



GDPR and OpenText™ Information Governance

What the new EU data privacy rules mean for your organization

Rapid technological developments and globalization have brought new challenges for the protection of personal data. To address this, the European Union (EU) entered into force the General Data Protection Regulation (GDPR) on May 25, 2016, replacing the European Data Protection Directive (95/46/EC). GDPR enforcement comes into effect on May 25, 2018. This new law will impose consistency across the EU and more regulatory and citizen control over personal data. Affected organizations now have less than two years to enact policies, procedures and technologies to comply with the GDPR. The penalty for non-compliance is steep, €20M or 4% of annual revenue, whichever is greater.

GDPR's Six Privacy Principles

The GDPR is designed to protect the privacy of EU citizens by requiring companies to follow six key principles:

1. **Lawfulness, fairness and transparency** - requirement to tell individuals (data subjects) how their information will be processed and it must be lawful to the regulation.
2. **Purpose limitation** - personal data can only be collected for explicit and legitimate purpose and its use cannot be expanded beyond the consent received from the data subject.
3. **Data minimization** - personal data collected should be adequate, relevant, and limited to only what is necessary in relation to the purposes for which they were collected and are processed.
4. **Accuracy** - personal data must be accurate; data subjects have the right to request corrections and such requests must be acted upon quickly.
5. **Storage limitation** - personal data must not be held for any longer than is necessary for the explicit and legitimate use authorized by the data subject.
6. **Integrity and confidentiality** (including "privacy by design and default") - personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

OVERVIEW

Information Governance is the ability to control the acquisition, management, retention, and disposal of all enterprise information – both structured and unstructured – within your business, to help reduce risk, ensure compliance, and increase business productivity and efficiency.

OpenText Information Governance solutions provide the tools to support your compliance strategy and meet GDPR requirements for:

- data minimization
- records management
- security, integrity, privacy,
- and data subjects' rights to erasure, rectification, and data portability.

OpenText Cloud Solutions offer a comprehensive set of security and compliance capabilities.

We interact with customers, regulatory bodies, and standards boards to advance compliance and serve customers' needs. We will remain closely engaged with you as we prepare together for GDPR enforcement to take effect.

OpenText Product Security Assurance Program ensures that all our products, solutions, and services are designed, developed, and maintained with security in mind.

Strengthened Rights of EU Citizens

Under the GDPR, EU citizens have more rights: the right to access information about their personal data held, the right to data portability (transfer their data to another data processor), the right to rectify or erase incorrect data ("right to be forgotten"), the right to restrict processing of their data under certain circumstances, the right to be notified of data breaches under certain circumstances (including alteration of data and unauthorized disclosures of data) and the right to object to processing, including digital marketing.

What Applies and Who is Subject

The GDPR applies to the personal data of EU citizens even if the data is collected, stored and processed outside of the EU. The GDPR applies to all types of companies, even if they are not resident in the EU. Organizations that collect or process personal data of EU citizens are subject to the law. The GDPR is not industry-specific. Unlike HIPAA for example, a privacy and security law for the U.S. healthcare industry, the GDPR applies to all industries. Further, the GDPR makes no distinction between B2B and B2C marketing – business customer data is also subject if it is personal data.

“Effective” and “Dissuasive” Fines for Non-Compliance

The May 2018 compliance deadline for the GDPR is fast approaching and failure to comply can result in regulatory fines that can be fatal to some companies. There are two tiers of fines depending on whether the data controller or processor committed any previous violations and the nature of violation:

- The lower fine threshold is two percent of a company's worldwide annual revenue or €10 million, whichever is higher.
- The higher fine threshold is four percent of a company's worldwide annual revenue or €20 million, whichever is higher.

International Data Transfers and Cloud Providers

Companies subject to the GDPR will want to ask their cloud services providers questions about where data is physically stored, their data protection policies for customer data, whether the data is moving outside of the EU, and the service provider's overall plan to achieve GDPR compliance. Article 28 of the GDPR specifically provides that to “ensure compliance in respect of the processing to be carried out by the processor on behalf of the data controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures which will meet the requirements of this Regulation, including for the security of processing.”

How OpenText Can Help with GDPR Compliance

OpenText is a leader in Enterprise Information Management (EIM) for which information security and protection are key tenets. For this reason, EIM is one of the most important tools for helping organizations meet regulatory requirements, and should be central to your overall GDPR compliance and data protection strategy. OpenText Information Governance products give customers the ability to control the acquisition, management, retention, and disposal of all

GAIN CONTROL OF PERSONAL INFORMATION WITH OPENTEXT INFORMATION GOVERNANCE SOLUTIONS

OpenText™ Content Suite

- *Transparent, automated, enterprise-wide governance to enable information security, privacy and compliance*
- *Capabilities for redaction, encryption, advanced search and defensible disposition*
- *Industry-leading OpenText™ Records Management to adhere to data minimization*

OpenText™ InfoFusion™ Discovery solutions

- *Information discovery, semantic classification, and organization of both internal and external information sources to enhance operations and reduce risk*

For more information on how OpenText can help with GDPR compliance, visit:

www.opentext.com/gdpr

InfoGov Basics

www.infogovbasics.com

enterprise information – both structured and unstructured – within their business to help reduce risk, ensure compliance, and increase business productivity and efficiency. Our solutions do this by giving organizations the confidence of knowing where their information resides, ability to control access and permissions, secure content at rest and in motion, advanced search to quickly find required information, and the ability to dispose of records in a systematic and defensible manner.

GDPR terminology

- **Personal data** - any information relating to an identified or identifiable natural person
- **Data subject** - an identified or identifiable natural person
- **Data controller** - the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.” The controller, therefore, is the entity that makes decisions about processing activities, regardless of whether it actually carries out any processing operations.
- **Data processor** - natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.” In other words, while the controller is the entity that makes decisions about processing activities, the processor is any entity contracted by the controller for carrying out the processing.

www.opentext.com/gdpr