Workday's Robust Privacy Program

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 delivers human capital management, financial management, and analytics applications to the world's largest organizations. Over one thousand companies, ranging from medium-sized businesses to Fortune 50 enterprises, have selected Workday.

Protecting the privacy of our customers' personal data is one of our highest priorities, and it is integral to the success of our business. Data privacy regulations are very complex, and businesses have to select a Software-as-a-Service provider that understands how to appropriately protect the privacy of their data. This paper spells out Workday's approach to global data protection and highlights some of the regulatory requirements regarding personal data in various jurisdictions.

Customers and prospective customers may have privacy concerns about the personal data that Workday processes. We want to help them understand our privacy practices so that they can determine whether our services satisfy their specific regulatory and compliance needs.

We are dedicated to fostering our customers' confidence in our services.

Data Privacy and Personal Data

In this document, "privacy program" refers to the way Workday manages and safeguards the collection, transfer, 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 its customers must comply with various international privacy regulations. These are the common privacy principles in most jurisdictions:

- **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.

These privacy principles fall into two categories.

1. The first set of principles applies to Workday customers and their data subjects. Specifically, where required, Workday's customers are responsible for providing notice, access, and choice to individuals whose data is collected and used within the Workday application. Workday's application is 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. The second set of principles, including restrictions on the use and disclosure of data, apply to Workday in its role as the data processor. Workday maintains a comprehensive, written information-security program that contains technical and organizational safeguards designed to prevent unauthorized access to and use or disclosure of customer data. We provide transparency into the geographical regions where your data is stored and processed. All of these are set forth in our standard Data Protection Agreement (DPA). The DPA supplements the Master Subscription Agreement and formalizes the terms and conditions applicable to the processing by Workday of a customer and its affiliates personal data. The DPA describes our practices as it relates to access, processing, transfer, and storage of customer data. The DPA contractually obligates Workday to serve as a data processor, and only processes customer data on behalf of and as instructed by our Customers, and only to the extent necessary to provide the Workday Service. In effect, the DPA satisfies multiple country-specific requirements regarding data processing.

For customers that will transfer data across multiple jurisdictions, please request our DPA by emailing legal@workday.com.

Workday's Privacy Program

Workday has established and integrated a holistic privacy program that is embedded into our services. This program is built upon our philosophy of "privacy by design," which guides how we build products and operate our services. Our Privacy, Ethics, and Compliance team, led by Workday's Chief Privacy Officer, manages the privacy program and monitors its effectiveness. The team is responsible for:

- Formulating, maintaining, and updating Workday's internal privacy policies, procedures and tools to protect the privacy of our 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 founded its privacy program on strict policies and procedures regarding access, use, disclosure, and transfer of customer data by Workday. 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 data. In other words, the customer chooses who can access, use, and disclose their data.

Additionally, to comply with our policies and agreements, 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 Privacy, Ethics, and Compliance team evaluates 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 Council, in relevant business processes to further safeguard the privacy of personal data.

Certifications and Audits

Aside from developing and implementing 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 pre-defined 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. 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 to production systems are operating effectively.

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 and security practices and the operating effectiveness of controls associated to any Workday system that contains Customer Data. Consistent with the SOC 1 report, the SOC 2 controls are evaluated by an independent third-party auditor according to industry standards.

Global Privacy Efforts

EU DATA PRIVACY

The European Union adopted a comprehensive directive on data protection, which sets forth guidelines that regulate the collection, use, and transfer of personal data. The EU Data Protection Directive permits data transfers of personal data from the European Economic Area (EEA) to other countries only when a country is deemed to provide an adequate level of protection.

The United States is not identified by the European Commission as a country with an adequate level of protection. However, the European Commission permits the transfer of data to organizations in the United States that certify to the U.S.-EU Safe Harbor privacy framework..

Workday self-certified to the Safe Harbor privacy framework in 2007 and has re-certified to the program every year thereafter. This framework allowed U.S. companies that commit to the Safe Harbor Privacy Principles to meet the "adequacy" standard for privacy protection established by the European Commission, and import data from the European Economic Area (EEA). Workday's Safe Harbor certification covers the transfer of Customer Data, EU personal data that is used for marketing purposes, employee data, as well as professional services data from the EEA and Switzerland.

Despite the recent decision by the European Court of Justice to invalidate the Safe Harbor program, Workday continues to annually self-certify to the Safe Harbor framework. To address the adequacy requirement for customers with operations in the EU, Workday has incorporated the European Commission's approved standard contractual clauses, also referred to as the "Model Contract," into our Data Protection Agreement. The Model Contract is another method of meeting the adequacy requirement.

The EU Data Protection Directive also requires that the data controller (the customer) and the data processor (Workday) enter into a written contract documenting that the data processor has appropriate technical and organizational measures in place to protect personal data against threats that include unauthorized access, disclosure, use and processing of personal data, or unlawful forms of processing. This requirement is fulfilled through the signing of Workday's DPA.

CANADA DATA PRIVACY

Similar to the EU Data Protection Directive, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the collection, use, disclosure, and processing of personal data in the public sector. In addition, PIPEDA regulates the handling of personal data in the Canadian private sector unless there's an equivalent provincial law. However, unlike the EU Data Protection Directive, PIPEDA does not prohibit or restrict cross-border data transfers. Canadian businesses must take steps to safeguard personal data. In particular, when sharing personal data with third-party processors, an organization must use contractual or other means to provide a comparable level of protection as it would provide if it were processing the personal data itself. This requirement is met through Workday's DPA.

ASIA-PACIFIC AND LATIN AMERICA DATA PRIVACY

Workday and its customers need to address data privacy in the Asia Pacific and Latin American regions a bit differently from other regions. Unlike the EU's common institutions and legal instruments addressing data privacy matters (EU Data Protection Directive, European Data Protection Supervisory, Art. 29 Working Party, etc.), there are limited equivalent instruments and institutions with jurisdiction over a similar group of countries in the Asia Pacific or Latin American regions. Despite the lack of a central data privacy governing body, many countries in these regions turn to the existing data privacy standards that have been successfully established by previous regulations, including the EU Data Protection Directive. Many countries like Australia, Japan, China, Colombia, South Korea, Nicaragua, and Singapore have their own data privacy laws and guidelines in place.

We expect other countries to enact data privacy regulations over time as existing requirements evolve. Workday is committed to monitoring these changing data-protection requirements for their applicability to Workday and keeping our agreements and processes up to date with privacy laws in jurisdictions where our customers and we operate. Our DPA demonstrates that we have appropriate controls in place to process our customers' data. We have helped many customers respond successfully to questionnaires and audits from data- privacy regulators in the APAC region, including China, Hong Kong, Singapore, Malaysia, Korea, and others.

U.S. GOVERNMENT ACCESS TO CUSTOMER DATA

Workday's current and prospective customers are sometimes concerned about the U.S. government gaining access to their data in the Workday applications. One cause for this concern is the Patriot Act, enacted in October 2001 after the September 11, 2001 terrorist attacks. However, we believe that government interest in the type of data that Workday maintains is unlikely because intelligence agencies focus on national security. Further, known access requests from government agencies, including the National Security Agency through programs like PRISM, have typically focused on consumer Internet companies processing email, web searches, or web browsers.

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 that 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 the customer of these requests.

Conclusion

Workday's certifications and growing list of customers is a testament to our robust privacy program. This white paper informs current and prospective customers about our commitment to safeguarding the privacy of our customers' data, and highlights the details of our privacy program. If you would like additional information regarding our privacy program, we are happy to provide that.

Disclaimer

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

workday.

Workday, Inc. | 6230 Stoneridge Mall Road | Pleasanton, CA 94588 | United States
1.925.951.9000 | 1.877.WORKDAY (1.877.967.5329) | Fax: 1.925.951.9001 | www.workday.com