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.

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

15. General Provisions

15.1 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.

15.2 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.

15.3 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.

15.4 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.

15.5 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 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.

15.6 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, 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.

15.7 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 1

Data subjects

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

Categories of data

- **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).