From: Chandler C. Morse <chandler.morse@workday.com>
Sent: Thursday, October 24, 2019 7:38 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

To whom it may concern,

Please find attached Workday's comments on the NIST Privacy Framework preliminary draft. We are pleased to have the opportunity to provide feedback and look forward to continued involvement in the process.

Sincerely,

Chandler

Chandler C. Morse
U.S. Public Policy Director
+1 703-639-3511
chandler.morse@workday.com

Image removed by sender.

Image removed by sender.

Thank you for considering the environment.

Response to NIST’s Request for Comment on the Preliminary Draft Privacy Framework

October 24, 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 comments on the *Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (“Preliminary Draft”).

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. Support for the Framework Development Process

Workday appreciates NIST’s efforts to develop a voluntary framework to address privacy. 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. In addition to the comments below, we submitted comments to the January 2019 Request for Information in which we detailed our privacy program; including highlighting our Service Organization Controls (SOC) I and SOC II reports, ISO standard certifications, General Data Protection Regulation (GDPR) compliance and Binding Corporate Rules, standard contractual clauses, Privacy Shield certification, and Asia-Pacific Economic Cooperation Cross-Border Privacy Rules and Privacy Recognition for Processors System certification. Most recently, we provided joint feedback with Okta on the previously released framework Discussion Draft urging inclusion of language that clearly delineates between data controllers and data processors. We are pleased to provide the following general and specific comments.

III. General Comments

A. Identification of Roles and Responsibilities

As outlined in the Preliminary Draft, unprecedented innovation in the use of the Internet and associated information technologies has fostered the flow of data about individuals through complex ecosystems. The Framework indicates that the role of those entities involved in the Data Processing Ecosystems “may be legally codified—for example, some laws classify organizations as data controllers or data processors—or classifications may be derived from industry sector designations.” Emerging privacy laws and standards do indeed seek to define the roles of those entities involved in the Data Processing Ecosystems in similar fashions.

For example, ISO 27701 requirements and responsibilities are mapped on the basis of Data Controller responsibilities and Data Processor responsibilities. This approach does not prevent organizations from becoming compliant as both Data Controller and Data Processor, but it does recognize the different types of relationships that are possible between the individual and those entities consuming the personal identifiable information.

In addition, the California Consumer Protection Act (CCPA) attaches compliance obligations to different types of entities, including businesses and service providers. "Businesses" are defined as a for-profit entity that determines the "purposes and means of the processing of ... personal information" similar to that of the controller. "Service Providers" are defined as a for-profit entity that processes personal information "on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract ...." Under the CCPA, this written contract must prohibit the service provider from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business.

Lastly, GDPR defines a Data Controller as the entity who determines the purposes and means of processing personal data. Similarly, the Data Processor is defined as the entity who process personal data on the instructions of the Data Controller. The EU Cloud Code of Conduct, in seeking to comply with the GDPR, defines the Cloud Service Provider (CSP) as a Data Processor and the Customer as the Data Controller.

B. Inclusion of Controller-Processor Distinction

We believe it would add value to the Preliminary Draft to expressly recognize the role of data controllers and data processors. This would allow entities to better align the framework's approach with their existing roles and responsibilities. As indicated, the suggestion to include references to data controller and data processor reflects the inclusion of these and other related terms in statute and regulation with which entities already comply. Without clarification of entity roles, it would be unnecessarily difficult for entities to tie the NIST privacy framework requirements to a range of different regulatory and legal requirements.

We recognize the desire of NIST to produce a framework that is agnostic with respect to individual laws and regulations and the resistance to adopting terminology specific to any one jurisdiction. In addition, however, NIST's goal is also to produce a framework that meets with widespread adoption with all its attendant benefits. While it may appear that these two goals are in tension, they are not. Rather than individual laws or specific jurisdictions, the controller-processor distinction has been widely adopted in both the U.S. and globally, and we believe it's inclusion will facilitate the adoption of the framework.

IV. Specific Comments

A. Controller-Processor Related Clarifications

In our review of the Preliminary Draft, we have identified a number of key areas where the absence of clarity around the roles of the entities involved in the Data Processing Ecosystem could make it difficult to rationalize and map the framework to other regulatory and legal requirements, such as those outlined above. The areas include:

- *The Executive Summary (p.3, line 100)*
  The Executive Summary states "[t]he Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises…" We suggest adding language highlighting the differing relationships between different kinds of enterprises and the individual by adding "and responsibilities" after "privacy needs."
- *1.0 Privacy Framework Introduction (p. 4, line 135)*
  The introduction states "[w]hat has been missing is a common language and practical tool that is flexible enough to address diverse privacy needs." We recommend adding specific language addressing the difference between data controllers and data processors by inserting "support the various roles and responsibilities of the parties involved (both different enterprises and individuals and" before "address diverse privacy needs."
- *1.0 Privacy Framework Introduction (p. 4, line 145)*
  The introduction includes the line "[t]he Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction" and continues with a series of bullets describing aspects of organizations. We believe NIST can maintain this agnosticism while including the following clarifying bullet "• Different organizations may take responsibility for different outcomes and activities depending on their roles and obligations to the individual."
- *2.0 Privacy Framework Basics (p. 9, line 304)*
  This section states "[d]ifferent types of entities—including sector-specific organizations—can use the Privacy Framework for different purposes, including the creation of common Profiles." We would suggest expanding on the entity differences with a reference such as "performing different roles in the collection and processing of data" following "entities."
- *3.5 Using within the Data Processing Ecosystem (p. 16, line 569)*
  The framework, in discussing relationships within the Data Processing Ecosystem, suggests that "[a]n organization should use the Privacy Framework from its standpoint in the data processing ecosystem and consider how to manage privacy risk not only with regard to its internal priorities, but also in relation to how they affect other parties' management of privacy risk." We would recommend that NIST add extensive implementation guidance detailing which roles and responsibilities can be universal in nature or exclusive to specific types of entities such as data controllers or data processors. Without such guidance, in an attempt to cover all bases, organizations may be stretched to the point of there being little practical value in the implementation of the framework.
- *Data Management Policies, Processes, and Procedures (CT.PO-P) (p. 24)*
  The Privacy Framework Core table recommends that "[p]olicies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles, responsibilities, management commitment, and, coordination among organizational entities) consistent with the organization's risk strategy to protect individuals' privacy" and suggests a number of specific policy areas. We would propose this section would benefit from clarifying the applicability of the data management responsibilities based on the type of entity (i.e., data controllers and data processors).
- *Communication Policies, Processes, and Procedures (CM.PP-P) (p. 24)*
  The Core also suggests that "[p]olicies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities) and associated privacy risks." We encourage NIST to clarify the type of entity (i.e., data controllers or data processors) to which these responsibilities would apply.

- *Appendix B: Glossary (p. 29)*
  The Glossary defines Data Processing Ecosystem as “[t]he complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.” We believe this definition should reflect some recognition of the types of entities, such as data controllers and data processors, that are contemplated in various statutory and regulatory approaches.
- *Appendix E: Implementation Tiers Definitions (p. 39, lines 870 and 889)*
  In two places, the Implementation Tiers Definitions references the “understanding of an organization’s role in the larger ecosystem with respect to other entities (e.g., buyers, suppliers, service providers, business associates, partners).” To reduce ambiguity, both the organization and the other entities should be defined by their responsibilities, such as data controllers and data processors and as contemplated in various regulatory and legal approaches. Without such context, all parties within the ecosystem will have little way of knowing what the Data Processing Ecosystem relationship entail and could influence the perception of assurances offered by the framework.

B. Implementation Guidance

In addition to the clarifications above, we have identified additionally areas that could benefit from considerations related to implementations, as described below:

- *3.1 Mapping to Informative References (p. 12, line 444)*
  The Privacy Framework is technology neutral, but it supports technological innovation because any organization or industry sector can map the outcome-based Subcategories in the Core to standards, guidelines, and practices…” We recommend that there be a significant amount of implementation guidance related to how this would work. Specifically, this guidance should include working through each subcategory and providing scenario-based examples like those used in ISO standards.
- *Appendix D: Privacy Risk Management Practices (p. 34, line 767)*
  The Preliminary Draft suggests a number of preparatory resources that “build a foundation for better decision-making,” including data maps (ID.IM-P). For reasons related to implementation, it would be helpful to ensure that the requirements involved in data mapping be closely linked to requirements in applicable privacy regulations such as GDPR. The current description appears to require extensive mapping and, as suggested above, this area of the framework would benefit from a definition of roles, such as controller and processor.

V. Conclusion

Thank you for the opportunity to provide both general and specific comments on the Preliminary Draft of NIST’s privacy framework. As we have raised previously, privacy protections have been a fundamental component of Workday’s services from our very beginning and we appreciate the attention to the issue. We congratulate NIST on the tremendous work put into crafting the framework thus far, including continued stakeholder involvement. We are committed to assisting NIST in developing a workable framework that will meet with widespread adoption. We stand ready to provide further information and to answer any additional questions. Please do not hesitate to reach out to Chandler C. Morse at chandler.morse@workday.com for further assistance.