



## UNIVERSAL DATA PROCESSING EXHIBIT

Protecting the personal data our customers submit to Workday is one of our highest priorities and integral to the success of our business. These FAQs provide information to assist customers when (1) selecting Workday as an enterprise cloud provider to process their workers' personal data and (2) reviewing Workday's Universal Data Processing Exhibit.

These FAQs do not form part of the contract and are for informational purposes only.

- **What is Workday's role?**

Workday acts as a processor or service provider for the personal data our customers submit electronically into our enterprise cloud applications or, where applicable, submit to Workday for implementation and consulting services ("Personal Data"). As such, Workday processes Personal Data on behalf of and according to our customers' instructions who are the controllers (or businesses).

Workday's customers either act as the controller or the processor of such Personal Data as set out in Section 2.1 of the DPE.

- **Does Workday make available a data processing agreement?**

Workday offers a comprehensive Universal Data Processing Exhibit ("DPE") that operates seamlessly as part of Workday's MSA to provide robust contractual terms for Workday's processing of Personal Data.

The DPE supports Workday's one-to-many service delivery model and our underlying technical and operational processes, such as our certifications, the performance of audits and our use of subprocessors.

- **Who are the parties to the DPE?**

You are entering into our DPE as either a controller or a processor and Workday is your processor. Any subsequent processors (both internal Workday subsidiaries and third parties) are subprocessors of Workday but are not party to the DPE.

- **Will Workday's DPE work for companies operating globally?**

Workday has customers around the globe, so we offer our customers industry-leading data processing terms that address data protection requirements around the globe. Our DPE incorporates the core privacy principles that underlie many international data protection laws.

Traditionally, European data protection laws have been among the world's strictest. To provide our global customers with a robust framework, we have used the strict GDPR requirements as the baseline for our DPE. As new laws take effect, including comprehensive state privacy laws in the United States, we adjust as necessary to ensure continued compliance with data protection laws.

- **Does Workday comply with data protection laws?**

Workday complies with all data protection laws directly applicable to Workday.

Nevertheless, it is our customers' responsibility to determine whether it is appropriate for them to use our enterprise cloud applications to process their Personal Data in light of the specific laws and regulations to which they are subject. It is also our customers' responsibility to configure and use our enterprise cloud applications in a manner consistent with their legal and regulatory obligations.

- **Does Workday have a Privacy Statement?**

Yes, Workday maintains a privacy statement that applies when Workday is the controller of personal data. Currently, our privacy statement can be found here <https://www.workday.com/en-us/privacy.html>.

- **Does Workday's DPE cover professional services delivered by Workday?**

Yes, Workday's DPE covers consulting and professional services delivered by Workday.

- **How does the CCPA apply to Workday's enterprise services?**



**UNIVERSAL DATA PROCESSING EXHIBIT**

To the extent the CCPA, as amended by the California Privacy Rights Act or CPRA, (collectively “CCPA”), applies to Workday’s enterprise services, Workday acts as a service provider, which is defined by the CCPA as an entity that processes information on behalf of a business. Workday’s customers act as the business, which the CCPA defines as an entity that determines the purposes and means of the processing of consumers’ personal information. (These concepts are similar to the processor and controller roles under the EU’s General Data Protection Regulation.)

Under the CCPA, a service provider can only process personal information provided by a business for a business purpose pursuant to a written contract. Moreover, that contract must prohibit the service provider from retaining, using, or disclosing that personal information for any purpose other than for the specific purpose of performing the services specified in the contract. Workday’s standard subscription agreement and data protection terms with our customers provide that we can process our customers’ data only to provide the services they’ve contracted for.

Workday addresses the requirements of a service provider under the CCPA in the California Privacy Addendum attached to this DPE.

- **How does the Workday California Privacy Addendum mentioned above map to the requirements of the CCPA/CPRA for service provider agreements?**

For informational use only, the table below provides an overview of the CCPA/CPRA’s requirements for service provider agreements, and a non-exhaustive mapping to the corresponding provisions in the Workday California Privacy Addendum (attached to this DPE below).

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
<p><b>§1798.100(d)</b></p> <p>(d) A <i>business that collects a consumer’s personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:</i></p>	<p>(d)(1) Specifies that the Personal Information is sold or disclosed by the business only for limited and specified purposes.</p>	<p><u>ADDENDUM, Sec. 2:</u></p> <p>“<b>Roles of the Parties.</b> Customer, as a Business under the CCPA, is disclosing Personal Information to Workday, and Workday is Processing the disclosed Personal Information solely as a Service Provider.”</p> <p><u>ADDENDUM, Sec. 3:</u></p> <p>“<b>Business Purpose.</b> Workday will Process Personal Information for the purpose of providing the Services described in the Agreement, including in the associated Order Forms.”</p> <p><u>ADDENDUM, Sec. 4:</u></p> <p>“<b>Service Provider Processing Limitations.</b> Workday will not retain, use, or disclose Personal Information outside of the direct business relationship or for any purpose other than those articulated in the Agreement,</p>



**UNIVERSAL DATA PROCESSING EXHIBIT**

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
		including this Addendum, or as permitted by the CCPA.”
§1798.100(d)(2)	(d)(2) Obligates the service provider or contractor to comply with applicable obligations under the applicable state law and obligates those persons to provide the same level of privacy protection as is required by applicable state law.	<u>ADDENDUM, Sec. 9:</u> “ <b>Ongoing Compliance.</b> 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 Information as required under CCPA.”
§1798.100(d)(3)	(d)(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the service provider or contractor uses the Personal Information transferred in a manner consistent with the business’ obligations under applicable state law.	<u>ADDENDUM, Sec. 9:</u> “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 Data Processing Terms.”
§1798.100(d)(4)	(d)(4) Requires the service provider or contractor to notify the business if it makes a determination that it can no longer meet its obligations under applicable state law.	<u>ADDENDUM, Sec. 9:</u> “Workday will notify Customer if it determines that it can no longer meet its obligations under the CCPA.”
§1798.100(d)(5)	(d)(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.	<u>ADDENDUM, Sec. 9:</u> “Customer shall also have the right to take reasonable and appropriate steps to stop or remediate any unauthorized Processing of Personal Information by Workday, for example by requesting that Workday provide a written statement confirming that applicable Personal Information has been deleted.”



**UNIVERSAL DATA PROCESSING EXHIBIT**

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
<p>§ 1798.140. Definitions <i>(ag) “Service provider” means a person that processes personal information on behalf of a business and to that receives from or on behalf of the business a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:</i></p>	<p>(1)(A) Selling or sharing the personal information;</p>	<p><u>ADDENDUM, Sec. 5:</u>  <b>“No Sale or Sharing or Personal Data.</b> Workday will not Sell or Share Personal Information.”</p>
<p>§1798.140(ag)(1)(B)</p>	<p>(1)(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.</p>	<p><u>ADDENDUM, Sec. 3:</u>  <b>“Business Purpose.</b> Workday will Process Personal Information for the purpose of providing the Services described in the Agreement, including in the associated Order Forms.”</p> <p><u>ADDENDUM, Sec. 4:</u>  <b>“Service Provider Processing Limitations.</b> Workday will not retain, use, or disclose Personal Information outside of the direct business relationship or for any purpose other than those articulated in the Agreement, including this Addendum, or as permitted by the CCPA.”</p>
<p>§1798.140(ag)(1)(C)</p>	<p>(1)(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.</p>	<p><u>ADDENDUM, Sec. 4:</u>  <b>“Service Provider Processing Limitations.</b> Workday will not retain, use, or disclose Personal Information outside of the direct business relationship or for any</p>



**UNIVERSAL DATA PROCESSING EXHIBIT**

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
		purpose other than those articulated in the Agreement, including this Addendum, or as permitted by the CCPA.”
§1798.140(ag)(1)(D)	(1)(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency.	<u>ADDENDUM, Sec. 6:</u> <b>“No Combining Personal Information.</b> Workday will not combine Personal Information that it receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person(s), or collects from its own interaction with a consumer, except as otherwise permitted by CCPA.”
§1798.140(ag)(1)(D) (continued)	The contract may, subject to agreement with the service provider, permit the business to monitor the service provider’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.	Customer audit rights are primarily addressed in Section 8 of the DPE. <u>Also, ADDENDUM, Sec. 9:</u> “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.”
§1798.140(ag)(2)	(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing	Use and engagement of subprocessors is addressed, in <u>Section 3 of the DPE.</u> <u>ADDENDUM, Sec. 9:</u> <b>“Ongoing Compliance.</b> Workday agrees to comply with all



**UNIVERSAL DATA PROCESSING EXHIBIT**

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
	<p>personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).</p>	<p>applicable requirements of CCPA pertaining to its role as a Service Provider, including by providing the same level of privacy protection for Personal Information as required under CCPA.”</p>
<p>§ 1798.121. Consumers’ Right to Limit Use and Disclosure of Sensitive Personal Information (c)</p>	<p>(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.</p>	<p><u>ADDENDUM, Sec. 4:</u>  <b>“Service Provider Processing Limitations.</b> Workday will not retain, use, or disclose Personal Information outside of the direct business relationship or for any purpose other than those articulated in the Agreement, including this Addendum, or as permitted by the CCPA.”</p> <p><u>ADDENDUM, Sec. 7:</u>  <b>“Consumer Requests.</b> 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 the data subject request provisions of the Data Processing Terms.”</p> <p><u>DPE Section 2.2:</u>  <b>“Instructions for Processing.</b> Workday shall Process Personal Data in accordance with Customer’s documented instructions.”</p> <p><u>Comment:</u> The WORKDAY CALIFORNIA PRIVACY</p>



**UNIVERSAL DATA PROCESSING EXHIBIT**

CCPA CITATION	CPRA REQUIREMENT	WORKDAY CALIFORNIA PRIVACY ADDENDUM (or DPE Provision) & Comments
		<p>ADDENDUM is intended only to fill any gaps not otherwise addressed in the existing DPE. The Addendum is not intended to replace the DPE, which includes requirements that Workday Process Personal Data in compliance with any documented instructions from a Customer, such as those referenced in the cited regulation.</p>
<p>§ 1798.130. Notice, Disclosure, Correction, and Deletion Requirements</p> <p>(a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:</p>	<p>(3)(A) [...] A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same.</p>	<p><u>ADDENDUM, Sec. 7:</u></p> <p><b>“Consumer Requests.</b> 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 the data subject request provisions of the Data Processing Terms.”</p>
<p>§ 1798.81.5</p>	<p>(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.</p>	<p>DPE Section 7:</p> <p><b>7. Security of Processing</b></p> <p>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.</p>

## UNIVERSAL DATA PROCESSING EXHIBIT

### Subprocessors

- **Does Workday use subprocessors?**

Workday uses subprocessors to provide the Covered Services. Any subprocessor that Workday engages to process our customers' Personal Data undergoes a thorough information security and data protection due diligence review and agrees to abide by data protection terms no less protective than the DPE.

- **Which subprocessors is Workday using?**

Workday's subprocessor list can be accessed through the Workday website at <https://www.workday.com/en-us/legal/subprocessors.html>.

- **How does Workday inform its customers about new subprocessors?**

Workday will update the subprocessor list at least thirty days prior to authorizing a new subprocessor to process Personal Data. Customers can subscribe to receiving email notifications for each Covered Service by signing up here. Our customers are responsible for ensuring that the individuals in their organization who need to be notified about new subprocessors (e.g., their Privacy Team or Data Protection Officer) subscribe to the relevant Covered Service email updates and monitor their email accounts.

- **Can customers object to Workday's use of a new subprocessor?**

Where required by law, Workday's customers can object to Workday's use of a new subprocessor on reasonable grounds relating to data protection. If Workday decides to retain a subprocessor to which a customer has objected, then the customer has the option to terminate the affected Covered Service.

### For International Data Transfers

- **How does Workday protect Personal Data transferred outside of Europe?**

Workday uses the following data transfer mechanisms to legitimize transfers of Personal Data outside of Europe:

#### **Adequacy Decisions**

The European Commission [recognizes certain countries](#) around the world as offering an adequate level of protection for personal data. The UK and Switzerland recognize the same countries. Workday relies on adequacy decisions in relation to transfers of Personal Data to New Zealand, Switzerland or the UK.

#### **Binding Corporate Rules**

Workday is one of the few companies worldwide to have an approved set of Processor Binding Corporate Rules (or "BCRs"). BCRs are a set of internal data protection policies that govern personal data processing within a multinational group. Under its BCRs, Workday can share the Personal Data it processes on behalf of its customers within its group in compliance with EU data protection laws. A list of enterprise cloud applications covered by the BCRs is provided in Addendum B of the DPE. The BCRs are accessible on Workday's website at <https://www.workday.com/en-us/why-workday/security-trust.html>.

#### **Standard Contractual Clauses**

Workday offers the European Commission's Standard Contractual Clauses (Commission Implementing Decision 2021/914 of 4 June 2021) ("SCCs"). The new SCCs were introduced in June 2021 to incorporate additional protections for transferred data.

The UK's Information Commissioner Office has validated the European Commission's SCCs as an equal alternative to the UK only international data transfer agreement ("UK IDTA"). This simplifies the position for businesses with UK data. For consistency across our customer base, we implement the SCCs via the ICO's "UK Addendum" as opposed to the UK IDTA within Workday's IGDTPA.

## UNIVERSAL DATA PROCESSING EXHIBIT

Switzerland has recognized the SCCs as the basis for personal data transfers to a country without an adequate level of data protection, provided that the necessary adaptations and amendments are made for use under Swiss data protection legislation (as set out below).

- **How does Workday assist customers in conducting transfer impact assessments (TIAs)?**

Workday has conducted transfer impact assessments in line with the recommendations issued by the European Data Protection Board. Workday has published a comprehensive TIA Whitepaper to assist customers who choose to perform their own TIAs in connection with their use of Workday's enterprise cloud applications.

### **General Data Protection Regulation**

- **What is the General Data Protection Regulation?**

The General Data Protection Regulation (the "EU GDPR") is a European data protection law that took effect on May 25, 2018. The EU GDPR sets a global standard for data protection compliance by implementing strict requirements on how organizations handle and protect personal data. Following Brexit, section 3 of the European Union (Withdrawal) Act 2018 brought the EU GDPR into UK law (the "UK GDPR"). For the purpose of our relationship with our customers, at this time, they do not differ in substance, so we refer to both laws collectively as "GDPR."

We are committed to supporting our customers' journey to compliance with the GDPR when they use Workday's enterprise cloud applications.

- **How does Workday assist its customers in fulfilling their obligations to respond to data subject requests under Chapter III of the GDPR?**

Workday offers a suite of configurable features to help customers respond to their workers' requests to exercise their data protection rights such as requests to access, correct, delete or restrict the processing of their Personal Data and comply with data portability requests under the GDPR.

- **What technical and organizational measures has Workday implemented to protect Personal Data?**

Workday has implemented robust technical and organizational measures designed to protect our customers' Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

However, data security is a shared responsibility. Our customers are responsible for implementing and maintaining privacy protections and security measures for components of the Workday enterprise cloud applications that they control.

Workday is certified to various industry standards such as ISO 27001, 27017, and 27018. See Workday's SOC 2 reports for more information on our technical and organizational measures.

Furthermore, Workday adheres to the [EU Cloud Code of Conduct](https://eucoc.cloud/en/public-register/list-of-adherent-services/) (EUCoC) which provides independent third-party verification of Workday's technical and organizational measures. According to Article 28 (5) of the EU GDPR, adherence to a Code of Conduct can be used to demonstrate that sufficient guarantees have been made to implement appropriate technical and organizational measures as a processor. Workday's adherence report can be accessed at <https://eucoc.cloud/en/public-register/list-of-adherent-services/>.

- **How does Workday assist its customers fulfilling their obligation to notify personal data breaches?**

Under the GDPR, controllers must notify the competent data protection supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Workday maintains incident response policies and plans, including a security incident policy, an incident response plan and a breach disclosure plan. If Workday becomes aware of a personal data breach affecting our customers' Personal Data, Workday will notify our customers without undue delay and assist our customers to meet their personal data breach notification obligations by providing the relevant information regarding the personal data breach.

**UNIVERSAL DATA PROCESSING EXHIBIT**

- **How does Workday assist its customers with the GDPR requirements to conduct data protection impact assessments and prior consultations in relation to their use of a Workday enterprise cloud application?**

To help identify risks to individuals’ rights, Article 35 of the GDPR requires controllers to carry out a Data Protection Impact Assessment (“DPIA”) if a specific processing activity is likely to result in a “high risk” to the rights and freedoms of an individual.

Where customers require additional information from Workday to carry out a DPIA in relation to their use of our enterprise cloud applications, they can rely on the information in Workday’s application audit reports and certifications. In addition, our customers can request Workday’s assistance.

- **Does Workday’s DPE meet the GDPR requirements for a data processing agreement?**

Workday’s DPE addresses the specific data processing agreement requirements laid out in Article 28 of the GDPR. The quick reference checklist below identifies each of the specific requirements of Article 28 GDPR and matches them against the relevant sections of Workday’s DPE.

GDPR Requirement		DPE
Art. 28 (3)	<b>Subject-matter</b> and duration of the processing, the <b>nature and purpose</b> of the processing.	Sec. 11.1
Art. 28 (3)	<b>Type of personal data</b> and <b>categories of data subjects</b> .	Sec. 11.1
Art. 28 (3) (a)	Processor processes the personal data only on <b>documented instructions</b> from the controller.	Sec. 2.2
Art. 28 (3) (b)	Persons authorized to process the personal data have committed themselves to <b>confidentiality</b> or are under an appropriate statutory obligation of confidentiality.	Sec. 5
Art. 28 (3) (c)	Processor has taken all <b>measures required pursuant to Article 32</b> (Security of Processing).	Sec. 7
Art. 28 (3) (d)	Processor respects the conditions referred to in paragraph 2 and 4 for <b>engaging another processor</b> .	Sec. 3
Art. 28 (3) (e)	Processor assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to <b>requests for exercising the data subject's rights</b> .	Sec. 4
Art. 28 (3) (f)	Processor assists the controller in ensuring <b>compliance with the obligations pursuant to Articles 32 to 36</b> .	
	<b>Article 32</b> (Security of processing)	Sec. 7
	<b>Article 33</b> (Notification of a personal data breach to the supervisory authority) <b>Article 34</b> (Communication of a personal data breach to the data subject)	Sec. 6
	<b>Article 35</b> (Data protection impact assessment) <b>Article 36</b> (Prior consultation)	Sec. 11.2



**UNIVERSAL DATA PROCESSING EXHIBIT**

Art. 28 (3) (g)	Processor will, at the choice of the controller, <b>delete or return all the personal data</b> to the controller after the end of the provision of services.	Sec. 9
Art. 28 (3) (h)	Processor makes available to the controller all <b>information necessary to demonstrate compliance</b> with the obligations laid down in this Article and <b>allow for and contribute to audits</b> , including inspections, conducted by the controller or another auditor mandated by the controller.	Sec. 8