

Voltage Powers Data Privacy (LGPD)

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

Voltage Data Privacy and Protection at a Glance

Privacy Compliance

Ensure that you can uncover sensitive and personally identifiable information.

Advanced Privacy-Enhancing Technology

Take protective action on data during discovery to power faster decision-making and establish data trust.

Drive More Business Outcomes

Beyond privacy compliance, Voltage technology powers data minimization, secure cloud analytics, information lifecycle management, greener IT and sustainability.

The LGPD (Lei Geral de Proteção de Dados) privacy law in Brazil, came into effect in August 2020 and aims to protect the personal data of individuals and regulate the collection, processing, and storage of such data by organizations.

Under the LGPD, organizations are required to obtain explicit consent from individuals before collecting and processing their personal data. The law defines personal data as any information that can be used to identify an individual, either directly or indirectly. For example, information such as name, address, phone number, email address, and IP address, as well as sensitive data such as racial or ethnic origin, religious beliefs, and health information.

Organizations must also implement appropriate technical and organizational measures to protect personal data against unauthorized access, use, disclosure, and destruction. As a part of LGPD, individuals have the right to access their personal data held by organizations and to request the correction or deletion of any inaccurate or incomplete information. They can also file complaints with the National Data Protection Authority (ANPD) if they believe their rights have been violated under the LGPD.

Advanced Privacy-Enabling Technology from Voltage

Brazil's General Privacy Protection Act (LGPD) provides a framework for how organizations can establish their privacy programs and practices to comply with regulations and

reduce risk. To augment these programs, Voltage Fusion by OpenText™ delivers advanced privacy-enhancing and privacy preserving technologies to help customers not only drive compliance while ensuring that the data can be securely and ethically shared across the business. Voltage Fusion also helps drive cost containment; data retention and disposition; and Environmental, Social, and Governance mandates such as reduced power consumption, sustainability, and Green-IT.

Voltage 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 include:

- **Encryption:** Preserves data from unauthorized use/ access or be 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.

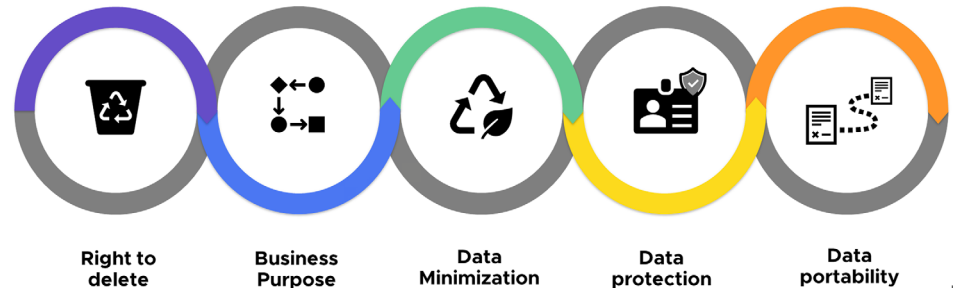
These privacy-preserving technologies are critical to business operations. They enable organizations to balance the collection and use of customer data and meet their obligation to protect individuals' personal information from being accessed, used, or shared without their consent.

Voltage Fusion Helps Organizations with the Following:

The Right to Delete—Articles 5, 16, 18(VI)

The “right to erasure” is split over multiple articles in the LGDP. The first requires the deletion of excessive, unnecessary, or unlawful data. The second involves deleting data on request if it has been collected based on consent. Voltage Fusion

enables the defensible disposition of personal information in accordance with policy, right to be forgotten or other data deletion requests.



Right to Delete	Business Purpose	Data Minimization	Data Security and Protection	Data Portability
Article 5, 16, 18(vi)	Article 6 (i)	Article 6 (iii)	Art. 5 (iii) (xi), Art. 6 (vii), Art. 12	Article 18(v)

Business Purpose—Article 6 (i)

LGPD introduces articles, including how data is processed and governed, limitations on storage, data minimization, and contract requirements.

The regulation also calls out the limitation on how long personal information can be retained. The LGDP specifies that controllers must disclose “the duration of the processing,” rather than personal data storage periods like in the GDPR.

Voltage Fusion can understand where duplicate and low-value data resides and assign retention policies and tagging to ensure ethical handling and processing of personal information.

Data Minimization—Article 6 (iii)

LGPD states that businesses must only retain what they need and have policies to ensure the proper disposition of that personal data. LGDP’s limitation of the processing also calls out minimization of personal information collected, used and for business purpose. To support this, personal information deemed “necessary” must have a specific business purpose for processing and retention period.

Voltage Fusion capabilities support data minimization efforts that reduce the cost and complexity associated with application and data sprawl. These use cases include application retirement and modernization, cloud migrations and data archiving. In addition, Voltage Fusion ensures that only the appropriate data is retained to support audit, legal and regulatory obligations.

Data Security and Protection—Article 5 (iii) (xi), Article 6 (vii), Article 12

LGPD states that a business that collects a consumer’s personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Articles 5, 6 and 12.

From a privacy compliance standpoint, Voltage can enable businesses to monitor data access and implement de-identification and encryption as technical safeguards that can protect personal information and corporate reputation in case of a breach.

Data Portability—Article 18(V)

LGPD states businesses that receive a consumer request to access their personal information shall promptly disclose and deliver, free of charge.

Voltage Fusion search capabilities can quickly find associated personal information and package responsive data as required to support data portability requests.

Privacy Compliance and Data Trust Support Downstream Corporate Objectives and Growth Drivers

As organizations embark on the journey to privacy management and privacy compliance, Voltage privacy-enhancing technology helps them prepare to comply with global regulations and support their existing privacy processes and practices. Moreover, Voltage 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” Voltage 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 Voltage, 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 Voltage 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 still 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, Voltage 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.

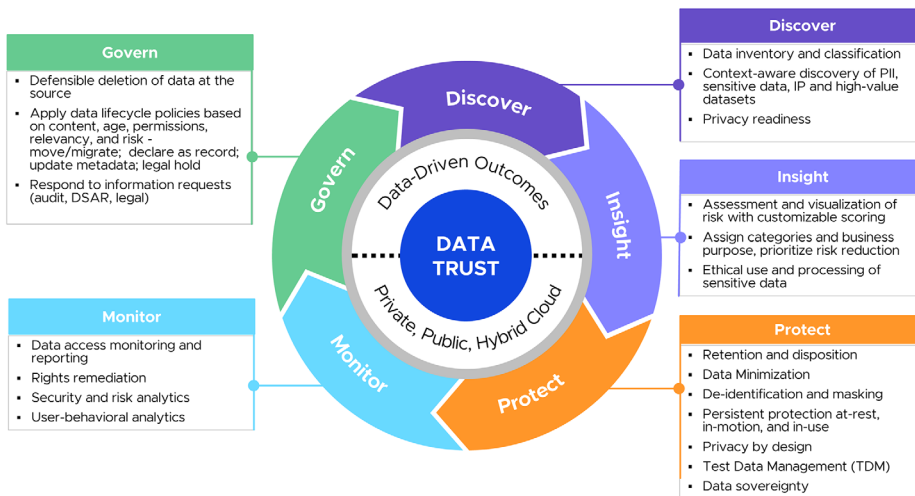
Secure Cloud Analytics

Voltage data-centric security integrates with data analytics platforms such as Google BigQuery, Amazon Redshift, Azure Synapse, Snowflake, Cloudera, and Teradata. Voltage 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.

Building Data Trust and Voltage Fusion



Connect with Us
www.opentext.com



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, Voltage can help organizations ethically process consumer data and protect it while in use. For legacy data, Voltage Fusion can drive cost efficiencies and reduce the threat landscape. By removing duplicate data and data that serve 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). Voltage Fusion, hosting and infrastructure services are certified to support the ISO 27001 risk-based approach for

implementing security controls around people, processes & technology. Voltage Fusion 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

Voltage Fusion provides privacy-enhancing technology within a data trust framework for data discovery and protection. Voltage enables organizations to reduce information risk, ensure data privacy, and secure quick access to critical data that drives the business. Voltage privacy-preserving technologies mitigate the risk of processing sensitive data while supporting other corporate initiatives that drive business growth, operational efficiency, and sustainability.