opentext™ | Cybersecurity

Solution Flyer

Voltage Powers Data Privacy CCPA/CPRA

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 California Consumer Privacy Act of 2018 (CCPA) and CCPA 2.0, also known as the California Privacy Rights Enforcement Act (CPRA), gives consumers more control over the personal information businesses collect about them, and regulations guide how to implement the law. This law secures privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to limit the use and disclose "sensitive personal information" (new protected data category under CPRA), including SSN, Driver licenses, Financial accounts/ card numbers, Geo-locations, Race/ethnic background, Religious affiliation, biometric data, union memberships and contents of an email, text messages;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt out of the sale of their personal information; and
- The right to non-discrimination for exercising their inherent rights.
- Businesses are required to give consumers specific notices explaining their privacy practices. The regulation applies to many businesses, including data brokers.

Advanced Privacy-Enhancing Technology from Voltage

The California Privacy Rights and Enforcement Act 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 Data Privacy and Protection by OpenText delivers advanced privacy-enhancing and privacy-preserving technologies to help customers not only drive compliance while ensuring the data can be securely and ethically shared across the business. Voltage also helps drive cost containment, data retention and disposition and Environmental, Social and Governance mandates like 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.

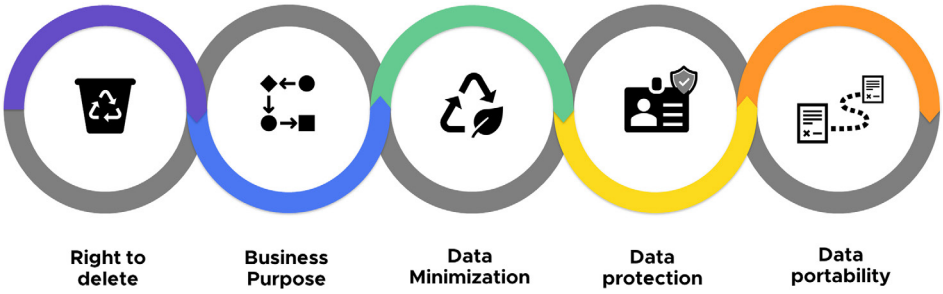
Privacy-preserving technology include:

- **Encryption:** preserves data from unauthorized use/ access or 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 as organizations look to balance the collection and use of customer data and their obligation to protect individuals' personal information from being accessed, used, or shared without their consent.

Voltage Data Privacy and Protection Helps Organizations with the Following:

The Right to Delete—Section 1798.105
Voltage 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
Section 1798.105	Recital 39, 83	Sections 1798.100(c) and 1798.100(a)(d)	Sections 1798.100(e) and 1798.150(a)	Sections 1798.100(d) and 1798.130(a)(2)

Business Purpose—Recital 39, 83
CPRA introduces new sections, 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. Each category of personal information should have a policy around "the length of time the business intends to retain each sensitive personal information, or for no longer than is reasonably necessary for that disclosed business purpose.

Voltage Data Discovery 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—Sections 1798.100(c) and 1798.100(a)(d)
CPRA states that businesses must only retain what they need and have policies to ensure the proper disposition of that personal data. CPRA also calls out minimization of personal information collected, used and disclosed. As a result, personal information deemed "necessary" must have a specific business use and retention period.

Voltage Data Discovery 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 Data Discovery ensures that only the appropriate data is retained to support audit, legal and regulatory obligations.

Data Security and Protection—Sections 1798.100 and 1798.185
CPRA 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 Section 1798.81.5.

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—Sections 1798.100(d) and 1798.130(a)(2)
CPRA states businesses that receive a consumer request to access their personal information shall promptly disclose and deliver, free of charge.

Voltage Data Discovery 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, the downstream value of Voltage privacy-enhancing technology is to help prepare your organization to comply with global regulations and support your existing privacy processes and practices. Moreover, it 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 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.

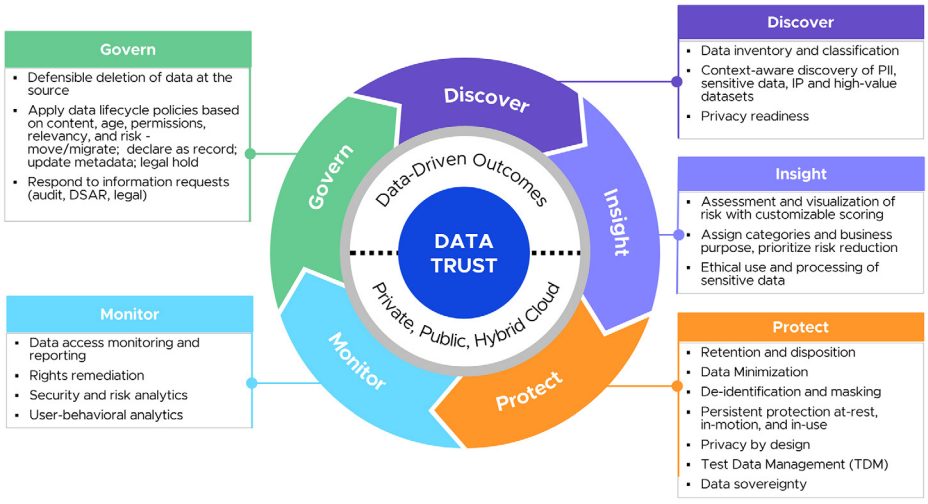
Data Protection
As information is continuously protected by Voltage, the unintended consequences of accidental exposure or an actual data breach can be mitigated through encryption and tokenization. In addition, sensitive information is protected from exposure if the data is subject to a breach. At the 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 allows business users to source analytics workloads ethically, while still ensuring insight and trends can be leveraged by data analysts.

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 estimate cyber insurance premiums better 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 Data Privacy and Protection



Connect with Us
www.CyberRes.com

Data Minimization
Keeping what you need and ensuring 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 data discovery can drive cost efficiencies and reduce the threat landscape. By removing duplicate data and data that serve zero value to the business data discovery reduces 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 Data Discovery, hosting and infrastructure services are certified to support the ISO 27001 risk-based approach for implementing security controls around people, processes & technology. Voltage Data Discovery 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 Data Privacy and Protection 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 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™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000085-003 | O | 03/23 |