



**OpenText  
GDPR commitment**

## A message from our DPO



At OpenText, we are committed to our customers' success and protecting their information. We recognize that this commitment isn't just about the products and services we offer, but how we operate as an organization with respect to our own compliance.

OpenText welcomes the GDPR as an opportunity to review our information governance program, and ensure our internal processes, procedures, data systems and documentation are ready when GDPR comes into force.

We have been helping our customers manage and protect their enterprise information assets since 1991. We are using the same technologies to support our own journey to GDPR readiness, with our own internal experts leading the way.

We would like to share the steps we've taken, and initiatives in the works, as we prepare for the GDPR. These steps will ensure success for both OpenText and our customers on this GDPR journey.

**Pieter J.L. (Berry) Wittenberg**

OpenText Global Data Protection Officer

## The General Data Protection Regulation


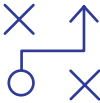


The [General Data Protection Regulation \(GDPR\)](#) is the new European Union data privacy legislation to modernize and reform the laws that address the handling of personal data of European Union residents. It represents the biggest overhaul of the world’s privacy rules in more than 20 years.

### Our commitment to the GDPR

As the leader in Enterprise Information Management, OpenText takes information security and privacy very seriously. We have long maintained industry best practices to incorporate data protection and privacy in our day-to-day practices, as well as helping our customers implement our solutions and expertise to build strong compliance programs of their own.

OpenText has thoroughly analyzed GDPR requirements and their relevance to us as both a data controller and data processor. In response, OpenText has implemented an organization-wide GDPR compliance strategy intended to meet all requirements when the new regulation comes into effect, involving a cross-functional team of internal resources. We are proud to say our business already incorporates many of these requirements and GDPR principles today. However, we are using the GDPR as an opportunity to further strengthen our practices.

#### Summary of our approach

Assess	Plan	Execute	Maintain
			
<ul style="list-style-type: none"> <li>Executive Leadership Team endorsed development of GDPR Program</li> <li>Appointment of Global Data Protection Officer</li> <li>Conducted enterprise GDPR diagnostic assessment led by global risk advisory firm EY LLP</li> </ul>	<ul style="list-style-type: none"> <li>Established a cross-functional GDPR task force and assigned responsibilities</li> <li>Prepared implementation plan to deliver on Assessment recommendations</li> </ul>	<ul style="list-style-type: none"> <li>Conducted data discovery of personal information across the enterprise</li> <li>Inventoried and documented records of processing activities</li> <li>Implemented action plans by each affected line of business including Marketing, HR, Procurement and IT</li> </ul>	<ul style="list-style-type: none"> <li>Maintain registry of processing activities</li> <li>Conduct privacy impact assessments on a regular cadence</li> <li>Update risk framework on a regular basis</li> <li>Confirm operating effectiveness of risk controls</li> </ul>



## OpenText as a Data Controller

As a company that collects and processes the personal data of our customers, partners and employees, we have implemented key GDPR preparedness initiatives including:

- **Consent management**—Consent standards have increased under the GDPR. However, OpenText has already been compliant with similar existing requirements inside data privacy regulations from other jurisdictions, including countries within Europe. Our Sales and Marketing organizations conducted a thorough review of their consent management practices and have brought them in line with the GDPR. This includes active opt-in to continue to receive communications from us as well as including privacy purpose statements when we collect personal info e.g. to share research papers.

As an existing or prospective customer, you may have seen some of those changes in your interactions with our web pages, events invitations and emails. Pre-checked or implied opt-ins are insufficient—individuals must know to what they are consenting and that they may withdraw consent at any time. At OpenText, we strive to create personalized and delightful experiences for those who engage with us and maximize the value for customers at each interaction, at the same time balancing this objective with security, trust and respect.

- **Human Resources**—The GDPR is not just about our customers. Although there are GDPR efforts focused on external data, the new regulation also extends to the personal data we hold regarding our job applicants and employees. Our Human Resources team has been working on several initiatives to prepare for the GDPR including:
  - Optimizing our HR systems to manage applicant and employee information in accordance with the GDPR.
  - Reviewing HR systems to better manage the information we hold, why we hold it, who has access to it and for how long we hold it.
  - Developing Consent and Privacy Notices to provide transparency to our candidates and employees of the information we hold, why we hold it, who has access to it and for how long we hold it.
  - Reviewing HR related policies and procedures to ensure data privacy compliance with the new legislation.
- **Records management**—We are working to ensure our records management policy includes retention schedules that authorize disposition when customer information is inactive, outdated or no longer needed. This will support the data minimization principle and assist us to avoid retaining the personal data of our customers for a longer period than necessary.
- **Security**—Data privacy and data security are two equally important parts of a comprehensive data protection strategy. While OpenText already follows information security and risk management industry best practices as defined by our ISO 27001:2013 global Information Security Management System (ISMS), we are aware of the new and increased security standards that GDPR introduces and will continue to evaluate and update our practices to ensure that they align with industry standards. Our ISMS provides continuous and rigorous risk management processes to help support the ongoing confidentiality, integrity, and availability of all information in the custody of OpenText.
- **Policies, procedures and training**—We are reviewing relevant policies and procedures to ensure updating them to reflect any new privacy requirements, including those relating to Security, IT, Privacy and HR. You can read our [OpenText Privacy and Security Policy](#) and [Cookie Policy](#) on our website. OpenText has a long-standing practice of mandatory Corporate Information Security and Compliance and Ethics training for all staff. Curriculums will be reviewed to incorporate any new content necessary to raise awareness and educate employees about their obligations under the GDPR.



## OpenText as a Data Processor

It is important that we fulfill our commitments under the GDPR as a data processor to our customers, the data controllers, who are using a third-party like us to process personal data. Some of our key activities in this area are:

- **Rights of data subjects**—GDPR gives individuals the right to access the data provided to and processed by the controller for purposes including deletion, rectification, transfer to another controller and objection to processing. The data we house on behalf of customers is owned by the customer, who is the data controller. Our customers also maintain the access control to their data, which means in the majority of cases, as data controller they can respond to and action requests from their data subjects. As a data processor, we do not respond directly to requests from data subjects. We continue to further enhance our processes and applications to better enable customers to respond to lawful requests from their data subjects.
- **Contractual commitments**—We work with our customers to ensure that the GDPR obligations are included in the contractual commitments for our cloud services to the customers satisfaction, including the use and management of sub-processors, timely security support and breach notifications in accordance with the new requirements. Cloud services agreements include statements regarding how data is to be handled while we are custodians of the data and how it can be repatriated to the customer upon termination of services. We are also reviewing our data processing agreements (DPA) to standardize the inclusion of GDPR requirements. OpenText has worked extensively with EU counsel to help ensure our agreements contain appropriate provisions for lawful personal data processing.
- **Cloud security**—Enterprises trust OpenText to manage their business-critical applications and information, in large part due to our commitment and expertise in cloud security, privacy and compliance. All our cloud services have a baseline standard of privacy and security, with technical and organizational security controls governed by industry standard third parties and proven via independent attestations.

OpenText has certified all levels (data center, infrastructure, platform–application and service certifications may vary) to assure our customers of the security controls, processes, procedures and policies that we have in place. Further certifications will be gained over time either to extend coverage or to add certifications as required by the industry and our customers.

Our EIM products and services are certified with many industry and regional standards eg. HIPAA, FDA 21 CFR Part 11, FINRA. We will continue to evolve our controls as industry standards change. Some of the current cloud certifications are as follows:

### Enterprise Cloud

- ISO 27001:2013
- SOC 1 Type II
- SOC 2 Type II
- SOC 3

### Business Network

- ISO 27001:2013
- SOC 1 Type II
- SOC 2 Type II
- SOC 3
- HIPAA

## Business Network–EasyLink

- SOC 1 Type II
- SOC 2 Type II
- SOC 3

## Documentum (DaaS) Cloud

- SOC 2 Type I
- SOC 2 Type II
- **Breach notification**—Operationalizing incident management and meeting the 72-hour breach reporting window is, and will continue to be, a challenge for all organizations. The OpenText Global Information Security Team has a well-established Data Breach Response Process that spans from the time a suspected breach has occurred to post-incident response closure steps. OpenText data breach procedures are comprised of five steps: discovery, assessment, response, protection and recovery. It is in the “response” step where breach reporting requirements and timeframes are determined. OpenText has reviewed data breach notification laws in all regions in which we operate, including the requirements under the GDPR, and is committed to compliance.



## Helping our customers along the GDPR journey

Enterprise Information Management (EIM) technologies are key to an effective and sound privacy compliance and data protection strategy. As the leader in EIM, OpenText is committed to helping our customers along their journey to GDPR readiness and compliance. However, it is important to recognize that compliance is a shared responsibility. Regulatory compliance requires a combination of processes, policies, expertise, education and training as well as the right technology tools. We believe that the path to compliance requires a shared understanding and common culture around privacy.

How we help our customers prepare for the GDPR:

- **GDPR resources**—We have posted whitepapers, videos, webinars-on-demand and blog posts explaining how organizations can comply with key GDPR principles using EIM and our services.
- **OpenText Product Security Assurance Program (PSAP)**—Long before the GDPR, OpenText has established our Product Security Assurance Program. The PSAP is intended to ensure that our products, solutions and services are designed, developed and maintained with security in mind.
- **Data protection by design and by default**—Under the terms of the GDPR, privacy should be built in deliberately and be adopted by default in processing systems. At OpenText, we are constantly reviewing privacy by design principles, such as end-to-end security, to incorporate them into not only our business processes and systems but into the software we develop.