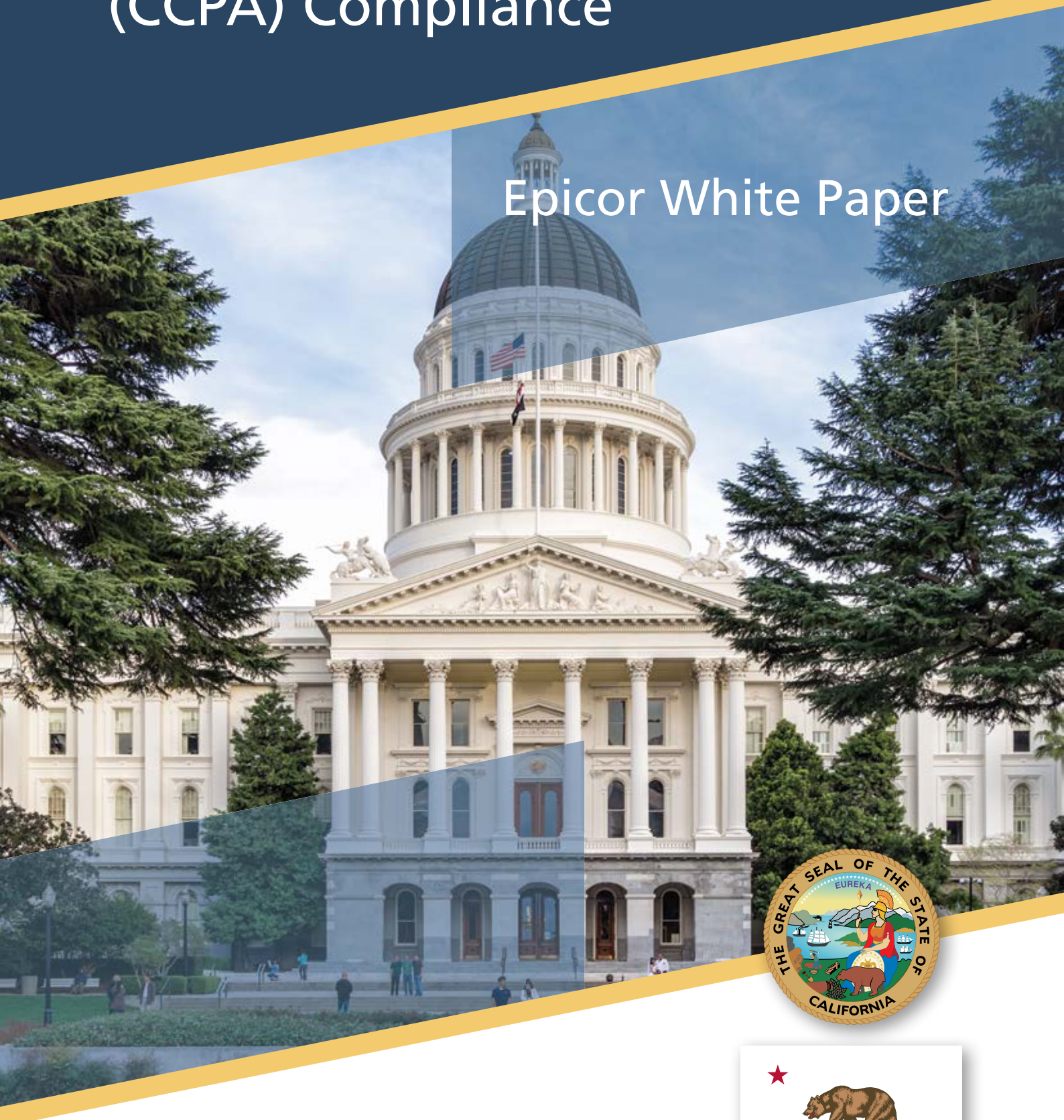
How Epicor® Helps With California Consumer Privacy Act (CCPA) Compliance

Epicor White Paper



EPICOR®

Introduction

The California Consumer Privacy Act (CCPA) entered into effect on January 1, 2020. The law introduces new privacy rights for consumers and requires in-scope companies doing business in the State of California to enhance their consumer data protection processes.

The new rights given to California consumers are similar to the rights provided by the General Data Protection Regulation (GDPR) in the European Union (EU). The CCPA also subjects non-compliant businesses to fines, class-action lawsuits, and legal action.

The CCPA requires all in-scope companies to comply with requests from individuals to provide access to the requestor's personal information, describe how it is used, prevent further sharing, or even delete personal information under certain circumstances.

All in-scope companies doing business in California will need to modify their operations, policies, and procedures to comply with CCPA.

This document focuses on the CCPA requirements and how Epicor products can help impacted businesses remain compliant and meet the obligations of the CCPA. It provides information on many standard tools and features that can help you respond to the new consumer rights on requesting access or deleting personal information.

Who Is Impacted by the CCPA?

The CCPA applies to for-profit companies that gather personal information from California residents and meet one of the following three criteria:

- Have at least $25 million annual gross revenue
- Annually receive the personal information of 50,000 or more consumer records, households, or devices
- Earn at least 50% of the annual revenue from selling California residents' personal information

Companies must evaluate their personal information management processes and amend noncompliant practices by January 1, 2020.

What Does the CCPA Provide?

The CCPA ensures consumers have the right to:

- Access (Right to Know) their personal information that is stored by the business
- Delete any personal information under certain circumstances
- Opt out of selling personal information to third parties
- Receive the same products or services when exercising the above rights

Businesses must provide at least two ways to their consumers to exercise their rights:

- Toll free phone call
- Web-based form

Penalties

Businesses have 45 days to comply with the CCPA after a noticed violation. Civil penalties may range from $2,500 to $7,500 per violation.

What Do I Need to Think About Regarding CCPA?

Your systems and software are important considerations when looking to meet the requirements of the CCPA and should be part of adopting a robust, organization-wide approach to CCPA compliance. Much of what is required to meet CCPA standards is process related, and organizations should consider the following steps:

- Identify the personal information you have, where it resides, and how it's used
- Identify any third-party organizations that have access to personal information of consumers and confirm if personal information is sold or shared with third parties and the purpose of such sharing
- Implement robust governance on how personal information is accessed and used
- Ensure appropriate security controls are in place to protect the confidentiality, integrity, and availability of personal information
- Respond to requests from individuals asserting their rights—for example, requests to provide an individual with a copy of their personal information stored with the organization
- Maintain documentation of compliance—including records of processing activities and responses to requests from individuals for at least two years

What Will Epicor Provide Me to Help My Organization Comply With CCPA Requirements?

Epicor is committed to data security and privacy for us and our customers around the world.

CCPA compliance is a shared responsibility between Epicor and our customers. Epicor products and services can contribute to your CCPA compliance when they process personal information. For example, our products and services provide functionality to help meet individual rights requests.

Products and services—including Epicor hosted solutions—have security measures and access controls. Organizations can incorporate the functionality and procedures in Epicor products and services to help them meet their CCPA compliance obligations.

Epicor is further committed to assisting our customers in complying with the various requirements applicable to their business—including CCPA. Thus, Epicor continues to monitor changing laws and best practices to help enhance our products, contracts, and documentation to help support our customers' compliance with legal obligations—including the CCPA.

Individual Rights

Request for access

Access requests that you may receive from an individual can be actioned with the help of system reports, dashboards, or product-dependent, user-customizable queries.

Request for deletion

Deleting an individual's personal information may be achieved using standard delete functionality. In some cases, historical data may require direct database access.

Please note that it's important that a full evaluation is undertaken for any other legal requirements that may prohibit you from deleting the personal information.

Controlling and Managing Access

In addition to an individual's rights for access to information, the CCPA is intended to ensure that personal information is appropriately managed and protected. Epicor products have several standard capabilities that will help you meet your obligations under the CCPA.

An important step when evaluating readiness and compliance with the CCPA is to ensure that you are appropriately managing security and access to your systems. Epicor products provide a variety of standard security options—with the flexibility to manage and control access using industry standard tools and capabilities—as well as application access restriction tools.

Epicor products provide comprehensive management of user, process, and data security settings so that you can restrict data and application accessibility as needed. There is also an option to use Microsoft® Windows® Authentication to support a Windows single-sign-on and password policy for selected products and versions. Epicor products provide the following security management capabilities as standard:

Access security

This verifies that whomever—or whatever—is attempting to access the application server is permitted to do so. This includes login security to the menu system either by entry of user ID and password or via Windows Authentication, session security—same as login security—for application components that are run directly from the desktop or other non-menu areas, and services security through the Epicor products to help ensure that an external system may access the business logic when allowed.

Business security

This ensures that individual users and groups of users only have access to the business functions and data that they are permitted to view or update.

Application security

This helps to ensure that the business logic protects the underlying database from corruption by always ensuring that an update is valid—regardless of the source of the transaction. This is necessary in a service-based architecture since the business logic can be called from many environments—including a desktop application, external web services, browser-based clients, and other smart devices.

Database access

You can manage user permissions and access to the Server to ensure this core system maintains its data integrity. Most Epicor product users do not need security access to the database, and you should only grant permissions to users who will help manage them.

For more information on controlling access and setting up users and database security, please refer to the System Administration Guide relevant to your Epicor product.

User security (authentication)

Controlling access to your business applications is one of the primary ways you can take steps to protect data—including personal information. When you authenticate the identity of users attempting to log in or call the application, you help prevent unwanted or malicious access. It is important that you evaluate and manage user access to Epicor products as part of your organization's general security policy.

Authorization (interface) security

Managing who has access to application functions and data is an important part of ensuring corporate governance and security. It also helps you meet your obligations under the CCPA. The standard comprehensive functionality built into the Epicor products allows you to manage and control access and helps manage which users need or do not need access to data and information within the application.

You can easily control and manage security. The Epicor products offer the flexibility to manage both group and individual user access to functional areas, individual programs, forms, or even specific fields. For example, you may want to prevent system-wide access to CRM programs and data to ensure that only authorized users can access personal information held within the contact management modules. You can use the security tools to only permit access to the members of the sales and marketing team security group and further limit the ability to change data to a subset of the sales and marketing team security group.

To ensure that you can effectively govern and manage access to sensitive or personal information, the authorization security in Epicor products provides you with the flexibility to:

- Prevent programs from being displayed for specific security groups and users
- Block access to a program or program function—like updating records—from wherever it can be launched
- Run standard security reports to display current access rights and review user activity

For more information on setting up user security, please refer to the System Administration Guide.

In addition, logs and audit capabilities ensure that any updates and changes can be traced, as well as provide ongoing monitoring and tracking.

Auditing and Reporting

Epicor products can help you manage and track the activities and data within your system using standard reporting and auditing capabilities. These logs and audit files will help you review processing from a number of application areas that may involve the capturing or changing of personal information. Examples include:

Change Logs

These allow you to view changes made to certain records in the database and can support you if you need to track changes made to personal information within your application. The Change Log can provide you with a complete list of changes made to certain parts of the systems.

Audit Logs

Audit Logs provide a permanent audit trail of access and changes within the system. By using the Audit Logs, you can validate what is happening and monitor the preventive controls and processes intended to help ensure transactional validity. The combination of preventive controls with continuous monitoring gives executives and auditors the confidence to attest to financial results and associated IT controls. Data Audit Logs help you meet the compliance required under the CCPA and other regulations such as FDA Title 21, CFR Part 11, HIPAA, Basel II, and more

System Activity Logs

The System Activity Log helps you easily navigate activities and monitor who has accessed the system. It also lets you monitor login failures, which can be useful to check for any potential hacking activity. For more information on the Logs available, please refer to the System Administration Guide.

Finding More Information

Epicor is committed to helping our customers comply with the various requirements applicable to their business—including the CCPA and GDPR. More information on the CCPA and GDPR can be found on Epicor.com. In addition, product-specific guidance is being prepared and will be made available via the EpicCare knowledge base.

This document is a commentary on the California Consumer Privacy Act (CCPA) and is intended to be a concise and simplified guide for organizations. The information contained in this document is not exhaustive and is for general guidance purposes only. It should not be relied upon as legal advice or to determine how the CCPA might apply to you and your company. We encourage you to work with legal counsel to discuss the CCPA, how it applies specifically to your organization, and how best to ensure ongoing compliance. If you would like more information about the CCPA, you can access the State of California Department of Justice, California Consumer Privacy Act (CCPA) website at https://oag.ca.gov/privacy/ccpa.

About Epicor

Epicor Software Corporation drives business growth. We provide flexible, industry-specific software designed to fit the precise needs of our manufacturing, distribution, retail, and service industry customers. More than 45 years of experience with our customers' unique business processes and operational requirements are built into every solution—in the cloud or on premises. With this deep understanding of your industry, Epicor solutions dramatically improve performance and profitability while easing complexity so you can focus on growth. For more information, connect with Epicor or visit www.epicor.com.

Contact us today info@epicor.com www.epicor.com