Workiva

General Data Protection Regulation (GDPR) and Wdesk

Both Workiva and our customers have responsibilities when it comes to GDPR compliance. With respect to customer data uploaded into Wdesk, Workiva is the "data processor," and the party deciding which data to upload is the "data controller" in terms of the regulation.

In brief, the "controller" is the party that determines the purposes and means of processing the personal data, and the "processor" is the party that performs operations on personal data or on sets of personal data. "Performing Operations" may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

As your data processor, Workiva is available to answer your questions on GDPR and to assist in your demonstration of compliance as the data controller.

Wdesk as data processor

To demonstrate compliance, Workiva has taken several actions, including:

Security: Wdesk security was designed from the ground up, and regularly passes rigorous third-party compliance reviews for security, confidentiality, availability, processing integrity, and privacy controls. Specifically, Wdesk allows customers to manage and control their users' access to Wdesk applications and offers a standardized framework for defining role-based access.

Cross-border data flows: GDPR continues to allow the flow of personal data across country borders pursuant to several adequacy measures, including the EU-US Privacy Shield Framework and EU Model Clauses. Workiva has self-certified to the Privacy Shield Framework. In addition, Workiva will cooperate with requests to enter into either a Data Processing Agreement or the EU Model Clauses on customer request. Finally, Workiva offers customers a choice of storing data in select geographical locations in the United States or the European Union.

Privacy impact assessments (PIAs): The GDPR requires PIAs for certain types of personal data processing. Workiva conducts PIAs on features, technology, third-party on-boarding, and operations related to our service as required by GDPR. Although we do not anticipate any significant changes to our current process, Workiva continues to monitor the Article 29 working party's guidance regarding GDPR to ensure our PIAs fulfill any new requirements.

Security breaches: GDPR introduces new notification rules for any security breaches that lead to the loss, destruction, or unauthorized access of personal data. Workiva has formal incident response plans, breach notification processes, and other measures in place to respond to a security breach in a manner that satisfies GDPR, as well as other jurisdictional statutes' notification requirements.

Customers as data controller within Wdesk

In addition to our compliance obligations under GDPR as a processor of our customers' personal data, Workiva also assists customers in meeting their obligations under GDPR in a variety of ways, including:

PIA assistance: If a customer determines that the use of personal data in Wdesk rises to a level requiring the performance of a PIA, Workiva will provide documentation around its policies and processes, as well as answer customer-provided security and privacy questionnaires.

Permission system: Wdesk offers a robust permission system to help customers comply with access rights under GDPR. The Wdesk application allows customers to manage and control their users' access to Wdesk and offers a standardized framework for defining role-based access.

Activities and notifications: To enable customers to protect personal data against security threats, Wdesk logs all activity

in an account, and logs are kept within a customer's Wdesk account for review. These activities include successful and failed login attempts, as well as changes or additions to data through the robust Wdesk document history. Wdesk customer administrators can view sign-on/failed sign-on reports and subscribe to notifications of these activities. Further, customers can review data changes made by any user and even run a blackline for a data comparison—which allows customers to manage access control and monitoring, and provides compliance assurance.

Security reviews: Workiva also provides customers with reports on our controls and processes. Customers can reference and rely on the procedures performed by our independent auditors as part of the SOC 1 and SOC 2 reports to demonstrate the security aspects related to GDPR compliance. For additional information on our privacy practices, please reference our TRUSTe Certification and Privacy Policy.