Deltek Know more. Do more.®

General Data Protection Regulation (GDPR)

GDPR is coming. What is it and what do you need to know?

What Is It?

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, better known as the General Data Protection Regulation (hereinafter GDPR or the Regulation), is designed to enable persons present in the European Union (EU) to better control their *personal data* and applies to all companies that process the personal data of individuals present in the EU. The GDPR was ratified in April 2016 and a two-year implementation period followed. The GDPR enters into force 25 May 2018. Personal data is any information relating to an identified or identifiable natural person. The Regulation identifies two primary parties that are governed by the GDPR – *controller* and *processor*. According to the Regulation, *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 its controllers (Deltek customers) collect and Deltek processes on their behalf.

The Regulation sets forth very 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.

The Regulation also provides for the rights of individuals in relation to their personal data. First and foremost, in these rights is the requirement that the controller lawfully collect and process personal data. With respect to data sets where Deltek is the controller, Deltek is directly responsible for responding to individual requests under the GDPR. With respect to personal data where Deltek is the processor, Deltek ensures that its controller customers are using a trusted platform and are well positioned to respond to individual requests. The following individual rights are key components of the Regulation:

- **Right of Access** (Article 15) – Individuals have the right to access their personal data and supplementary information. The right to access allows individuals to be aware of and verify the lawfulness of the processing.
- **Right to Rectification** (Article 16) – The GDPR provides individuals the right to have personal data rectified. Personal data may be rectified if it is inaccurate or incomplete.
- **Right to Erasure / Right to be Forgotten** (Article 17) – The regulation states that a data subject has the right to be forgotten or the right to have his or her data erased "where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed."

- **Right to Restriction of Processing** (Article 18) – Individuals have a right to block or suppress processing of personal data. When processing is restricted, controllers and/or processors are permitted to store the personal data, but not further process it.
- **Right to Data Portability** (Article 20) – In essence, data portability provides the ability for data subjects to obtain and reuse their data for their own purposes and across different services. This right facilitates their ability to move, copy or transfer personal data easily from one IT environment to another, without hindrance. In addition to providing consumer empowerment by preventing lock-in, it is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner under the control of the data subject.
- **Right to Object** (Article 21) – Individuals have the right to object to processing for purposes related to the performance of a task in the public interest/exercise of official authority, direct marketing, and for purposes of scientific/historical research and statistics.

Data controllers and data processors have increased responsibilities to ensure that personal data is effectively protected. Supervisory authorities have powers to ensure that the principles of the Regulation, as well as the rights of the individuals concerned, are upheld according to the wording and the spirit of the Regulation. Fines for companies that do not comply with the GDPR can be significant. Regulators will now have authority to issue penalties equal to the greater of €10 million or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations. In addition, violations of obligations related to legal justification for processing, data subject rights, and inappropriate cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross revenue.

Given the broad reach of the GDPR and the scale of the penalties that can result from the lack of compliance, all impacted firms should be looking closely at the GDPR to ensure they have the processes, policies and systems in place to demonstrate compliance.

Deltek and the GDPR

In the context of the GDPR, in most cases, Deltek takes on the role of processor in its relationship with its customers. 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 closely with the European Data Protection Authorities, and have implemented strong security and privacy protections that reflect their guidance.

Deltek is well situated to meet the privacy and security requirements of the GDPR. Deltek's services are backed by robust, state-of-the-art technical and administrative safeguards, dedicated security, operational and privacy teams, and Deltek products and services are regularly reviewed by third-party auditors. Deltek has processes in place to build security and privacy into its products from the very earliest stages and are further evolving practices, including Data Protection Impact Assessments, to meet the GDPR's requirements regarding Privacy by Design and Privacy by Default.

Deltek Product Functionality and the GDPR

In addition to Deltek's general responsibilities in relation to the GDPR, Deltek products have very specific capabilities that enable customers' ability to comply. While compliance with the GDPR is heavily dependent on processes, policies and strategies, the Deltek products can also be used, configured and implemented in ways to help controllers comply with the Regulation. As part of Deltek's release management processes, a catalog of personal data within each relevant product is maintained and reviewed to ensure the proper handling, visibility and management of that personal data on an ongoing basis.

When it comes to product functionality, considerations in the context of the GDPR apply primarily to the access to, auditing of and existence of information that falls into the definition of personal data under the Regulation. Deltek's products can assist a company's ability to comply with the regulation in ways such as:

- **Audit Visibility/Logging** – Deltek products have audit capabilities to track any changes or additions to personal data within the system. This functionality assists companies in complying with the Regulation's requirements to maintain detailed records of processing activities. Controllers may be required to make records of processing activities available to the relevant supervisory authority for the purposes of an investigation.
- **Employee/Contact Reporting** – Deltek products provide extensive reporting tools to harvest personal data related to employee and contact records. This functionality assists companies in complying with the Regulation's requirements, at the request of a data subject, to provide access to their personal data and/or allow a data subject to rectify their personal data.
- **Extensive Application Security –** Deltek products provide robust controls around access to data and access to transactional and processing functions. This functionality assists companies in responding to requests from data subjects to exercise their rights under the GDPR.
- **Data Export –** All relevant products provide data export functionality in relation to both contact and employee data. This functionality assists companies in complying with the Regulation's requirements to provide data portability for a data subject's personal data.

Availability of the product functionality described here may be dependent on customers being up to date on the latest versions of the affected products. Additional enhancements to product functionality will make it even easier for controllers to comply with the Regulation in future product releases.

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. These include 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. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The GDPR will introduce 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 breach detection and 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 in production instances.

Moving Forward

Deltek welcomes the GDPR as an opportunity to strengthen its commitment to data privacy. Deltek will continue to work closely with regulators and customers as the Regulation enters into force. As additional clarity is established around GDPR, Deltek will continue to evolve and refine product capabilities and implement any required operational changes. 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 and 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 the GDPR can vary widely based on the specific facts involved. Readers are cautioned to determine how the GDPR applies to their business through independent analysis and consultation with legally qualified professionals.

Last Updated: 10 December 2017