Complying with the **CCPA** Using Seclore's Data-Centric Security

SECLORE™

Privacy Concerns in California's Tech-Driven Economy

The growing role of technology and data in consumers' everyday lives has increased the amount of personal information shared with businesses. As a result, companies are now aware of the consumers' personal details such as their family backgrounds, health and financial information, location, and even biometric profiles. Unauthorized access to such personal information can lead to disastrous consequences such as financial fraud, reputational damage, and even physical damage.

California is one of the world leaders in developing new technologies and related industries. Many businesses collect personal information from Californian consumers. The collection of personal data with no accountability has restricted Californians' ability to protect and safeguard their privacy.

What Is the California Consumer Privacy Act (CCPA)?

The California Consumer Privacy Act (CCPA) was authorized in 2018 and became effective on January 1, 2020, to provide consumers more control over the data they share and prevent unmanaged access controls and privacy management. It has a massive impact on corporate privacy initiatives across all technology, media, entertainment, and telecommunications (TMT) sectors.

Designed after the European Union (EU)'s General Data Protection Regulation (GDPR), the new regulations give users more data control. Businesses primarily focused on the United States and markets in the Americas largely avoided GDPR's scope for a long time. Regardless, the alarming data breach incidents and privacy concerns among consumers and legislatures globally drive data privacy deployment. Considered one of the strictest privacy laws in the United States, CCPA allows California residents to control how businesses process their personal information. Businesses will have to respond to requests from California residents to access, delete, and opt out of sharing or selling their information. Additionally, businesses must design privacy programs to comply with CCPA's prescriptive opt-out measures and overall data protection.

The CCPA Act and Its Objectives

CCPA applies to enterprises operating in California or collecting or processing personal information about California residents. It applies to businesses that meet at least one of the following criteria:

Generates gross annual revenue of more than $25 million

Purchases, procures, sells, or shares personal information for 50,000 or more consumers, households, or devices

Generates at least 50% of its annual revenue from selling consumers' personal information

Unlike GDPR, CCPA is more focused on compliance, with data protection being a critical component. It focuses on the cybersecurity of the infrastructure storing consumer data. Here, protected data includes any personally identifiable information (PII) that can be used to identify a consumer. CCPA defines personal information as "information that identifies, relates to, describes, and is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Lack of access controls and data security protections could result in huge penalties, so CCPA enforces cybersecurity implementation.

The objective of the Act is to provide consumers with more control over the personal information that businesses collect about them and establish new privacy rights for California consumers, including:

- The right to know about how companies are handling their data
- The right to delete personal data collected by companies
- The right to control who can access their data, mainly with third parties
- The right to opt-out

Introduction to Seclore

Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our Data-Centric approach to security ensures that only authorized individuals have access to sensitive digital assets inside and outside their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Leading enterprises choose Seclore to protect and control digital assets without sacrificing seamless collaboration and data sharing.

With Seclore, you can know, protect, and control your organization with Data-Centric Security capabilities.

Know

Know exactly what's shared and where your data is:

- Risk insights and trends
- Access patterns and usage analytics
- Location awareness

Protect

Protect every single data asset wherever it goes:

- Policy management
- Dynamic watermarking
- Classification labeling
- AES256-bit encryption

Control

Control who has access and revoke it at any time:

- Granular access control
- Real-time access revocation
- Dynamic policy federation

How Seclore Can Help Organizations Comply with CCPA

The scope of CCPA includes all personal data processed by businesses based inside the State of California and personal data of California citizens processed by enterprises based outside the State.

Implementing and adhering to the "reasonable security procedures and protections" required by the California Consumer Privacy Act (CCPA) protects private or sensitive personal data from unauthorized access. Irrespective of where the information resides - even outside California - it should remain fully private, secure, and monitored. Due to multi-cloud environments, data sharing and third-party collaboration can expose personal consumer data, leading to data breaches and loss. Traditional perimeter-centric security tools fail to secure data in this Data-Centric manner. However, Enterprise Digital Rights Management (EDRM) technology can provide persistent, granular, centralized, Data-Centric controls that secure information wherever it goes. Simply put, EDRM security controls always stay with the data.

Right to Know

Requirement

999.308. Privacy Policy

Right to Know About Personal Information Collected, Disclosed, or Sold

- Identification of the categories of personal information the business has collected about consumers in the preceding 12 months.
- Identification of the categories of sources from which the personal information is collected.
- Identification of the business or commercial purpose for collecting or selling personal information.
- Disclosure or Sale of Personal Information
  - » Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties.
  - » For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.

999.313. Responding to Requests to Know

- A business shall use reasonable security measures when transmitting personal information to the consumer.
- If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information. If the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements outlined in Article 4.

How Seclore Can Help

Each protected file is assigned a classification, which can be managed using Seclore Digital Asset Classification (DAC) without encrypting the data. For instance, a file marked as "Confidential" may be restricted from being copied to a USB drive or emailed to external email addresses. A file labeled as "Top Secret" is encrypted immediately when it is detected.

In addition to the access controls and protection applied to the files, Seclore allows you to monitor all activities performed on the protected data, no matter where it is located. You can also revoke access to the data at any point, ensuring its secure disposal.

Moreover, Data Classification can help you identify the information assets, create a classification taxonomy, and implement the associated protection parameters assigned by the Enterprise Digital Rights Management (EDRM) solution.

EDRM can integrate with enterprise applications such as EFSS, ERP, ECM, and core banking systems. Documents downloaded from these applications can be protected by default before downloading. This Policy Federation gives the applications the capability to extend their security and governance to public networks, third-party networks, or even other countries. Thus, data protection can be incorporated into the IT infrastructure by default, ensuring that data is always kept private.

Right to Delete Information

Requirement

999.308. Privacy Policy

- Right to Request Deletion of Personal Information.
  - » An explanation that the consumer has a right to request the deletion of their personal information collected by the business.

999.313. Responding to Requests to Know and Requests to Delete

- A business shall comply with a consumer's request to delete their personal information by:
  - » Permanently and completely erasing the personal information on its existing systems except for archived or backup systems.
  - » Deidentifying the personal information; or
  - » Aggregating the consumer information.
- When responding to a Request to Delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.

How Seclore Can Help

Seclore's Data-Centric Security can govern, secure, and control your data wherever it travels – to any location, network, machine, and device. The security is information-centric and always remains in effect and locations. This allows agencies to outsource and collaborate with the confidence that their data is being used without being misused.

The data owner controls every document protected by Seclore, ensuring their ownership throughout the data life cycle.

The Seclore Risk Insights dashboard enables organizations to gain complete visibility over their sensitive data wherever it travels. Organizations can track every interaction/processing activity on a Seclore-protected digital asset anywhere in the world. They can feed this data to the enterprise SOC program (SIEM integrations) to get a holistic view of risks to the organization.

Service Providers

Requirement

999.314. Service Providers

- A service provider shall not retain, use, or disclose personal information obtained while providing services except:
  - » To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal data and comply with the written contract for services required by the CCPA.
  - » To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations
  - » To detect data security incidents or protect against fraudulent or illegal activity

How Seclore Can Help

Shared data can be protected, ensuring access only on a strictly need-to-know basis. Protected data can be shared safely and securely with EDRM while successfully mitigating third-party and outsourcing risks. Unlike other security solutions, the jurisdiction and boundary of EDRM protection is the information itself, not the network, device, or location.

With EDRM, you can now enforce your data governance policies on third parties who receive your data. After all, a legal contract does not absolve the agency of its liability towards the information.

EDRM allows you to eliminate your dependency on their security infrastructure to secure your data. You can exercise complete control over the confidential information you send to these third parties, such as vendors, partners, contractors, sub-contractors, lawyers, and auditors. After the collaboration period is over, you can remotely destroy all of your shared data. This eliminates your dependency on the third party's non-compliance with contract clause(s) related to information destruction. Thus, you can now outsource with confidence and successfully mitigate third-party risks.

Miscellaneous

Requirement	How Seclore Can Help
999.323. General Rules Regarding Verification • The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive. • The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request. • A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent unauthorized access to or deletion of a consumer's personal information. **999.324. Verification for Password-Protected Accounts** • If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the company follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themself before disclosing or deleting the consumer data.	Data sharing can be risky, which is why it's crucial to protect shared data. With EDRM, you can protect your data by ensuring that it's only accessible on a strictly need-to-know basis. This means that you can safely and securely share protected data with EDRM, mitigating any potential third-party and outsourcing risks. EDRM protects the information itself rather than just the network, device, or location. This means that you can enforce your data governance policies on third parties who receive your data. Even if there's a legal contract in place, the agency is still liable for the information it receives. By using EDRM, you can eliminate your dependency on third-party security infrastructure to secure your data. You can exercise complete control over the confidential information you send to these third parties, such as vendors, partners, contractors, sub-contractors, lawyers, and auditors. Once the collaboration period is over, you can remotely destroy all of your shared data, eliminating any dependence on the third party's non-compliance with contract clauses related to information destruction. This allows you to outsource with confidence and successfully mitigate third-party risks. EDRM also monitors all activities performed by all users in the system. Access levels to sensitive information can be modified or revoked for any user by the information owner, from any location. In addition to standard details such as username, type of access, and date and time of information access, forensic information such as file path, current and original file name, machine name, and IP address are also captured.

Protect Your Information – Anytime, Anywhere

Unauthorized access to personal data are punishable by the law. CCPA violation can cost companies up to $7,500 per violation. In the case of data theft or misuse, companies are liable for fines of up to $750 per consumer per accident. The bill, therefore, is likely to push businesses to protect the data itself, whether at rest or at transit, which encompasses controlling access and usage and deleting any information that has been collected and is not essential.

CCPA compliance can be twisted and confusing when cybersecurity is involved. Security professionals familiar with data security can help strategize the Data-Centric Security aspects like:

- Data identification or classification
- Implement controls to protect data
- Define policies and continuously monitor the usage of personal information, including third-party access and supply chain risk management.

Seclore embeds security controls into the data itself to protect, revocable, and auditable regardless of the device, network, or application – for every digital asset, wherever it goes.

With Seclore, financial services firms can:

- Securely collaborate internally and externally on a need-to-know basis.
- Gain visibility of where and how your sensitive data is used.
- Reduce incident costs, driving down the impact and containment.
- Mitigate risks from human error, control gaps, or malicious intent.
- Achieve compliance with internal and regulatory policies, standards, or requirements.
- Make data security independent from infrastructure security.

Learn more about how Seclore can help your organization to become CCPA-compliant

Ask for Demo

SECLORE™

About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our Data-Centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing.

Visit **www.seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054