Global FAQ to the Universal Data Processing Exhibit

Protecting the personal data our customers submit to Workday is one of our highest priorities and is 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 (or "**DPE**").

These FAQs do not form part of the contract or the DPE 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 DPE that operates seamlessly as part of Workday's UMSA 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 at 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?

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 the 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 the DPE). Note: The WORKDAY CALIFORNIA PRIVACY 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.

CCPA or Regulation Requirement	Workday California Privacy Addendum or DPE Section
§1798.100(d)(1) Requires businesses that sell personal information to enter into an agreement with the service provider or third party, which specifies the Personal Information is sold or disclosed by the business only for limited and specified purposes.	ADDENDUM, Sec. 2: "**Roles of the Parties**" ADDENDUM, Sec. 3: "**Business Purpose**" ADDENDUM, Sec. 4: "**Service Provider Processing Limitations**"
§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.	ADDENDUM, Sec. 9: "**Ongoing Compliance**"
§1798.100(d)(3)	ADDENDUM, Sec. 9: "**Ongoing Compliance**"

CCPA or Regulation Requirement	Workday California Privacy Addendum or DPE Section
(d)(3) Grants the business rights to take reasonable and appropriate steps to ensure the service provider uses of personal information are consistent with the business' obligations under applicable state law.	
§1798.100(d)(4) (d)(4) Requires the service provider or contractor to notify the business if it determines it can no longer meet its obligations under applicable state law.	ADDENDUM, Sec. 9: "**Ongoing Compliance**"
§1798.100(d)(5) (d)(5) Grants the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.	ADDENDUM, Sec. 9: "**Ongoing Compliance**"
§ 1798.140. Definitions *(ag)* Requirement that service provider agreement prohibit the sale or sharing of personal information;	ADDENDUM, Sec. 5: "**No Sale or Sharing or Personal Data**"
§1798.140(ag)(1)(B) (1)(B) concerning the limited business purposes specified in the contract on retaining, using, or disclosing personal information.	ADDENDUM, Sec. 3: "**Business Purpose**" ADDENDUM, Sec. 4: "**Service Provider Processing Limitations**"
§1798.140(ag)(1)(C) (1)(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.	ADDENDUM, Sec. 4: "**Service Provider Processing Limitations**"
§1798.140(ag)(1)(D) (1)(D) restrictions on combining personal information.	ADDENDUM, Sec. 6: "**No Combining Personal Information**"

CCPA or Regulation Requirement	Workday California Privacy Addendum or DPE Section
§1798.140(ag)(1)(D) (continued) Concerning requirement for the business to monitor the service provider's compliance with the contract through measures, including, 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. See also, ADDENDUM, Sec. 9: "**Ongoing Compliance**"
§1798.140(ag)(2) (2) service provider requirement to notify a business of the engagement of another party to assist it in processing personal information, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).	Use and engagement of subprocessors is addressed, in Section 3 of the DPE. See also ADDENDUM, Sec. 9: "**Ongoing Compliance**"
§ 1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information (c) (c) concerning service provider restrictions on use of sensitive personal	ADDENDUM, Sec. 4: "**Service Provider Processing Limitations**" ADDENDUM, Sec. 7: "**Consumer Requests**" DPE Section 2.2: "**Instructions for Processing**"
§ 1798.130. Notice, Disclosure, Correction, and Deletion Requirements (a)(3)(A) […] concerning a service provider's assistance with a consumer request.	ADDENDUM, Sec. 7: "**Consumer Requests**"
§ 1798.81.5 (c) concerning security requirements to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.	DPE Section 7: **7. Security of Processing**

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.

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 (and properly certified commercial organizations) around the world as offering an adequate level of protection for personal data. Workday relies on adequacy decisions in relation to transfers of Personal Data to the United States ("**U.S.**"), New Zealand, Switzerland and the UK.

U.S. Data Privacy Frameworks

Workday, Inc. is self-certified under the EU-U.S., Swiss-U.S. and UK-U.S. Extension to the Data Privacy Framework maintained by the U.S. Department of Commerce. Workday, Inc.'s certifications can be inspected in the official Data Privacy Framework List of the U.S. Department of Commerce by searching for 'Workday'.

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 and UK data protection laws. A list of enterprise cloud applications covered by the BCRs is provided in the DPE and BCRs. The BCRs are accessible on Workday's website at http://workday.com/legal/bcrs.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 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.

Switzerland recognizes 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 in the DPE).

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 ("**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.

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 applicable 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)	**Subject-matter** and duration of the processing, the **nature and purpose** of the processing.	Sec. 2.4
Art. 28 (3)	**Type of personal data** and **categories of data subjects**.	Sec. 2.4
Art. 28 (3) (a)	Processor processes the personal data only on **documented instructions** from the controller.	Sec. 2.2
Art. 28 (3) (b)	Persons authorized to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality.	Sec. 5
Art. 28 (3) (c)	Processor has taken all **measures required pursuant to Article 32** (Security of Processing).	Sec. 7
Art. 28 (3) (d)	Processor respects the conditions referred to in paragraph 2 and 4 for **engaging another processor.**	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 **requests for exercising the data subject's rights**.	Sec. 4
Art. 28 (3) (f)	Processor assists the controller in ensuring **compliance with the obligations pursuant to Articles 32 to 36.**	
	Article 32 (Security of processing)	Sec. 7
	Article 33 (Notification of a personal data breach to the supervisory authority) **Article 34** (Communication of a personal data breach to the data subject)	Sec. 6
	Article 35 (Data protection impact assessment) **Article 36** (Prior consultation)	Sec. 9

Art. 28 (3) (g)	Processor will, at the choice of the controller, **delete or return all the personal data** to the controller after the end of the provision of services.	Sec. 10
Art. 28 (3) (h)	Processor makes available to the controller all **information necessary to demonstrate compliance** with the obligations laid down in this Article and **allow for and contribute to audits**, including inspections, conducted by the controller or another auditor mandated by the controller.	Sec. 8