Asia, Pacific, and Japan Privacy Overview

Overview of Privacy Landscape

Introduction

As a leading provider of enterprise cloud applications for human resources, financial management, and planning, Workday takes its privacy and security responsibilities seriously. 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 has proven itself to be a trailblazer in this area, being one of the first companies to be certified to the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) and Privacy Rules for Processors (APEC PRP). The APEC certifications are a voluntary set of privacy standards developed for data controllers and processors, respectively, to facilitate data transfers among APEC economies. These certifications demonstrate compliance with rigorous privacy standards throughout this region.

By combining Workday's unique ability to attain global recognition by reputable certification bodies (for example, the third-party certification from TRUSTe, which is the APEC Accountability Agent for the United States) with our track record of a strong commitment to privacy and security, Workday demonstrates its strong position on data protection. Below, we highlight some key privacy and security considerations that our customers are subject to while explaining how our privacy and security practices satisfy those needs.

Broad Overview of Asia, Pacific, and Japan

Most jurisdictions are governed by general personal data protection regimes that set out certain individual rights and business requirements, including Australia, China, Japan, Singapore, South Korea and Thailand. Often echoing the General Data Protection Regulation (GDPR), national personal data protection laws generally grant fundamental rights to individual data subjects as they pertain to personal data, while simultaneously setting out business obligations to follow, including contractual requirements for handling personal data, third party processing requirements, security obligations, appointments of data protection officers, and cross-border transfer requirements. Workday confidently asserts its commitment to global data privacy and security compliance, and details some of the critical concerns for businesses across the region. We have helped many customers respond successfully to questionnaires and audits from data privacy regulators in the Asia-Pacific region, including China, Hong Kong, Singapore, Malaysia, Korea, and others.

Third Party Processing

Third party processing requirements across the APJ region reflect a wide range of disparate requirements. Certain national data protection laws (for example, Australia's Privacy Act) do not mention data processors, whereas other nations (for example, Japan's Act on the Protection of Personal Information (APPI) or Singapore's Personal Data Protection Act (PDPA)) lay out specific requirements for processors, intermediaries, or other third parties. In one notable deviation, South Korea's Personal Information Protection Act differentiates between "outsourcing" and "transferring" personal data, and assigns various obligations based on that distinction. Workday recognizes the complexities relating to a third party processing personal data, and our Master Subscription Agreement ("MSA") includes a Universal Data Processing Exhibit ("DPE") that demonstrates we have appropriate controls in place to process our customers' data in compliance with data processing requirements. We have helped many customers respond successfully to questionnaires and audits regarding our role as a cloud service provider throughout the region, and we regularly reassess our suite of privacy and security protections.

Cross-Border Data Transfers

Nations often place significant restrictions on the transmission of personal information from one jurisdiction to another, often creating complex problems for businesses. Workday, however, is constantly identifying innovative ways to help our customers comply with cross-border data transfer requirements, and this is especially true in the Asia, Pacific, and Japan region. Many of the APJ countries--including Australia, Japan, South Korea, and Singapore--are participants in the APEC CBPR System. As indicated above, CBPR is a government-backed data privacy certification that companies can join to demonstrate compliance with

internationally-recognized data privacy protections. As one of the first companies to be certified to APEC CBPR, Workday demonstrates it is an industry leader, committed to facilitating our customers' compliance with cross-border data transfer requirements, and to privacy and security of personal data in this region. Further, Workday continues to monitor cross-border transfer approvals and developments, including assessing potential technical solutions.

China

China's Personal Information Protection Law ('PIPL') establishes personal information processing rules, data subject rights, and obligations for personal information processors. Under PIPL, there is a consent requirement for sharing and disclosure of personal information, which is subject to a series of limited exceptions. PIPL also contains third party processing agreement requirements for agreements with "entrusted parties," including consent requirements to use subprocessors, and a requirement for a data processing agreement covering the (i) purpose, (ii) period, and (iii) method of the entrusted processing, (iv) the type of personal information to be processed, (v) any protection measures to be taken, and (vi) the rights and obligations of both parties. Workday's current MSA and DPE have been designed to satisfy the main contractual requirements between personal information handlers (i.e. customers) and entrusted parties (i.e. Workday). Perhaps most different from other privacy regimes, the PIPL enables processing entities to export personal information out of mainland China, though with some restrictions. These restrictions are similar to those in the EU's GDPR, which requires a valid transfer mechanism to transfer personal data from the EU to non adequate jurisdictions. A similar concept exists within the PIPL. Namely, personal information may not be exported out of mainland China unless an organization uses one of 3 transfer mechanisms, as determined by your company:

1. Certification: Obtain a certification by Chinese-approved organization in accordance with regulations
2. SCCs: Execution of agreement between our customer and their entity in China based on standard contract stipulated by the regulator.
3. Security Assessment: Successful completion and review by the government of a service-specific security assessment.

Because of these and other requirements, it is more crucial than ever for companies to ensure that personal data in their possession is adequately protected, and Workday has strived to ensure its protections satisfy applicable PIPL requirements. To support our customers who must complete a security assessment conducted by CAC, Workday has made available a detailed questionnaire containing common questions and answers customers can leverage when completing their own security assessment documentation. In addition, Workday has also published a PIPL white paper, available on Privacy: Transparency and Trust (workday.com), which provides further details about Workday's approach to the PIPL. Workday Customers can also find a detailed PIPL FAQ on Workday Community.

Thailand

Thailand's Personal Data Protection Act ("PDPA") is the country's first comprehensive privacy law and provides substantial protection to personal data of Thai-based individuals. The PDPA's requirements reflect a blend of requirements familiar to several privacy laws across the region. The law also borrows heavily from the GDPR, but with a stronger emphasis on data subject consent as the legal basis for processing.

The PDPA applies to most organizations that conduct business or target individuals located within Thailand. Workday customers subject to the law are controllers. Workday itself is a processor of the personal data submitted by its controller-customers.

The PDPA doesn't forbid the transfer or processing of personal information outside of Thailand, so long as the destination country or international organization receiving the data has an adequate level of data protection and one of these circumstances applies:

1. Where the transfer is for compliance with a law;
2. Where the data subject has consented to the transfer;
3. Where it's necessary for the performance of a contract to which the data subject is a party; or,
4. Where it's for compliance with a contract between the data controller and the processor for the interests of the data subject.

Customers should consult their own legal experts to determine the basis for international transfers. Most customers will likely either obtain consent from their employees or rely upon the fourth basis as their rationale for transfers.

Workday provides robust features and functionalities that can help customers meet their obligations regarding individual rights.The PDPA requires that controllers and their relevant processors enter into a contract committing the parties to

specific obligations that are included by default in Workday's DPE. Workday has assisted customers with their obligations under other privacy laws, such as the EU's GDPR, for years. We expect that those same features and functionality will be well suited to address the PDPA's requirements.

Workday's Commitment to Privacy and Security

Workday stridently maintains an up-to-date suite of privacy protections designed to comply with global privacy regulations, including those in the Asia, Pacific, and Japan region. 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 and data protection. Our DPE, which provides strong contractual obligations, and our comprehensive security and compliance programs--consisting of 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. In addition, Workday's highly configurable systems help enable our customers to meet the varying requirements of global data protection laws.

Workday 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. Please visit workday.com/trust for more information on Workday's Privacy Program (including regional datasheets for Canada & the US and EU & UK), compliance and security.

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