



## **Universal Data Processing Exhibit**

This Universal Data Processing Exhibit is an exhibit to the Agreement between Workday and Customer and sets forth the obligations and rights of the parties regarding the Processing of Personal Data pursuant to such Agreement.

### **1. Definitions.**

Unless otherwise defined below, all capitalized terms have the meaning given within the applicable Agreement and/or exhibits thereto.

**"Agreement"** means the UMSA, the Professional Services Agreement, and Order Forms, including any exhibits or attachments applicable to the Covered Service.

**"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., its implementing regulations, and amendments, including the California Privacy Rights Act ("**CPRA**") and its implementing regulations.

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

**"Covered Data"** means (i) Customer Content (as defined in the UMSA), and (ii) Professional Services Data.

**"Covered Service"** means (i) any Service provided under the UMSA, and/or (ii) any Professional Services.

**"DPE"** means this Universal Data Processing Exhibit including any appendices, or documents incorporated by reference.

**"Data Protection Laws"** means all data protection or privacy laws and regulations applicable to the Processing of Personal Data.

**"Data Subject"** means the person to whom the Personal Data relates.

**"Europe"** or **"European"** means the European Economic Area ("**EEA**"), the United Kingdom ("**UK**"), and Switzerland.

**"GDPR"** means either or both the (i) General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"), and (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") as the context may require.

**"Personal Data"** means any Covered Data that (i) relates to an identified or identifiable natural person, or (ii) is defined as "personal data" or "personal information" (or any substantively analogous term) by applicable Data Protection Laws.

**"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, 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.

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

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



**“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 Professional Services Agreement, the Delivery Assurance terms, the Professional Services Addendum, and/or the Consulting and Training Addendum and Amendment.

**“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 a Service, or any other Covered Data accessed within or extracted from a Service to perform the Professional Services.

**“Restricted Transfer”** means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a recipient in a country outside of the EEA which is not subject to a valid adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a recipient in a country outside the UK which is not based on adequacy regulations pursuant to section 17A of the UK Data Protection Act 2018 (“UK DPA”); and (iii) where the Swiss Federal Act on Data Protection of September 25, 2020 (“Swiss FADP”) applies, a transfer of Personal Data from Switzerland to recipient in a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Council.

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

**“Subprocessor List”** means the subprocessor list identifying the Subprocessors that are authorized to Process Personal Data, accessible through Workday’s website (currently located at <https://www.workday.com/en-us/legal/subprocessors.html>).

## **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 Covered Service. For the purposes of this DPE, Customer is a Controller or a Processor and Workday is a 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 Covered Service in accordance with the Agreement (including this DPE) and as further specified via Customer’s use of the Covered Service. Workday will comply with additional written instructions issued by Customer if they are consistent with the terms and scope of the Agreement.

**2.3 Compliance with Laws.** Each party will comply with its obligations related to the Processing of Personal Data under applicable Data Protection Laws. Customer shall ensure that any instruction it issues to Workday complies with applicable Data Protection Laws. Workday shall inform Customer without undue delay if, in its reasonable opinion, an instruction issued by Customer violates applicable European Data Protection Laws.

**2.4 Description of Processing.** The agreed subject-matter, the nature, purpose and duration of data processing, the types of Personal Data and categories of Data Subjects are set forth in Addendum B to this DPE.

## **3. Subprocessors.**

**3.1 Use of Subprocessors.** Customer agrees that Workday and Workday Affiliates may engage Subprocessors. Workday or the relevant Workday Affiliate engaging a Subprocessor 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 a 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.** Customer may object to Workday's use of a new Subprocessor on reasonable grounds relating to data protection by providing written notice to Workday within fourteen (14) days following Workday's notification pursuant to Section 3.2 above. Should Workday choose to retain the objected-to Subprocessor, Workday will notify Customer and Customer may terminate the relevant portion(s) of the Covered 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 Covered Service that were to be provided after the effective date of termination.

#### **4. Data Subject Rights.**

**4.1 Assistance with Data Subject Requests.** Workday will, in a manner consistent with the functionality of the Covered Service and Workday's role as a Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under applicable Data Protection Laws ("**Data Subject Requests**").

**4.2 Handling of Data Subject Requests.** For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests. If Workday receives a Data Subject Request or other complaint from a Data Subject regarding the Processing of Personal Data, Workday will promptly forward such request or complaint to Customer, provided the Data Subject has given sufficient information for Workday to identify Customer.

#### **5. Workday Personnel.**

Workday shall 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 survive their termination of employment.

#### **6. Personal Data Breach.**

If Workday becomes aware of a Personal Data Breach, it shall without undue delay notify Customer in accordance with the Unauthorized Disclosure provisions of the UMSA. Workday shall take appropriate measures to address and mitigate the adverse effects of the Personal Data Breach. 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.

#### **7. Security of Processing.**

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

#### **8. Audit.**

Where Workday has obtained third-party audit reports and certifications for its Covered Services ("**Audit Reports and Certifications**"), Workday will, at Customer's request and subject to the confidentiality terms set forth in the UMSA, make its most recent Audit Reports and Certifications available to Customer for the applicable Covered Service.



To the extent that Workday has not obtained Audit Reports and Certifications for a Covered Service, or that Customer reasonably determines that the Audit Reports and Certifications are not sufficient to demonstrate compliance or to respond to a regulatory audit, Workday will allow Customer or an independent auditor appointed by Customer to conduct an audit, subject to the following: (a) Customer and Workday will mutually agree upon the scope, timing, duration, and control and evidence requirements; (b) Customer is responsible for all costs and fees related to such audit and will reimburse Workday for any services performed by Workday at Workday's then-current rates; and (c) to the extent the audit is conducted by a third-party audit firm, (i) the third-party audit firm is not a competitor of Workday and (ii) Customer has, prior to such audit, entered into an agreement with such third-party audit firm containing confidentiality terms no less protective than the confidentiality terms set forth in the UMSA

## **9. Data Protection Impact Assessments.**

Workday will, at Customer's request and subject to the confidentiality terms set forth in the UMSA, make its most recent Audit Reports and Certifications available to Customer. To the extent Customer requires additional assistance to meet its obligations under applicable Data Protection Laws to carry out a data protection impact assessment or prior consultation with the competent supervisory authority related to Customer's use of the Covered Service, Workday will, taking into account the nature of Processing and the information available to Workday, provide reasonable assistance to Customer.

## **10. Return and Deletion of Personal Data.**

Upon termination of the Covered Service, Workday shall, and shall cause any Subprocessors to, at the choice of Customer, return all Personal Data to Customer or securely delete Personal Data in accordance with the relevant provisions of the Agreement.

## **11. International Provisions.**

**11.1 Transfers of European Personal Data.** To the extent Customer's use of the Covered Services involves a Restricted Transfer, Addendum A to this DPE will apply.

**11.2 Processing of Personal Information of California Residents.** To the extent Customer instructs Workday to Process Personal Information of a California Resident, Addendum D to this DPE will apply.

**11.3 Specific Provisions for Certain Australian Customers** To the extent Workday Processes Personal Data relating to Data Subjects in Australia for a Customer subject to the Australia Privacy Act, Addendum C may apply.

## **12. General Provisions.**

**12.1 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 enter into this DPE and any transfer safeguards entered into under this DPE, issue instructions, and make and receive any communications or notifications in relation to this DPE on behalf of its Affiliates.

**12.2 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.

**12.3 Conflict.** This DPE is subject to the non-conflicting terms of the Agreement. With regard to the subject matter of this DPE, if inconsistencies between the provisions of this DPE and the Agreement arise, the provisions of this DPE shall prevail with regard to the parties' data protection obligations.

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

- i. 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.

**12.5 Remedies.** Customer's remedies (including those of its Affiliates) with respect to any breach by Workday (including any breach caused by Workday's Affiliates and Subprocessors) of the applicable 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.

**12.6 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.



## ADDENDUM A

### International Transfers of European Personal Data

#### 1. Definitions.

**"Data Privacy Framework"** means the EU-U.S., Swiss-U.S., and UK-U.S. Extension to the Data Privacy Framework maintained by the United States Department of Commerce determined to provide an adequate level of protection for Personal Data transfers to certified commercial organizations in the United States under (i) the European Commission's Adequacy Decision 2023/4745 of 10 July 2023 and (ii) other applicable Data Protection Laws.

**"SCCs"** means (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 ("**EU SCCs**"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the UK DPA (version B1.0 of 21 March 2022) as updated or amended ("**UK Addendum**"); and (iii) where the Swiss Federal Act on Data Protection applies, the EU SCCs with Swiss Amendments (Section 3.2.2.3).

**"Workday BCRs"** means Workday's EU Processor Binding Corporate Rules ("**EU BCRs**") and UK Processor Binding Corporate Rules ("**UK BCRs**"). The Workday BCRs are accessible through Workday's website (currently located at <http://workday.com/legal/bcrs.html>).

#### 2. Data Privacy Framework.

Workday, Inc. is self-certified to and complies with the Data Privacy Framework and will remain certified for the term of the Agreement.

#### 3. Transfer Mechanisms.

**3.1 BCRs.** The EU BCRs apply to the Processing of Personal Data protected by the EU GDPR and the UK BCRs apply to the Processing of Personal Data protected by the UK GDPR, for the Covered Services listed in Schedule 3 to the Workday BCRs. All provisions of the Workday BCRs are incorporated by this reference and shall be binding and enforceable for Customer according to Sections 1.3 and 1.4 of the Workday BCRs as if they were set forth in this DPE in their entirety. If any conflict or inconsistency arises between this DPE and the Workday BCRs, the Workday BCRs shall prevail.

#### 3.2 Standard Contractual Clauses.

**3.2.1 Processor-to-Processor SCCs.** Where Customer is contracting with Workday Limited, all Restricted Transfers of Personal Data will be governed by SCCs Module 3 implemented between Workday Limited (as "data exporter") and its Subprocessors (as "data importers").

**3.2.2 Controller-to-Processor SCCs.** Where the transfer from Customer to Workday is a Restricted Transfer, the SCCs will apply to such Restricted Transfers between Customer (as "data exporter") and Workday (as "data importer") as follows:

**3.2.2.1 EU Personal Data.** In relation to Personal Data protected by the EU GDPR, the EU SCCs will apply (and be incorporated into this DPE by this reference) completed as follows:

- i. Module 2 applies unless the Customer is a Processor in which case Module 3 applies;
- ii. in Clause 7, the optional docking clause will not apply;
- iii. in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes will be in accordance with the notification process set out in Section 3.2 of this DPE;

- iv. in Clause 11, the optional redress language will not apply;
- v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law specified in the UMSA, provided that law is an EEA Member State law recognizing third party beneficiary rights, otherwise, the laws of Ireland apply;
- vi. in Clause 18(b), disputes shall be resolved before the courts specified in the UMSA, provided these courts are located in an EEA Member State, otherwise those courts shall be the courts of Ireland;
- vii. Annex I of the EU SCCs shall be deemed completed with the information set out in Addendum B to this DPE; and
- viii. Annex II of the EU SCCs shall be deemed completed with the information set out in the Universal Security Exhibit to this DPE.

**3.2.2.2 UK Personal Data.** In relation to Personal Data protected by the UK GDPR (“**UK Personal Data**”), the UK Addendum will apply as follows:

- i. the EU SCCs, completed as set out in Section 3.2.2.1 of this Addendum A, shall also apply to transfers of UK Personal Data;
- ii. the UK Addendum shall be deemed executed (and incorporated into this DPE by this reference) between the transferring Customer and Workday, and the EU SCCs shall be deemed amended as specified by Part 2 (Mandatory Clauses) of the UK Addendum in respect of the transfer of UK Personal Data;
- iii. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from within this DPE and the EU SCCs, completed as set out in Section 3.2.2.1 of this Addendum A;
- iv. the start date of the UK Addendum (as set out in Table 1) shall be the effective date of this DPE; and
- v. Table 4 of the UK Addendum shall be deemed completed “neither party”.

**3.2.2.3 Swiss Personal Data.** In relation to Personal Data protected by the Swiss FADP, the EU SCCs will apply amended and adapted as follows:

- i. references to the EU and EU Member States shall mean Switzerland;
- ii. under Clause 18(c) of the EU SCCs, data subjects in Switzerland shall also have the right to sue for their rights at their place of habitual residence
- iii. references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss FADP; and
- iv. the Swiss Federal Data Protection and Information Commission is the supervisory authority.

**3.2.2.4 Clarifications.** The SCCs will be subject to the following clarifications:

- i. Workday will allow Customer to conduct audits as described in the SCCs in accordance with Section 8 of this DPE.





- ii. Customer authorizes Workday to appoint Subprocessors in accordance with Section 3 of this DPE, and Customer may exercise its right to object to Subprocessors under the SCCs in the manner set out in Section 3.
- iii. Workday shall return and delete Customer's data in accordance with Section 10 of this DPE.
- iv. Customer agrees that any assistance that Workday provides to Customer under the SCCs shall be provided in accordance with Section 8 of this DPE.
- v. Nothing in this Section 3.2.2 of this Addendum A varies or modifies the SCCs nor affects any supervisory authority's or Data Subject's rights under the SCCs. If any provision of this DPE contradicts, directly or indirectly, the SCCs, the SCCs shall prevail.

**3.3 Order of Precedence.** Where more than one transfer mechanism applies, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) the Workday BCRs, and (ii) the SCCs.

**3.4 Transfer Impact Assessments.** Workday has carried out transfer impact assessments in accordance with the GDPR evaluating Workday's opinion that the DPE including the Workday BCRs and SCCs provide appropriate safeguards taking into account the information available to Workday and the nature of the Processing. Upon request, Workday shall provide Customer with a summary of such transfer impact assessments to Customer.





## **ADDENDUM B**

### **Description of Processing**

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

##### **Data exporter**

Data exporter: Customer

Contact details: The individuals designated as named contacts by Customer in Customer's account

Relevant activities: Use of Workday's enterprise cloud applications.

Signature and Date: By entering into the Agreement, data exporter is deemed to have signed these SCCs incorporated herein as of the effective date of the Agreement.

Data exporter role: The data exporter's role is set forth in the DPE.

##### **Data importer**

Data importer: Workday

Contact details: Workday Privacy Team, [legal@workday.com](mailto:legal@workday.com)

Relevant activities: Provide and support enterprise cloud applications, including human resource and financial management.

Signature and Date: By entering into the Agreement, data importer is deemed to have signed these SCCs incorporated herein as of the effective date of the Agreement.

Data importer role: Processor

#### **B. DESCRIPTION OF TRANSFER**

##### **Categories of data subjects whose personal data is transferred**

1. Job applicants, candidates, current and former members of staff
2. Related persons (e.g., emergency contacts, dependents, or beneficiaries).
3. Staff of prospects, customers, business partners and suppliers.

##### **Categories of personal data transferred**

Customer determines the categories of Personal Data Processed within Covered Services subscribed to. Typically, the transferred personal data will include the categories of data identified below:

##### **1. Job applicants, candidates, current and former members of staff:**

Name; contact information (including home and work address; home and work telephone numbers; mobile telephone numbers; web address; instant messenger; home and work email address); marital status; citizenship information; visa information; national and governmental identification information; drivers' license information; passport information; banking details; military service information; date of birth and birth place; gender; 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; sentiments, personal opinions, feedback, training and development information; award information; membership information; information on emergency contacts, beneficiaries and dependents.

**2. Related persons:**

Name and contact information (including home address; home and work telephone numbers; mobile telephone numbers); date of birth; gender.

**3. Staff of prospects, customers, business partners and suppliers:** Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; instant messenger; work email address); business title; company; course enrollment information, including completion of courses, exam results and feedback provided.

**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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

Unless otherwise agreed, the transferred Personal Data may comprise special categories of personal data, such as ethnicity, religious beliefs, trade union membership information and health data (employee sick leave, disability information). Taking into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons, Workday has implemented the technical and organizational measures as described in the Universal Security Exhibit, including specialized training of staff and system access logs, to ensure an appropriate level of protection for such sensitive data.

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

Transfers will be made on a continuous basis.

**Nature of the processing**

Workday acts as a processor for the Personal Data Customer submits electronically into Workday's enterprise cloud applications or provides to Workday in connection with the Agreement.

1. Processing Personal Data to set up, operate, maintain and support the enterprise cloud applications
2. Storage of Personal Data in secure data centers
3. Provision of Covered Services

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

Provision of enterprise cloud applications and professional services (as applicable) to Workday customers.

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

Personal data will be retained for the duration of the Agreement in accordance with Section 12.2 of the DPE.



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

The subject matter and duration of the processing is outlined above within this Addendum B. The nature of the specific sub-processing services are further particularized within the Subprocessor List (currently located at: <https://www.workday.com/en-us/legal/subprocessors.html>).

### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The competent supervisory authority is determined in accordance with Clause 13 of the EU SCCs unless required otherwise by Addendum A Sections 3.2.2.2 (UK Personal Data) and 3.2.2.3 (Swiss Personal Data).



### **Technical and Organizational Measures**

The technical and organizational measures set forth in the Security Exhibit have been implemented by the data importer 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.



## **ADDENDUM C**

### **Specific Provisions for Certain Australian Customers**

The following applies only to Australian Customers that are subject to the Australia Privacy Act, where "Australian Privacy Act" means the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs). To the extent Workday Processes Personal Data relating to Data Subjects in Australia for such Australian Customers, the following terms shall apply:

For the avoidance of doubt the term:

"Data Protection Laws" includes the Australian Privacy Act; and

For purposes of this Addendum C, "Personal Data" shall include any Covered Data about an identified individual, or an individual who is reasonably identifiable (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not.

Customer shall obtain all consents from, and provide all notifications, to Data Subjects in Australia, that are necessary to enable Workday (and its Affiliates and Subprocessors) to lawfully Process Personal Data as contemplated by this DPE. Customer indemnifies Workday for any loss, damage, cost, expense, fine or liability arising from Customer's failure to obtain such consents or provide such notifications.

Customer agrees that if Workday provides notice of a Personal Data Breach in accordance with Section 6 of the DPE, notwithstanding any provision of applicable Data Protection Laws, as between the parties the Customer is fully responsible for, and will, undertake all notification requirements to Australian Data Subjects and relevant regulators, and will indemnify Workday for any loss, damage, cost, expense, fine or liability arising from Customer's failure to fulfil those notification requirements. Workday relies on the Customer to comply with this clause in satisfaction of section 26WM of the Australian Privacy Act.



## ADDENDUM D

### California Privacy Addendum

This California Privacy Addendum ("Addendum") supplements the DPE to which it is attached. Any term not defined in this Addendum shall have the meaning assigned to it, if any, in the DPE or the Agreement. To the extent the Agreement and this Addendum conflict, the terms of this Addendum shall take precedence with respect to Processing of Personal Data under the CCPA.

To the extent Workday Processes Personal Data under the CCPA, as defined above, the following supplemental terms shall apply to such Processing:

1. The terms "**Business**," "**Business Purpose**," "**Consumer**," "**Sell**," "**Service Provider**," and "**Share**," shall have the same meanings as provided for in the CCPA. As used in this Addendum, the term "**Personal Data**" shall refer to any data that qualifies as "Personal Information" under the CCPA.
2. **Roles of the Parties.** Customer, as a Business under the CCPA, is disclosing Personal Data to Workday, and Workday is Processing the disclosed Personal Data solely as a Service Provider.
3. **Business Purpose.** Workday will Process Personal Data for the purpose of providing the Services described in the Agreement, including in the associated Order Forms.
4. **Service Provider Processing Limitations.** Workday will not (i) Sell Personal Data, or (ii) retain, use or disclose Personal Data outside the direct business relationship with Customer or for any purpose other than to provide the Covered Services as articulated in the Agreement, including this Addendum, or as permitted by the CCPA
5. **No Sale or Sharing.** Workday will not Sell or Share Personal Data.
6. **No Combining Personal Data.** Workday will not combine Personal Data that it receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except as otherwise permitted by CCPA.
7. **Consumer Requests.** Workday will, in a manner consistent with the functionality of the applicable Service and Workday's role as a Service Provider, provide reasonable support to Customer to enable Customer to respond to Consumer requests to exercise their rights under the CCPA, as set forth in Section 4 of the DPE.
8. **Security of Processing.** Workday will maintain technical and organizational measures to protect Personal Data as set forth in the DPE and as required by the CCPA.
9. **Ongoing Compliance.** Workday agrees to comply with all applicable requirements of CCPA pertaining to its role as a Service Provider, including by providing the same level of privacy protection for Personal Data as required under CCPA. Customer shall have the right to take reasonable and appropriate steps to ensure compliance with this Addendum by exercising its rights in the audit provisions of the DPE. Customer shall also have the right to take reasonable and appropriate steps to stop or remediate any unauthorized Processing of Personal Data by Workday, for example by requesting that Workday provide a written statement confirming that applicable Personal Data has been deleted. Workday will notify Customer if it determines that it can no longer meet its obligations under the CCPA.