eBOOK

How to Comply with CCPA

SailPoint

The California Consumer Privacy Act (CCPA) was passed in June of 2018 in the wake of backlash from numerous high-profile data breaches and incidents in which data brokers and marketing agencies mishandled consumers' personal data. In effect as of January 2020, CCPA is the first law of its kind to bring European-style data privacy regulations to the United States. It serves as a harbinger of new consumer protections across the nation. Additional states that have passed privacy regulations include Vermont, Colorado, and New Jersey, while as of June 2019 bills are pending in the states of New York and Washington, with more likely to follow. Congress is also weighing a number of privacy proposals on the national level. While the specifics vary, all of these acts share the goal of protecting consumer information.

The CCPA in particular impacts for-profit businesses with consumers in California that meet one of three requirements: they must have more than $25 million in annual revenues, possess personal information for more than 50,000 California residents, or get more than half of their annual revenues from the sale of personal information.

Key mandates include rules that give consumers control over their personal information. This control includes the right for consumers to access all data about them, opt out of sales of their personal data, delete their data, and move their data to another service provider. The Act includes very broad definitions of what it considers personally identifiable information (PII). CCPA defines PII as any type of information that can create a profile of the customer and identify a consumer or household, such as social security numbers, driver's license numbers, records of purchase history, internet activities, physical characteristics, and much more. Fines and penalties for failure to comply with CCPA are steep: $7,500 for each intentional violation of the Act and $100-$700 in statutory damages per incident, per consumer in the event of a data breach.

If your organization has been diligent about addressing existing regulations, such as GDPR, HIPAA, or SOX, you already have a good foundation. Still, with the passage of CCPA, it's important to revisit your existing architecture to ensure you can confidently comply. You need to be able to identify the data you store about your consumers to address customer requests regarding their information. You must also ensure the protection of that consumer data.

For many years, enterprises focused on securing the network perimeter as a means of protecting their applications and data; however, organizations have seen a growing number of data breaches occurring due to compromised credentials, malicious insider behavior, and the proliferation of sensitive data being saved in ungoverned locations. The way to mitigate these risks is to implement tight governance of the identities of employees, contractors, and partners within your organization and control the data, applications, and systems they're allowed to access.

5 Steps to CCPA Compliance

To comply with CCPA, focus on these identity governance priorities: locating sensitive data, minimizing the data you store, understanding who has access to it, controlling access, and maintaining compliance through automation.

1

Identify Your Sensitive Data

To protect customer data, you must first know where it is. The data may be in structured systems, such as applications or databases, or it may reside as unstructured data, such as Excel spreadsheets or PDF reports located on file systems, collaboration portals, such as SharePoint, or even in cloud storage systems such as Box or Microsoft OneDrive. By knowing where data is located, you can act on customer requests for it in a timely fashion. Knowing where your data resides also allows you to assess your vulnerabilities for data breaches so you can prioritize and address your most immediate security needs.

2

Minimize the Data You Store

Security experts advise organizations to lower their risk of data breaches by adhering to data minimization practices. Data minimization means that instead of saving all the data you gather about consumers, you should identify and remove data that you don't need for a particular business purpose. By removing unnecessary data, you reduce your vulnerability to attack.

3

Identify Who Has Access

Before you can safeguard data from breaches by unauthorized users, you need to understand who should have access to customer data and reconcile it with who actually does have access. This should be an ongoing process, not a one-time effort. Make sure to include all applications and file storage platforms (both those running on-premises and in the cloud) where you are actively storing customer data.

4

Strictly Control Access

In organizations that rely on traditional perimeter security, once a user logs into the network, they can access any system, application or device on it. As a result, a hacker that steals an end user's access privileges through, say, a phishing scheme, can walk into the front door of your network and move to whatever data, applications or systems they want. To prevent such unrestricted movement, you should give users access to only the minimum resources they need (least privilege). You need to build a governance model that aligns access to applications and data based on business need. A comprehensive identity governance program can ensure users are not able to attain improper access.

5

Maintain Compliance

Keeping control over who can access your data must be an ongoing task. Employees, partners, contractors and suppliers that need data access come and go, and your ability to provision appropriate controls needs to track with them. Comprehensive identity governance solutions can automate the provisioning and deprovisioning processes so you can maintain CCPA compliance without impacting your overall business operations. Additionally, solutions that use artificial intelligence and machine learning can provide recommendations to help you make more intelligent decisions about who should have what access to data or whether that access should be taken away. Automated review and auditing of user access ensures you remain in compliance.

A Holistic Identity Governance Strategy

With a comprehensive identity governance solution that spans applications and data stored in files, your organization can gain full visibility into what data you have as well as who has access to what and how they're using that access. This will help you address consumer requests, better protect sensitive data, and make the right decisions.

At first, you may feel overwhelmed by the requirements of CCPA, especially considering the financial ramifications of non-compliance. However, leveraging identity governance at the core of your security strategy to protect access to customer data can go a long way toward helping your organization comply with CCPA requirements, and mitigate the risk of a data breach and the resulting penalties that may occur.

EB1314-1907