Workday's Robust Privacy Program

Introduction

Workday is a leading provider of enterprise cloud applications for human resources and finance. Founded in 2005 by Dave Duffield and Aneel Bhusri and publicly traded since 2012, Workday applications for financial management, human resources,planning, spend management, and analytics have been adopted by more than 10,000 organizations around the world and across industries from medium sized businesses to more than 50% of the Fortune 500.

Protecting the privacy of our customers' personal data is one of our highest priorities. We understand data privacy regulations are quite complex, and businesses have to select a software provider whose data security and privacy practices are best-in-class and align with your regulatory needs. We want to help you understand our privacy practices so that you can determine whether our services satisfy your specific regulatory and compliance requirements. We are dedicated to fostering our customers' confidence in our services. This paper spells out Workday's approach to global data protection and highlights some of the regulatory requirements regarding personal data in various jurisdictions.

Workday's Privacy Principles

We are committed to three privacy principles that reflect our core values. These privacy principles drive how we train our employees, how we design and build products, and how we process personal data:

1. We put privacy first:
Privacy protections have been a fundamental component of our services from the beginning. We embed privacy into our people, processes, and technology, and our configurable privacy tools help customers meet complex privacy needs.

2. We innovate responsibly:
We embrace the concept of privacy by design. We understand that privacy requirements may differ based on industry, geography, and approach. To help you meet your obligations, Workday products include configurable privacy tools.

3. We safeguard fairness and trust:
A comprehensive compliance program underpins our privacy practices. We demonstrate how we protect your data through our robust third-party audits and certifications, which are listed below, and are often among the first to receive them.

Data Privacy and Personal Data

In this document, "privacy program" refers to the way Workday manages and safeguards the collection, transfer, use and storage of personal data. We define "personal data" as any piece of information related to an identified or identifiable individual that is provided to Workday by customers or their affiliates for processing in the Workday service.

Workday and our customers must comply with various international privacy regulations. These are the common privacy principles in most jurisdictions and Workday's Privacy Principles align with these elements:

- **Notice:** The data subject is made aware of what data is collected and how it will be used, disclosed, or shared, and with whom;
- **Choice:** The data subject has the ability to opt in or out of their data being collected, stored, or shared;
- **Access:** The data subject has access to their data for review or correction;
- **Use:** The data is used for the purpose agreed to by the data subject;
- **Disclosure:** The data is only shared for business needs and as agreed to by the data subject;
- **Security:** The business has appropriate safeguards to secure personal data.

The application of these privacy principles fall into two categories.

.1. **Notice, Access,Choice and Security.** These principles apply to our customers and their employees (or data subjects). Specifically, where required by law, Workday's customers are responsible for providing notice, access, and choice to individuals whose data is collected and used within the Workday services. Workday's services are designed to allow customers to achieve differentiated configurations, enforce user-access controls, and manage data categories that may be populated and made accessible on a country-by-country basis.

2. **Use, Disclosure and Security.** These principles apply to Workday in its role as the data processor. Of note, security is listed in both categories. Workday is responsible for maintaining a comprehensive, information-security program that contains technical and organizational safeguards designed to prevent unauthorized access, use or disclosure of customer data. To continuously protect your data, Workday has detailed operating policies, procedures, and processes for our data centers, network, and applications. As noted above, our customers also have security responsibilities to configure the service to meet their needs. We provide transparency into the geographical regions where your data is stored and processed. All of our commitments are set forth in the Master Subscription Agreement (MSA) and our standard Data Protection Exhibit (DPE). The DPE supplements the MSA and formalizes the terms and conditions applicable to the processing of a customer's personal data by Workday. The DPE describes our practices as it relates to access, processing, transfer, using, and storage of customer data. As a data processor, the DPE contractually obligates Workday to only process customer data on behalf of and as instructed by our customers, and only to the extent necessary to provide the Workday Service.

Workday's Privacy Program

Workday has implemented a holistic privacy program that is embedded into all of our services. This program is built upon our philosophy of "privacy by design," which guides how we build products and operate our services. Our Global Privacy team and Chief Privacy Officer (CPO) are responsible for:

• Formulating, maintaining, and updating Workday's internal privacy policies, procedures and tools to protect the privacy of personal data handled by our employees and partners on behalf of Workday;

• Monitoring compliance with our customer-facing privacy policies, which are audited annually by a third party;

• Ensuring that privacy commitments made to our customers, partners and employees are met;

• Maintaining the company's certifications and regulatory-compliance obligations;

• Training Workday staff on our privacy program; and monitoring changing data privacy laws across the globe and making necessary updates and modifications to our privacy program.

Policies and Procedures

Workday's privacy program was founded more than a decade ago. Because companies were unsure about cloud technology and Workday aimed to have a privacy program companies can trust, Workday developed comprehensive and strict policies and procedures regarding access, use, disclosure, and transfer of customer data by Workday. As a result of the maturity of Workday's privacy program, our teams are readily able to focus on new and emerging privacy concerns.

The core of our privacy program is that Workday employees and contractors (hereinafter "employees") do not access, use, disclose, or transfer customer data unless it is in accordance with a contractual agreement or at the direction of the customer. Access to customer data is limited based on business needs and job role. By design, Workday's applications equip customers with control over their data. While Workday provides its customers with the infrastructure supporting the applications, each customer is responsible for entering their data, configuring the applications, and implementing procedures to safeguard their data. Customers can authorize selected parties to have access to their data. In other words, the customer chooses who can access, use, and disclose their data.

Additionally, Workday's employees receive thorough privacy training as part of the onboarding process. All employees must

complete ongoing data privacy training that describes our requirements for the use, transfer, access, and disclosure of customer data. Workday employees who require access to unencrypted customer data as part of their job (such as the customer support team) receive additional training and regular refreshers on Workday's privacy policies.

Privacy by Design

Workday's privacy-by-design philosophy underlies many privacy-enhancing features in our applications. The CPO and Privacy teams evaluate new features early in the development stage to assess and address potential privacy impacts. Additionally, Workday's Chief Privacy Officer reviews and approves all major releases before they become generally available. Workday applications may be configured to mask or purge certain data to meet the requirements of data protection laws. Customers also have the ability to include individuals or an employee-selected group, such as Works Councils, in relevant business processes to further safeguard the privacy of personal data.

Certifications and Audits

Our international certifications and third-party audits demonstrate our commitment to data security and privacy, protection against data breaches, security threats, and unauthorized access to our customers' data. In addition to comprehensive policies and procedures, Workday maintains a transparent privacy program. We engage independent third parties to conduct audits and maintain a variety of certifications to help ensure our privacy and security programs operate effectively. Details of these audits, certifications and compliance efforts are available to our customers.

ISO 27001 and 27018

To affirm our commitment to privacy and security, Workday is ISO 27001 and ISO 27018 certified through an independent assessment of our business's conformity to predefined ISO standards. The scope of the ISO 27001 and ISO 27018 certificates includes the management of information security and protection of personal data for Workday's cloud-based enterprise applications related to the processing of customer data. The ISO 27018 certification helps to ensure that customers stay in control of their own data. Workday only processes personal data provided to us by customers, with complete transparency regarding how their data is returned, transferred, and deleted if the agreement comes to an end. In order to maintain our ISO certifications, annual surveillance audits are conducted in addition to an ISO recertification audit conducted every three years.

SOC 1

Every six months, Workday issues a Service Organization Controls 1 (SOC 1) Type II report, in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). An independent third-party auditor conducts this audit to demonstrate that Workday's controls associated with production systems are operating effectively. Areas covered within this report include change management, access management, training,and physical security measures.

SOC 2

Annually, Workday publishes a Service Organization Controls 2 (SOC 2) Type II report based on the Trust Services Criteria. The SOC 2 report, like the SOC 1 report, attests to the evaluation of existing controls. Currently, Workday's SOC 2 evaluation addresses the security, confidentiality, privacy and availability principles of the Trust Services Principles and Criteria of the American Institute of Certified Public Accountants. The SOC 2 report provides our customers additional insight into Workday's privacy, security, and availability practices and the operating effectiveness of controls associated with any Workday deployment that contains customer data. Consistent with the SOC 1 reports an independent third-party auditor evaluates the SOC 2 controls according to industry standards. Examples of additional topics covered in this report include measures on disaster recovery, data privacy, processing integrity, and availability.

Please find more information on Workday's compliance program at Compliance and Third Party Assessments | Workday.

Global Privacy Efforts

We recognize that countries all over the world have enacted comprehensive privacy laws. Workday stridently maintains an up-to-date suite of privacy protections designed to help our customers comply with complex global privacy and 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 data protection laws and that facilitate cross-border data transfers, Workday's data protection safeguards address most requirements. For example, Workday's Master Subscription Agreement (MSA) and Universal Data Processing Exhibit (UDPE) harmonize the data processing terms across our various offerings and provide our customers a robust set of terms designed to satisfy the main data protection contractual requirements under various national laws. Also, Workday's highly configurable systems help enable our customers to meet the varying requirements of data protection laws.

Additionally, where customers must undergo privacy impact assessments, customers can rely on the information in Workday's application audit reports and certifications and customers can utilize Workday's fee-based Customer Audit Program for additional assistance. Workday also maintains incident response policies in the event of a security incident.

For more information on specific geographical requirements and Workday's commitments, please see our datasheets for Canada & the United States (US), Asia, Pacific and Japan (APJ), and the European Union (EU) and the United Kingdom (UK).

U.S. GOVERNMENT ACCESS TO CUSTOMER DATA

Workday's current and prospective customers are sometimes concerned about the potential of the U.S. government gaining access to their data in the Workday applications. Workday is committed to protecting the privacy and security of our customers' data and meeting our obligations as a processor of that data. We've published a summary of our Government Access Principles for our customers in Workday Community. Most importantly, Workday understands that the data we process in the Workday enterprise cloud applications belongs to our Customers. Workday won't disclose such data to a government agency unless compelled by law.

It is also worth noting that, in most cases where the U.S. government is interested in the type of enterprise human resources or financial data Workday stores, the U.S. government has existing agreements or alternate methods of gaining access to that data. In all likelihood, if the U.S. government is interested in customer data that is maintained in the Workday applications, the request for information would be made directly to the customer who has the relationship with the data subject. Additionally, and to the extent permitted by law, Workday would notify customers of these requests. Providing transparency to our customers in the event we receive a valid legal process from law enforcement or other government agencies for access to electronic information customers submit into Workday's software-as-a-service applications ("Government Request") is an ongoing part of that Workday commitment. Workday publishes a Transparency Report twice a year of any Government Requests from any U.S. law-enforcement agency or other U.S.-government agency, or any law-enforcement agency or other government agency outside of the United States.

PRIVACY IN NEW AND EMERGING TECHNOLOGIES

At Workday, we take a balanced approach that allows us to leverage the latest advancements in AI and ML technology, while preserving our commitment to privacy and AI Ethics principles. Workday's Responsible AI team takes advantage of Workday's long history of privacy-by-design principles in the development and management of our AI governance program. Responsible AI works closely with the oCPO and the privacy team on key aspects of the program including Workday's principles, policies, standards, and guidelines. Also, these teams are closely-knit to help ensure no one works in silos.

Conclusion

Workday's array of international certifications, third-party audits and contractual commitments serve as a testament to our robust privacy program. Workday complies with global security and privacy protocols, including SOC 1 Type II, SOC 2 Type II, Privacy Shield, Asia-Pacific Economic Cross-Border Privacy Rules, and GDPR. Moreover, Workday is certified with global security and privacy standards such as ISO 27001, ISO 27017, ISO 27018, and ISO 27701. Current and prospective customers can find more

information on Workday's Global Privacy, including datasheets for Canada & the US, APJ and EU & UK, by visiting Trusting Workday with Your Data. We equip our customers' compliance and legal teams with a wealth of resources through the Workday Community portal, assisting them in meeting their privacy and compliance needs.

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