SecurityFirst™
Protecting Critical Data

DataKeep™

Supporting the Data Protection requirements in CCPA

The California Consumer Protection Act (CCPA)

The CCPA builds upon existing California data security laws that provide for the confidentiality of personal information and require a business or person that suffers a breach of personal information to disclose that breach. The CCPA itself focuses on the online collection and management of consumer personal data for business applications.

The CCPA furthers Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

- The Right of Californians to know what personal information is being collected about them
- The Right of Californians to know whether their personal information is sold or disclosed and to whom
- The Right of Californians to say no to the sale of personal information
- The Right of Californians to access their personal information
- The Right of Californians to equal service and price, even if they exercise their privacy rights
- The Right of Californians to request the deletion of the collected personal information

Beginning January 1, 2020, the law will grant a consumer a right to request a business to disclose what specific personal information they have, the purpose for which it was collected and who the data has been shared with. While the CCPA doesn’t specifically define how to protect personal data in support of these privacy rights, it does create the right for a citizen to pursue legal action and penalties against businesses for the *breach* of a consumer’s nonencrypted or nonredacted personal information, as currently defined in California law.

CCPA – Section 1798.150-a

Any consumer whose *nonencrypted or nonredacted personal information* is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action through the State of California Attorney General’s office.

California Civil Code Section 1798.81.5 (2016)

Businesses shall ensure that personal information about California residents is protected by implementing and maintaining reasonable security procedures and practices to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

California Civil Code Section 1798.82 (2016)

A person or business that conducts business in California, and that owns or licenses data that includes personal information, shall disclose a breach following discovery or notification of the breach to a resident of California whose *unencrypted personal information* was, or is reasonably believed to have been, acquired by an unauthorized person, or,

whose *encrypted personal* information was, or is reasonably believed to have been, acquired by an unauthorized person and *the encryption key* or security credential was, or is reasonably believed to have been, acquired by an unauthorized person

How DataKeep from SecurityFirst helps support CCPA

While the CCPA takes effect January 1, 2020, businesses should already have data security procedures in place under existing law. DataKeep can help organizations immediately protect personal data, while they develop and implement processes to support the provisions in the CCPA. DataKeep's easy-to-use, agent-based deployment model helps protect sensitive data-at-rest wherever it resides -- server managed storage, network file systems or in object storage. It provides a broad range of protection that includes data access management, integrated key management, sophisticated encryption and event logging, that combine to deliver the scalability and flexibility to help protect the most sensitive workloads. DataKeep provides the following capabilities to support California data protection requirements.

- Encrypt personal data
- Manage access to personal data (by role or process)
- Audit data access requests / denials for encrypted personal data
- Provide data erasure through cryptographic shredding
- RESTful API to support Security by Design and Security by Default requirements

The CCPA defines what must be done to protect the personal data of Californians, as well as the impact of noncompliance. DataKeep helps support the rights of California consumers to exercise control over their personal information by helping businesses safeguard against the misuse of their personal information.

Section	Brief Description – California Civil Code	Policy	Log/Audit	Encryption
1798.150-a	Right to civil action for a breach of personal data	✓	✓	✓
1798.81.5	Implement and maintain security procedures / practices	✓	✓	✓
1798.82	Breach notification of unencrypted personal data	✓	✓	✓

While January 1, 2020 is an important date for the CCPA, current law states that businesses handling the personal information of Californian consumers should already have security in place to protect sensitive data. DataKeep encryption and access policies specifically help meet the requirements for implementing and maintaining reasonable security procedures and practices, as well as help you avoid costly fines and reporting requirements, all while supporting an individual's personal data rights.

FOR MORE INFORMATION PLEASE VISIT THE SECURITYFIRST DATAKEEP WEBPAGE

About SecurityFirst™

SecurityFirst delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.