Service Privacy Policy

Last Updated: December 27, 2019

This Privacy Statement covers the privacy practices Workday employs when Workday customers ("Customers") use our Cloud-Based Enterprise Applications (the "Service"), including our cloud-based planning management software ("Adaptive Insights"). This Privacy Statement does not cover any information or data collected by Workday for other purposes, such as information collected for marketing purposes. Please see: **workday.com/en-us/privacy.html**

How Workday Processes Information

Personal Data Workday Processes
In the normal course of using the Workday Service, Customers will input electronic data into the Workday systems ("Customer Data"). The use of information collected through the Service shall be limited to the purpose of providing the Service for which the Customer has engaged Workday. Workday may access Customer Data for the purposes of providing the applicable service, preventing or addressing service or technical problems, responding to support issues, and responding to Customer's instructions, or as may be required by law, in accordance with the relevant agreement between Customer and Workday.

Workday processes Customer Data under the direction of its Customers, and has no direct control or ownership of the personal data it processes. Customers are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the data to Workday for processing purposes.

An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to the Workday Customer (the data controller). If the Customer requests Workday to remove the personal data to comply with data protection regulations, Workday will respond to their request within 30 days.

Workday will refer any request for disclosure of personal data by a law enforcement authority to the Customer. Workday may, where it concludes that it is legally obligated to do so, disclose personal data to law enforcement or other government authorities. Workday will notify Customer of such request unless prohibited by law.

Accessing the Service
Customers and their authorized users may access the Service directly through a URL unique to their individual tenant, or may elect to use internal launch pages for single sign-on or other purposes. Customers input information for processing and storage as they use the Service. Customers may also configure the Service to allow end users to input information directly into the Service.

Global Privacy

EU-U.S. and Swiss-U.S. Privacy Shield Statement
Workday complies with both the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and the United Kingdom to the United States, and from Switzerland to the United States, respectively. Workday has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit **privacyshield.gov**.

View our EU-U.S. and Swiss-U.S. Privacy Shield Notice.

If you have an unresolved concern regarding EEA, UK or Swiss privacy or data use that we have not addressed satisfactorily, please contact the relevant EU data protection authority or the Swiss Federal Data Protection and Information Commissioner, as applicable. If you have a non-EEA and UK or non-Swiss privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge): **https://feedback-form.truste.com/watchdog/request**

Workday has also obtained the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) Certification to further demonstrate its ability to assist our customers in complying with their relevant privacy obligations.

Additional Workday Privacy Information

Data Retention
Workday retains Customer Data according to the timeframes set forth in the relevant agreement with its Customers.

Security
The security of Customer Data, including personal data, is very important to Workday. Workday maintains a comprehensive, written information security program that contains industry-standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Data. Workday designs its applications to allow Customers to achieve differentiated configurations, enforce user access controls, and manage data categories that may be populated and/or made accessible on a country-by-country basis. Configuring these settings appropriately is the Customer's responsibility. Additional information about the security settings and configurations can be found in the Workday Documentation made available to Customers.

Changes to This Privacy Statement
We reserve the right to change or update this Privacy Statement at any time. Changes to the Privacy Statement will be posted on this website and links to the Privacy Statement will indicate that the statement has been changed or updated. We encourage you to periodically review this Privacy Statement for any changes. For new Customers, changes or updates are effective upon posting. For existing Customers, changes or updates are effective 30 days after posting.

Compliance
Workday has appointed a chief privacy officer responsible for overseeing the implementation of the privacy program within the organization. If you have further questions related to this statement, please ask your Customer Support contact to log a customer care case with the privacy question.