Europe Union and United Kingdom Privacy Overview

Overview of European Union (EU) and United Kingdom (UK) Privacy Landscape

Introduction

As a leading provider of enterprise cloud applications for human resources, financial management, and planning, privacy is a top priority at Workday. We employ rigorous measures across our people, processes and technology to protect the privacy of our customers' data. Workday's core values and "privacy by design" philosophy guides all aspects of Workday's product lifecycle and comprehensive and robust privacy program.

Workday is proud to have a global footprint representing over 10,000 companies and recognizes that our wide-spanning customer base has a diverse set of regulatory and compliance needs. Workday is dedicated to fostering our customers' confidence in our service, and below we highlight some of the key regulatory and compliance considerations our customers are subject to while explaining how our privacy and security practices satisfy those needs.

Europe

European Union and European Economic Area (EEA)

As of May 25, 2018, the global privacy landscape was significantly altered with the implementation of the General Data Protection Regulation (GDPR). The GDPR sets a high standard for data protection compliance by implementing strict requirements on how organizations handle and protect personal data. The GDPR has become the seminal privacy and security law and Workday has long been able to confidently assert its commitment to compliance since GDPR's implementation.

General Data Protection Regulation

As a general rule, the GDPR applies to all companies established in the European Union (EU), regardless of whether they're a controller or a processor. However, under certain circumstances, the GDPR can also apply to companies located outside of the EU if they process personal information of individuals in the EU when offering goods or services to such individuals or monitoring their behavior.

Workday acts as a processor for the personal data our customers submit electronically into our enterprise cloud applications. Because Workday processes personal data on behalf of and according to our customers' instructions, Customers are the controllers.

The GDPR grants eight fundamental consumer privacy rights to individual data subjects as they pertain to personal data. These rights result in compliance obligations that can often be complex for companies subject to GDPR, such as contractual requirements for handling personal data, third party processing requirements, security obligations, appointments of data protection officers, and cross-border transfer requirements. However, Workday has robust experience in steadfastly complying with GDPR and helps enable your compliance by:

- offering a suite of configurable privacy and compliance 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. In the unlikely event that an individual writes directly to Workday, we forward the correspondence to the customer identified by the data subject promptly.
- implementing recurring role-based employee training on security and privacy practices;
- developing processes to capture Data Protection Impact Assessments (DPIAs),
- offering data transfer mechanisms to legalize transfers of personal data outside of the European Economic Area (as detailed below),
- maintaining records of processing activities;
- mapping GDPR requirements to our SOC2 controls; and
- appointing its own Data Protection Officer which provides oversight and monitoring for Workday's GDPR compliance.

Workday continuously monitors guidance from EU supervisory authorities to ensure that our compliance program remains up-to-date.

United Kingdom

Within the UK, data protection obligations are regulated by the Data Protection Act and the 'UK GDPR', Heavily based on GDPR, the UK GDPR sets out the key principles, rights and obligations for processing of personal data in the UK, except for law enforcement and intelligence agencies. The UK GDPR has some important differences from GDPR and/or other global data protection laws, including nuanced differences in data transfer requirements and enhanced data security requirements.

Workday serves as a data processor to our customers, and our contract terms include data processing obligations designed to satisfy EEA and UK privacy and data protection requirements, including the applicable standard contractual clauses ("SCCs") to facilitate a customer transferring personal data outside of the EEA or UK. Our DPE (defined below)--along with other contractual mechanisms like Workday's relevant SCCs and BCRs (defined below) --demonstrates that we have appropriate controls in place to process our customers' data in compliance with data processing requirements. Our suite of privacy and security protections is constantly reassessed to ensure European, UK, and global compliance.

International Data Transfers

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 that offer an adequate level of protection for personal data for data transfers from the EU. The UK and Switzerland recognize the same countries.

The EU-U.S. Data Privacy Framework (DPF). The DPF establishes a binding adequacy decision and EU supervisory authorities must accept the adequacy decision as creating a valid mechanism for EU-U.S. data transfers in compliance with the transfer provisions of the GDPR. For companies certified to the DPF, a transfer impact assessment (TIA), which is a formal risk assessment to assess all applicable privacy risks and mitigating safeguards relating to those risks, is not required. Customers can find the link to the DPF certification lists on workday.com/trust. We will maintain the certification throughout the term of the Master Subscription Agreement between Workday and its customers.

Binding Corporate Rules. Workday is one of the few companies worldwide to have an approved set of Processor Binding Corporate Rules (BCRs). Binding Corporate Rules 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. Workday's BCRs are readily available to our customers. In order to leverage the BCRs as an additional transfer mechanism, certain provisions need to be incorporated into the customer's data processing terms to make the provisions of the BCRs enforceable between Workday and its customers. Workday customers who want to incorporate Workday's BCRs into their existing data processing terms should visit Workday Community and review our BCR FAQ. The BCRs are accessible on Privacy: Transparency and Trust (workday.com).

Standard Contractual Clauses. Workday offers the European Commission's Standard Contractual Clauses (Commission Implementing Decision 2021/914 of 4 June 2021) (SCCs). The SCCs are a widely used safeguarding tool for international transfers. The 2021 SCCs are in a template format approved by the European Commission so there is very little need for amendments, if at all. We have ensured the 2021 SCCs are aligned across our customer base with the one-to-many service delivery model we offer, so there is less for our customers to worry about. Under the 2021 SCCs, the responsibility for conducting TIAs primarily sits with the data exporter. Workday provides resources to assist customers in performing TIAs in connection with their use of Workday's software-as-a-service application.

Workday's Commitment to Privacy and Security

Workday stridently maintains an up-to-date suite of privacy protections that comply with global privacy regulations. By instituting a series of technical, administrative, and organizational standards derived from a "privacy by design" base, including special attention for privacy and security practices that support legal regime compliance with data protection laws and that facilitate cross-border data transfers, Workday forges ahead as an industry-leader in privacy.

We partner with our global customers to help them meet their compliance requirements, including assistance with their TIA prior to transferring personal data to third-party countries. We proactively share information, such as FAQs and whitepapers, to help you navigate these assessments. Our DPE, which provides strong contractual obligations and our comprehensive compliance and security programs - which include third-party audits and a wealth of international certifications - reflect a privacy and data protection program that is appropriately designed to protect our customers' data. Workday's highly configurable systems help enable our customers to meet the varying requirements of global data protection laws. e We continuously monitor cross-border transfer approvals and developments, and seek potential technical

solutions.

Workday maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats and prevent unauthorized access to our customers' data. Workday Trust details the specifics of our security program in our third-party security audits and international certifications. Workda's security program includes up-to-date SOC and ISO certifications alongside other specialized attestations including authorization to be a G-Cloud service provider, a certification indicating Workday's adherence to the EU Cloud Code of Conduct (CCoC), and the UK government-backed Cyber Essentials certification. We make all of these resources available to customers to facilitate compliance with their data protection processes and obligations.

For more information on Workday's Privacy Program (including regional datasheets for Canada & the US and APJ), compliance and security, we invite you to visit workday.com/trust.

Disclaimer

This document is for informational purposes only. Please note that Workday does not make any expressed or implied warranties in this paper.

1.925.951.9000 | 1.877.WORKDAY (1.877.967.5329) | Fax: 1.925.951.9001 | www.workday.com