



## Canada and United States Privacy Overview

# Overview of 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. Below we highlight some of the key privacy and security considerations in the Americas that our customers are subject to while explaining how our privacy and security practices satisfy those needs.

## United States

As of July 2023, there is no Federal privacy law in the United States but Workday is a strong supporter of federal legislation. Currently, privacy requirements within the U.S. are uniquely comprised of a "patchwork" system centered on state consumer privacy laws in addition to certain sector-specific legal regimes.

### *U.S. State Laws*

More than 10 states have passed or enacted consumer privacy laws and that number continues to grow. While California's privacy law, the California Privacy Rights Act (CPRA) is the most stringent, generally, the state laws create certain rights for consumers, including allowing consumers to access and correct their data, providing consumers with the opportunity to request companies to delete their data, and granting consumers the right to opt-out of the sale of their personal information. Certain types of sensitive personal information--like an individual's Social Security number, driver's license information, or passport information--must be treated with special protections.

Importantly, under California law, all business-to-business (B2B) and HR contacts (for example, a company's employees, vendors and contractors) must be able to exercise the full set of "consumer" rights afforded to them.

In addition to consumer rights, the state laws generally establish obligations for businesses to follow, including: (i) privacy notice requirements, (ii) training and recordkeeping requirements, (iii) and contractual obligations with service providers, contractors, and third-parties.

Workday has implemented policies and procedures that comply with state laws, including CPRA. Workday's data protection and security standards regularly pass rigorous third-party compliance audits for security, confidentiality, availability, processing integrity and privacy controls. Privacy by Design is deeply enshrined in the Workday Service. Importantly, all new major feature releases related to the Workday Service are approved by Workday's Chief Privacy Officer. We include contractual mechanisms like Workday's Master Subscription Agreement ("MSA"), and Universal Data Processing Exhibit ("DPE"), which harmonizes the data processing terms across our various offerings and provides our customers a robust set of terms designed to satisfy the main contractual requirements under various state laws and help enable customers' regulatory compliance.

To best serve our customers, Workday provides resources on established and emerging state privacy laws. For example, to support customers' needs based on the latest requirements under the CPRA, Workday now offers a *California Privacy Amendment (CPA)* that addresses each of the CPRA's latest requirements for service provider contracts. Customers can access a complete FAQ and a link to the pre-signed CPA through their access to Workday Community.

### *U.S. Sectoral Laws*

Depending on what kind of data a company handles, it may be subject to certain other federal sectoral laws within the U.S. For example, the Health Insurance Portability and Accounting Act (HIPAA) protects the collection of health information and medical records of employees. Among other requirements, HIPAA deems cloud services providers (CSPs) to be Business Associates, as defined under HIPAA. In our role as a CSP, Workday has a standard Business Associate agreement that we make available to customers who plan to leverage Workday to capture, transmit, or store protected health information.

## Canada

Within Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to organizations that conduct commercial activities. PIPEDA generally regulates the handling of personal data in the Canadian private sector and sets out ten privacy-related principles to which organizations must adhere in order to safeguard personal data. Workday addresses PIPEDA requirements in its suite of privacy and security protections, including through contractual mechanisms like Workday's MSA and DPE.

PIPEDA institutes several business compliance requirements that our customers are often subject to. PIPEDA requires companies to institute certain physical protection measures, organizational measures, and technological measures. Workday has implemented appropriate organizational security, architectural security, and operational security measures.

PIPEDA also lays out requirements for third party processing, including requirements for third parties to adhere to applicable privacy legislation, to use or process the information only as instructed by the transferring organization and to return or securely destroy it on the termination of the agreement, and maintain adequate safeguards. To satisfy these third party processing requirements, Workday has a comprehensive process that includes contractual mechanisms, like Workday's DPE.

Many of Workday's customers have international data transfer obligations, however, PIPEDA does not prohibit cross-border personal information transfers, nor does PIPEDA distinguish between domestic and international transfers. Workday has well-developed processes that provide strong protection when there is a cross-border transfer of personal data, including Workday's Processor Binding Corporate Rules (BCRs) and a dedication to privacy hygiene (for example, by performing privacy impact assessments).

## Workday's Commitment to Privacy and Security

Workday stridently maintains an up-to-date suite of privacy protections designed to comply with complex 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 compliance with data protection laws and that facilitate cross-border data transfers, Workday forges ahead as an industry-leader in privacy. Also, Workday's highly configurable systems help enable our customers to meet the varying requirements of data protection laws.

Additionally, Workday also maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats or data breaches, and prevent unauthorized access to our customers' data. The specifics of our security program are detailed in our third-party security audits and international certifications, including up-to-date SOC, ISO, and NIST certifications alongside other specialized attestations including HIPAA and PCI-DSS attestations (further detailed on [Workday's Trust Site](#)), which we make available to customers to help facilitate compliance with their data protection processes and obligations.

For more information, we invite all to read about Workday's Privacy Program (including datasheets for APJ and EU & UK) and Workday's compliance, and security commitments on [Workday's Trust site](#)

## 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](http://www.workday.com)

© 2023 Workday, Inc. All rights reserved. WORKDAY and the Workday logos are trademarks of Workday, Inc. registered in the United States and elsewhere. All other brand and product names are trademarks of their respective holders.