Response to the National Institute of Standards and Technology's Request for Information on Developing the Privacy Framework: An Enterprise Risk Management Tool

Docket No. 181101997-8997-01
January 14, 2019

I. Introduction

Workday is pleased to have the opportunity to provide information in response to the National Institute of Standards and Technology's (NIST) request for information to help guide the development of the NIST Privacy Framework: An Enterprise Management Tool.

Workday is a leading provider of enterprise cloud applications for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, and analytics applications designed for the private sector, educational institutions, and government agencies. Our cloud-based applications empower enterprises to process a wide variety of human resources and finance-related transactions, gain new insights into their workforce and financial performance, and manage employee financial outcomes consistently on a companywide basis. At Workday, privacy protections have been a fundamental component of our services from the very beginning.

II. Comments on Process

Workday appreciates NIST's efforts to develop a voluntary framework to address privacy. In addition to these comments, we were pleased to support the process by attending the kickoff workshop in Austin, Texas in October of last year and watched with interest the Privacy Framework Q&A Webinar in November. Workday has similarly participated in the National Telecommunications and Information Administration's parallel effort to develop the Administration's approach to consumer privacy.

Events within the tech sectors, actions taken by both foreign governments and state lawmakers, and considerable interest on Capitol Hill have galvanized attention on the issue of digital privacy. Workday is forward leaning in our belief that comprehensive privacy legislation consistent with the Organization for Economic Cooperation and Development (OECD) Fair Information Principles is necessary. While the path forward for reforms to U.S. digital privacy policy are unknown, processes like the one undertaken by NIST are extremely helpful. First and foremost, the development of a voluntary framework akin to the work the Institute has done with respect to cybersecurity has the potential for widespread adoption and an overall increase the level of assurance of the safety of digital information. In addition, the focused attention and consideration of related issues in the development of the privacy framework through a voluntary and consensus-based approach will have benefits for the ongoing discussion of digital privacy best practices writ large.

Workday encourages NIST to continue with the valuable effort and provides the following responses to selected queries raised in the request for information.

III. Responses to Specific Queries

A. Risk Management

The request for information seeks information related to "the current usage of existing privacy standards, frameworks, models, methodologies, tools, guidelines, and principle." Workday achieves compliance with international privacy regulations by maintaining 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 are pleased to provide selected details of our privacy efforts below.

1. SOC Reports

The operations, policies, and procedures at Workday are audited regularly to ensure that Workday meets and exceeds all standards expected of service providers. Workday publishes a Service Organization Controls 1 (SOC 1) Type II report. The SOC 1, which is the successor to the SAS 70, is issued in accordance with the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402).

Workday also publishes a Service Organization Controls 2 (SOC 2) Type II report. The Workday SOC 2 report addresses all trust services principles and criteria (security, availability, confidentiality, processing integrity, and privacy). The scope of the SOC 2 covers any Workday system that contains data that the customer submitted to Workday Services. The intended audience for this report is a customer or prospect who is interested in understanding Workday internal security controls. The SOC 2 audit is conducted once a year by an independent third-party auditor and is available to customers or prospects upon completion.

Both the SOC 1 and the SOC 2 audits validate Workday physical and environmental safeguards for production data centers, backup and recovery procedures, software development processes, and logical security controls.

2. ISO Standards

ISO 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's Information Security Management System. Workday has been continually ISO 27001-certified since 2010, which affirms our commitment to security. We also certify to:

- ISO 27017 which provides controls and implementation guidance for information security controls applicable to the provision and use of cloud services. Workday has been ISO 27017-certified since 2017, and
- ISO 27018 which contains guidelines applicable to cloud service providers that process personal data. Workday has been continually ISO 27018-certified since 2015 and is proud to have been the first in our industry to achieve this certification.

These ISO certifications affirm our commitment to privacy and security and demonstrate that our controls are operating effectively.

3. *GDPR Compliance and BCRs*

Workday has comprehensively evaluated General Data Protection Regulation (GDPR) requirements and implemented numerous privacy and security practices to ensure compliance with the GDPR from day one. These include:

- Training employees on security and privacy practices,
- Conducting Privacy Impact Assessments,
- Providing adequate data transfer methods to our customers,
- Maintaining records of processing activities, and
- Providing configurable privacy and compliance features to our customers.

Privacy by Design and Privacy by Default are concepts deeply enshrined in the Workday Service and Workday continues to monitor guidance that European Union (EU) supervisory authorities issue on the GDPR to ensure that our compliance program remains up-to-date.

Workday has also obtained approval from EU data protection authorities for global Binding Corporate Rules for Processors (BCRs) that focus on safeguarding customer data. The Irish Data Protection Commissioner conducted the review, with peer review by both the UK Information Commissioner's Office (ICO) and the Dutch Data Protection Authority (DPA).

As part of the approval process, the data protection authorities conducted a thorough review of our data privacy program, including our internal training programs, policies and procedures, and technical and organizational controls. This approval demonstrates that Workday has implemented a consistent set of robust privacy practices for processing personal data across our global Workday affiliates.

4. *Standard Contractual Clauses*

European data protection laws regulate the transfer of personal data outside the European Economic Area (EEA), e.g. to the United States. To help its European customers legalize cross-border data transfers and meet the "adequacy" requirements for European personal data, Workday's customers may choose to leverage the European Commission's Standard Contractual Clauses for the transfer of personal data to processors established in third countries pursuant to Commission Decision (2010/87/EU), also referred to as the "Model Clauses."

5. *Privacy Shield Certification*

In 2016, Workday, Inc. self-certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks on the first day the U.S. Department of Commerce launched the Privacy Shield certification process, demonstrating our strong, ongoing commitment to privacy and protecting our customers' data. The Privacy Shield is a data transfer framework to allow personal data transfers between the EU and the U.S., as well as between Switzerland and the U.S. Four key principles are emphasized in the Privacy Shield:

- Clear safeguards and transparency obligations on U.S. government access,

- Strong obligations on companies handling data,
- Effective protection of individual rights, including redress options for EU citizens, and
- An annual joint review by the European Commission and the U.S. Department of Commerce.

While companies can self-certify to the Privacy Shield, Workday uses TrustArc as our third-party verification method. In addition, Workday continues to have third parties review our data privacy program regularly to ensure that our customers enjoy the highest possible levels of data protection and privacy.

6. APEC CBPR & PRP

Workday is also compliant with the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR). The APEC CBPR is a voluntary set of privacy standards developed to facilitate data transfers among APEC economies and demonstrates compliance with high standards of privacy compliance throughout the Asia-Pacific region.

Workday was one of the first companies to join the APEC CBPR system and has received a third-party attestation from TrustArc, who is the APEC CBPR Accountability Agent for the United States. Our current APEC CBPR certification applies to our role as a data collector. By maintaining compliance with the APEC CBPR and privacy requirements in the EEA, Workday is able to globally demonstrate an adherence to robust privacy frameworks.

Workday is also the first company to be certified by TrustArc to the APEC Privacy Recognition for Processors (PRP) System. This certification further demonstrates Workday's strong privacy protections for customer data, and our commitment to accountability in our global privacy program.

The PRP System implements the nine privacy principles set forth in the APEC Privacy Framework and is intended to strengthen privacy protections and trust across the Asia-Pacific region. In addition, the certification aims to minimize barriers to the cross-border flow of information.

To obtain PRP certification, Workday completed a comprehensive review with TrustArc and with the Federal Trade Commission as the enforcement authority. As part of this review, Workday confirmed that our data privacy policies and practices comply with the PRP System's accountability standards for data protection. We also demonstrated to TrustArc the strong data governance measures we have in place for protecting our customers' personal data.

7. Additional Efforts

Workday supports PCI DSS compliance within the scope of the Workday Secure Credit Card Environment, which is an isolated environment that stores, processes, and transmits unmasked cardholder data through predefined integrations.

Workday has also completed a Health Insurance Portability and Accountability Act (HIPAA) third-party attestation for Workday enterprise cloud applications, which provides assurance that Workday has a HIPAA-compliance program with adequate measures for saving, accessing, and sharing individual medical and personal information.

B. Organizational Considerations

The request for information seeks suggestions on the minimum set of attributes and describes a number of specific potential attributes under consideration and derived from previous stakeholder engagement. Among those potential attribute is the concept of compatibility, including the suggestion that the framework should "should be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regime."

Workday supports this concept. That utilization of the voluntary tool NIST seeks to develop will likely be expanded if redundancy is kept at a minimum and the tool assistances in complying with adoption of existing statutory and regulatory requirements.

C. Structuring the Privacy Framework

With respect to structuring the framework, the request for information seeks suggestions on the preferred organizational construct, including specifically whether the framework should be structured around the fair information practice principles (FIPPS).

As mentioned, Workday believes that privacy rights must be protected through strong legislation and enforcement that ensures ethical use of individuals' information. Along those lines, we have publicly called for strong and comprehensive federal privacy legislation. In our view, the U.S. and other countries around the world should adopt privacy laws based on the OECD Fair Information Principles. A law based on the OECD principles will ensure fair treatment of individuals and their personal information, regardless of where they live or with whom they interact. The OECD principles provide a widely-shared common baseline for the 35 countries that are OECD members. The voluntary OECD principles cover all the core tenets of data privacy rights—data collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. Enacting these principles in U.S. national legislation should result in U.S. law being deemed adequate by the EU and will facilitate the continued free flow of personal data.

Similarly, we would suggest for consideration NIST specifically using the OECD principles as the organizational structure around which to build the voluntary framework. Doctrinally, the FIPPS provided the basis for the OECD principles. In additional, however, the OECD principles have the benefit of a global footprint which would suggest, if used as the basis of the privacy tool, a heightened level of potential synchronicity with global digital privacy protection efforts.

IV. Conclusion

Thank you for the opportunity to provide input in response to the request for information to help guide the development of the NIST Privacy Framework. At Workday, privacy protections have been a fundamental component of Workday's services from our very beginning and we appreciate the attention to the issue. As privacy is a fundamental value around the globe as well as in the U.S., it is incumbent on the U.S. to lead in protecting the privacy of its citizens. NIST's efforts are contributing to that goal. We stand ready to provide further information and to answer any questions. Please do not hesitate to reach out to Chandler C. Morse at chandler.morse@workday.com for further assistance.