Workday Universal Data Processing Exhibit
Frequently Asked Questions

Protecting our customers' personal data is one of Workday's highest priorities and is integral to the success of our business. These FAQs provide information to assist customers when (1) selecting Workday as a software-as-a-service 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 for the personal data our customers submit electronically into our software-as-a-service 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.

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.

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.

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 software-as-a-service 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 software-as-a-service applications in a manner consistent with their legal and regulatory obligations.

Subprocessors

Does Workday use subprocessors?

Workday uses subprocessors to provide the Covered Services (e.g., as part of our global follow-the-sun operations to make updates to our software-as-a-service applications and prevent or address service or technical issues). 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 our 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

Is Personal Data transferred outside Europe?

In order to provide its software-as-a-service applications, Workday may use subprocessors (both Workday affiliates and third parties) located outside the European Economic Area ("EEA"), the United Kingdom ("UK") and Switzerland (together, "Europe"). For example, Workday provides follow-the-sun 24/7 support which necessarily means processing data in multiple time zones.

How does Workday protect Personal Data transferred outside of Europe?

Workday uses the following data transfer mechanisms to legitimise 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 software-as-a-service 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 has indicated that the SCCs can also be used as a safeguard to legitimatize transfers of personal data from the UK to processors located in other countries.

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).

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

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

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 you, 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 software-as-a-service applications.

How does Workday assist our 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 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 software-as-a-service 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 data processor. Workday’s adherence report can be accessed at https://eucoc.cloud/en/public-register/list-of-adherent-services/.

How does Workday assist our customers fulfilling their obligation to notify personal data breaches?

Under the GDPR, our customers, as 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 our customers with the GDPR requirements to conduct data protection impact assessments and prior consultations in relation to their use of a Workday software-as-a-service 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 software-as-a-service applications, they can rely on the information in Workday’s application audit reports and certifications. In addition, our customers can request Workday’s assistance under our optional, fee-based Customer Audit Program.

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		Relevant Section in DPE
Art. 28 (3)	**Subject-matter** and duration of the processing, the **nature and purpose** of the processing.	Sec. 11.1
Art. 28 (3)	**Type of personal data** and **categories of data subjects**.	Sec. 11.1
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. 11.2
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. 9
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