

Privacy and Data Security at Deltek

Our commitment to customers

Keeping our customers' information safe and secure is a high priority for Deltek. Security and customer trust are fundamental components of our product development, daily operations, and business planning. We have implemented and continually maintain strong security and privacy protections that reflect industry best practices while also considering the impact of new and changing regional security and privacy regulations. Deltek's services are backed by technical and administrative safeguards and dedicated security, operational and privacy teams. Our products and services are reviewed by third-party auditors and we have processes in place to build security and privacy into our products from the early stages of development. Whether our customers are working in the United States government contracting space or doing business in the European Union, Deltek's suite of products are designed with security and privacy in mind from the early stages of development.

Deltek and the CCPA

The California Consumer Privacy Act (CCPA) goes into effect on January 1, 2020. The CCPA creates an array of new consumer privacy rights and governs the sale and sharing of consumers' personal information.

Deltek processes personal information through its products on behalf of its customers, some of whom may be subject to the CCPA. Pursuant to their business purpose, customers may disclose individuals' personal information in accordance with the terms of our written agreement. In the context of the CCPA, Deltek takes on the role of a service provider in relation to its customers who are governed by the CCPA. Deltek is well situated to meet its obligations as a service provider and is establishing processes to ensure the security and privacy features of its products provide the capabilities to enable customers to comply with their obligations under the CCPA.

Deltek and the GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, better known as the General Data Protection Regulation (GDPR), is designed to enable persons present in the European Union (EU) to better control their *personal data*. The GDPR applies to all companies that process the personal data of individuals present in the EU. Under the GDPR, personal data means any information relating to an identified or identifiable natural person. The GDPR sets forth specific guidelines in relation to the privacy and security of personal data. These guidelines are intended to ensure personal data is processed in a manner that ensures appropriate protection of the personal data. This includes protection, using appropriate technical or administrative measures, against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Additionally, the GDPR identifies two primary parties that it governs – *controllers* and *processors*. According to the GDPR, a *controller* means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.” A *processor* means “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.” For example, Deltek is a processor with respect to personal data that Deltek customers (the controllers) collect and Deltek processes on their

behalf. As a result of this role, Deltek has certain general responsibilities as outlined by the GDPR. Keeping customers' information safe and secure is among Deltek's highest priorities and most important responsibilities. Deltek has been working to implement strong security and privacy protections that reflect best practices as it relates to the GDPR.

Deltek Product Functionality and the GDPR

In addition to Deltek's general responsibilities related to privacy and data security, Deltek products may have specific capabilities that enable customers' ability to comply with the GDPR. While compliance with the GDPR is heavily dependent on processes, policies and strategies, Deltek products can also be used, configured, and implemented in ways to help controllers comply with the GDPR. As part of Deltek's release management processes, Deltek reviews a catalog of personal data types within each relevant product to ensure the ability to properly handle and manage those personal data types on an ongoing basis.

In the context of the GDPR, considerations with regard to product functionality apply primarily to the protection of, access to, auditing of, and existence of information that falls into the GDPR's definition of personal data. Deltek's products' capabilities can support a customer's ability to meet their compliance obligations, with additional enhancements making the process even easier. However, the availability of certain product functionalities may be dependent on a customer's configuration and whether they are up to date on the latest versions of the products. Additional information on [security](#) and [compliance](#) is available in those respective sections of [Deltek's Security and Trust Center](#). Customers may submit a request for more product-specific information by contacting their Account Manager or Deltek's Customer Care team.

The Deltek Cloud and the GDPR

Under the GDPR, data controllers have an obligation to implement technical and administrative measures to show that they have considered and integrated data protection principles in their processing activities. The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unsanctioned or unlawful processing and against accidental loss, destruction, or damage. Through Deltek's cloud offerings, controllers are provided with services and resources, above and beyond core product functionality, to help them comply with the GDPR requirements that may apply to their operations. Deltek cloud products may use granular data access controls, multi-factor authentication, data loss prevention efforts, monitoring and logging tools, encryption in flight and at rest, audit capability, and adherence to IT security standards. In addition, the GDPR imposes restrictions on the transfer of personal data outside of the EU, requiring onward transfers of personal data to third countries be governed by a European Commission adequacy decision or other appropriate cross border data transfer mechanism as outlined in Chapter 5 of the GDPR. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The GDPR, as well as other laws and regulations, imposes a duty on all companies to report certain types of data breaches to the relevant supervisory authority. In certain cases, companies will also have to report certain types of data breaches to affected individuals. Deltek has implemented robust incident response measures across all of its cloud offerings that are designed to reduce the time required to identify, investigate and report data breaches.

As a part of Deltek's off-boarding procedures for customers of cloud-based offerings, at the conclusion of data processing efforts for that customer, unless prohibited by law, Deltek will return personal data to the controller and delete personal data and copies thereof from the customer's cloud environment upon request.

Moving Forward

Deltek welcomes the opportunity to strengthen its commitment to privacy and data security. Deltek will continue to evolve and refine product capabilities and implement any required operational changes as regional privacy and data security regulations evolve. At Deltek, privacy is a fundamental right, and Deltek is committed to assisting its customers in their GDPR compliance efforts.

If you have specific questions about the GDPR or other applicable privacy, and privacy and data protection related requirements, as they relate to your use of Deltek products, you may email privacy@deltek.com.

Disclaimer: This content is provided for informational purposes only and should not be relied upon as legal advice. The application and impact of privacy and data protection regulations and laws can vary widely based on the specific facts involved. Readers are cautioned to determine how the relevant requirements, regulations, and/or laws apply to their business through independent analysis and consultation with legally qualified professionals.

Last Updated: December 5, 2019