OpenText powers data privacy

Organizations must balance compliance with business objectives to comply with global privacy regulations, such as the GDPR. Advanced privacy-enabling technologies can help turn privacy into a catalyst for growth.

OpenText™ Core Data Discovery & Risk Insights (Voltage) at a glance

- **Privacy compliance:** Ensure that you can uncover sensitive and personally identifiable information
- **Advanced privacy-enhancing technology:** Take protective action toward data during discovery to power faster decision-making and establish data trust
- **Drive better business outcomes:** Beyond privacy compliance, OpenText technology powers data minimization, secure cloud analytics, information lifecycle management, greener IT, and sustainability

The General Data Privacy Regulation

The General Data Protection Regulation (GDPR), the comprehensive data protection law introduced in the European Union (EU) in 2018, replaced the previous EU data protection directive and aims to give individuals greater control over their personal data and how organizations use it. The regulation applies to any organization that processes the personal data of individuals in the EU, regardless of where the organization is based. In addition, companies operating outside the EU must also comply with the GDPR if they process the personal data of EU citizens.

The GDPR sets out a range of rights for individuals, including the right to access their personal data, the right to have their data deleted, and the right to have their data transferred to another organization. It also imposes strict obligations on organizations that handle personal data, such as obtaining explicit consent from individuals before collecting their data and ensuring that data is secure and protected from unauthorized access.

In addition to these requirements, the GDPR includes penalties for organizations that breach the regulation, with fines of up to four percent of an organization's annual global turnover, or 20 million euros (whichever is greater).

The GDPR set a new standard for data protection and privacy in the EU and has influenced similar privacy laws worldwide. It is considered a significant milestone in developing data protection law and serves as an example of how organizations can be held accountable for handling personal data.

Right to delete	Business purpose	Data minimization	Data security and protection	Data portability
Article 17	Article 6	Article 5 (1)(c)	Article 5(f), 6, 32, 34, Recitals 39, 83	Article 20

Advanced privacy-enabling technology from OpenText

The General Data Protection Regulation (GDPR) provides a framework for how organizations can establish their privacy programs and practices to comply with regulations and reduce risk. OpenText™ Core Data Discovery & Risk Insights (Voltage) delivers advanced privacy- enabling and privacy-preserving technologies to augment these programs. It helps customers drive compliance while ensuring that the data can be securely and ethically shared across the business. It also helps drive cost containment; data retention and disposition; and environmental, social, and governance mandates, such as reduced power consumption, sustainability, and Green-IT.

OpenText privacy-enhancing and privacy-preserving technologies

Privacy-enhancing technology (PET) refers to technologies designed to improve privacy by reducing the amount of personal data collected and shared. These technologies include PII detection, de-identification, anonymization, and data minimization techniques. The goal of PET is to reduce the risk of personal data being used or misused in ways that could harm the user if not handled ethically.

Privacy-preserving technology (PPT) refers to a subset of privacy-enhancing technologies that offers a variety of techniques and tools designed to protect the privacy of individuals and organizations when they share, collect, or personally process data. These technologies are used in various contexts, including consumer privacy, data analytics, and data lifecycle management. The goal of PPT is to ensure that personal data remains secure and cannot be accessed or used by unauthorized parties.

Privacy-preserving technology includes:

- **Encryption:** Preserves data from unauthorized use/access or being able to see the data in clear text.
- **Masking/Anonymization:** Preserves data by removing personally identifiable information (PII) from data sets, making it difficult to trace the data back to specific individuals.
- **Tokenization:** Preserves data by replacing sensitive data with a unique, reversible token that can be used to represent the data but cannot be used to reveal the data itself without the presence of the token.

- **Pseudonymization:** Preserves data by replacing PII with a pseudonym, or fake name, that cannot be traced back to the individual.
- **Data minimization:** Preserves data by collecting and storing only the minimum amount necessary to achieve a specific purpose, reducing the risk of data misuse or abuse.
- **Data access monitoring and controls:** Preserves privacy by ensuring that unauthorized parties cannot access or use personal data.

These privacy-preserving technologies are critical to business operations. They enable organizations to balance the collection and use of customer data and meet their obligation to protect individuals' personal information from being accessed, used, or shared without their consent.

OpenText helps organizations with:

The Right to Delete—Article 17

OpenText Core Data Discovery & Risk Insights' data discovery capabilities help organizations understand the value of their data and how they can apply retention and disposition policies on high-value data-in-use to lessen the disruption of subject rights requests. For example, in cases where the right to delete is requested and valid, OpenText Core Data Discovery & Risk Insights' can delete that data from the source location or lead application.

Business Purpose—Article 6

OpenText Core Data Discovery & Risk Insights' capabilities provide insight and analysis around sensitive data. They can dynamically tag data with categories that map to regulations, specifically around the right to process customer and consumer data.

Data Minimization—Article 5 (1)(c)

During data discovery processes, legacy, duplicate, and low-to-no value data can be remediated. In addition, customers can archive and retire application data for compliance purposes and delete redundant, out-of-date, and trivial unstructured data at the source.

Data Security and Protection— Articles 5(f), 6, 32, 34, and Recitals 39 & 83

Acting on data that is responsive and relevant to data privacy regulations is a "game changer" for organizations looking to have technology assist them in achieving privacy compliance. OpenText supports a myriad of protective actions on data that can protect consumer information and support broader corporate objectives.

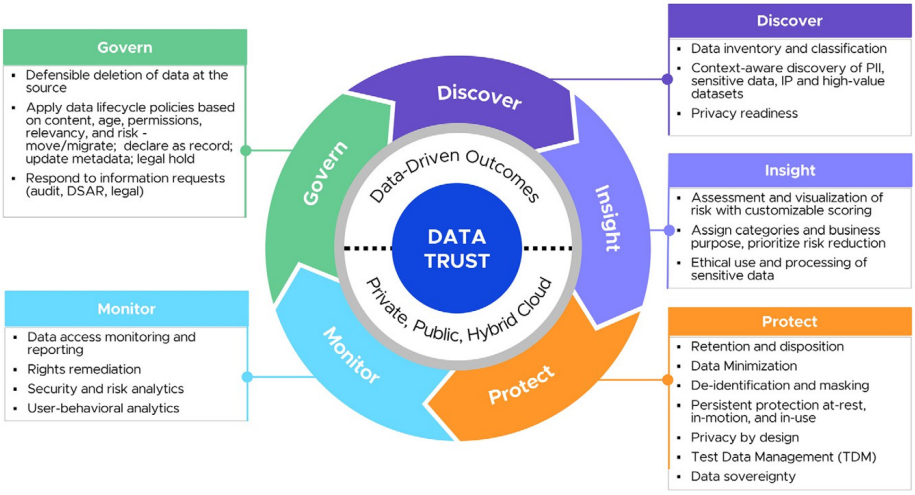
OpenText can:

- Encrypt data at the source or leverage workloads in cloud data warehouses and analytics platforms. In the event of a breach, this can protect your organization from sanctions and fines.
- Protect the identity and personal information via dynamic data masking while in use by the business.
- Apply information lifecycle policies to data to ensure proper business use and that data deletion requirements are met automatically.

Data Portability—Article 20

If a data portability request is made and is valid, OpenText Core Data Discovery & Risk Insights can produce a data subject's information in a structured, commonly used, and machine-readable format.

Building data trust and voltage data privacy and protection



Privacy compliance and data trust support corporate objectives and growth drivers

As organizations embark on the journey to privacy management and privacy compliance, OpenText privacy-enhancing technology helps them prepare to comply with global regulations and support their existing privacy processes and practices. Moreover, OpenText helps build data trust to support many different business outcomes that drive business growth, operational efficiency, and sustainability.

Sustainability

Many organizations have taken on corporate objectives to support greater sustainability, reduce their carbon footprint, and operate an increasingly green business. “Green” OpenText technologies help organizations achieve these mandates by reducing the storage, power consumption, and operational costs associated with managing legacy data. In addition, data minimization efforts and archiving and cloud migration capabilities drive the business towards lower costs, reduced data and application sprawl, and streamlined operational expenses.

Data protection

As information is continuously protected by OpenText, the unintended consequences of accidental exposure or an actual data breach can be mitigated through encryption and tokenization. In addition, sensitive information is protected from exposure if the data is subject to a breach. At the same time, data protected by OpenText can be leveraged by data analysts and business users in its protected state to derive value for the business. For example, business intelligence and cloud analytics tools can manipulate the data to look for ways to grow the business while maintaining the data’s referential integrity. This enables business users to source analytics workloads ethically, while ensuring that data analysts can leverage insights and trends.

Financial risk

Understanding the risk exposure around sensitive data should go beyond simple risk scoring. For example, OpenText provides visibility into the financial risk of managing and protecting large data estates by visualizing the economic impact of managing and protecting data. This data can be used to better estimate cyber insurance premiums, while monitoring data protection

activities.

Secure cloud analytics

OpenText data-centric security integrates with data analytics platforms, such as Google BigQuery, Amazon Redshift, Azure Synapse, Snowflake, Cloudera, and Teradata. OpenText enables high-scale secure analytics and data science in the cloud and on-premises using format-preserved tokenized data, mitigating the risk of data exposure while enabling privacy compliance.

Defensible disposition

Data privacy requirements for data deletion and the right to be forgotten can be disruptive to IT and content owners. Having data lifecycle policies applied to business-critical data (mapped to its business purpose) can reduce the impact of these requests. In addition, automating defensible disposition based on policy further streamlines this process, ensuring compliance and driving down the cost of managing data.

Data minimization

Keeping what you need and ensuring that what is preserved is protected and has a business purpose is a core principle of data minimization. On collection, OpenText can help organizations ethically process consumer data and protect it while in use. For legacy data, OpenText Core Data Discovery & Risk Insights can drive cost efficiencies and reduce the threat landscape. By removing duplicate data and data that serves zero value to the business data discovery, you can reduce the overall storage footprint and application sprawl, while reducing the personnel required to manage data and the lead application or database.

ISO 27701

ISO 27701 is a data privacy extension of ISO 27001 (Information Security Management System). OpenText Core Data Discovery & Risk Insights hosting and infrastructure services are certified to support the ISO 27001 risk-based approach for implementing security controls around people, processes, and technology. OpenText Core Data Discovery & Risk Insights' capabilities drive compliance and support privacy management mandates covered in ISO 27701, including privacy impact assessments, ethical records of processing, data minimization, deletion requests, data portability, and data protection.

Summary

OpenText Core Data Discovery & Risk Insights provides privacy-enhancing technology within a data trust framework for data discovery and protection. OpenText enables organizations to reduce information risk, ensure data privacy, and secure quick access to critical data that drives the business. OpenText provides data protection and preservation and mitigates the risk of processing sensitive data while supporting other corporate initiatives that drive business growth, operational efficiency, and sustainability.

opentext™