SailPoint

SOLUTION BRIEF

Are You Prepared to **Comply with CCPA?**

If you're a for-profit business with customers in California, you may soon have to comply with the new California Consumer Privacy Act (CCPA). In effect as of January 1, 2020, CCPA involves a set of requirements to ensure the privacy and protection of personal data that businesses hold about customers who live in the state. The law applies to your business if you meet one of three requirements: you have more than $25 million in annual revenues, you process personal information for more than 50,000 California residents or you get more than half your annual revenues from the sale of personal information.

Some key mandates enacted by CCPA include:

- Rules that give consumers control over their personal information, including the right to access all data collected about them, opt out of sales of their personal data, delete their data, and move their data to another service provider.
- Broad definitions of what is considered 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.
- Significant financial penalties of up to $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.

Meeting these challenges requires a holistic approach focused as much on process and planning as technology. SailPoint identity governance supports CCPA compliance by enabling your organization to confidently identify personal data you have stored across the enterprise, assess risk of improper access, strengthen governance controls, and automate access monitoring and auditing processes. With visibility into what personal data you store and its location, you can quickly address

customer requests to view or take actions regarding their personal information. You can also determine who within your organization has access to what data and how that access is leveraged to improve the security posture across your enterprise. With a foundation of identity governance, not only can you comply with CCPA, you can stand ready to address other regulations.

CCPA compliance is demanding and the potential financial and reputational impact is significant. You should take a comprehensive approach that addresses three key challenges:

Assess: Gain Visibility into What PII You Hold and Who Is Responsible for Managing It

CCPA grants consumers residing in California a high degree of control over the personal information that businesses keep about them. Consumers will have the right to find out what data you store about them, request access to that information, control whether you can sell that data, or ask you to delete their data or transfer it to another service provider (i.e., provide data portability). The data that CCPA defines as personal, and thus subject to these customer demands, is extensive. It consists of any information that can identify an individual and includes everything from social security and driver's license numbers to records of purchase history to internet activities or physical characteristics.

Addressing customer demands for access to their personal information means your organization must identify and classify all of the PII you have on hand as well as understand who within your company owns and accesses that data. SailPoint gives you visibility into the data you have stored, who within your organization is responsible for maintaining that data and who is actually accessing it. By automating the discovery and classification of personal data, identifying the right data owners and monitoring user access, SailPoint enables you to:

- Identify and classify what personal data you have, its type, as well as where and how it's stored (SharePoint, Box, NAS, or other repository) to address customer requests and assess risk
- Determine the internal employees who are the stewards of this data to ensure accountability for its protection
- Validate user access in accordance with compliance requirements to prevent unauthorized access
- Easily monitor how users are accessing data in a dashboard and get alerted to policy violations to quickly identify suspicious activity

Not only does classifying data and assigning responsibility for it allow you to protect consumer data, it also enables you to assess risk so you can prioritize and address your most immediate security needs. Organizations that fail to actively assign accountability to data owners and understand who should have access – and just as important, who actually has access – are leaving themselves open to data breaches and regulatory penalties.

Control: Reduce the Risk of Data Breaches

CCPA provides a right of action for data breaches that result from violations of an organization's duty to implement and maintain reasonable security procedures and practices to protect consumers' personal information. Businesses are subject to penalties if hackers access, exfiltrate, steal or disclose unencrypted or non-redacted consumer data due to lack of safeguards.

Security experts typically advise businesses to lower risk of data breaches by adhering to security best practices such as data minimization and least privilege access. Data minimization means that instead of saving all the data you collect about consumers, you should identify and remove data that is not required for a particular business purpose. Jettisoning unnecessary data saves your company from having to store mounds of useless data while reducing your vulnerability to cybersecurity breaches.

Least privilege requires organizations to give users access only to the resources they need to do their jobs. In organizations that rely on traditional perimeter security, once a user logs onto the network, they can access any system, application or device on it. Thus, a hacker that steals an end user's access privileges through nefarious means, such as phishing, can walk in the front door to the network and move anywhere they want through it. Least privilege access prevents such unrestricted movement, strictly limiting where users can go on the network.

SailPoint enables organizations to reduce unnecessary data and adhere to least privilege standards by:

- Identifying stale data or data stored in inappropriate locations that should be remediated
- Limiting access to authorized users and detecting and revoking inappropriate or unauthorized access rights to minimize the risk of abuse of account privileges
- Validating user access on a regular basis to demonstrate compliance
- Identifying data that has open access or does not have a data owner so you can take steps to control access
- Requiring a manager or data owner to approve all access changes and giving them a complete user profile as context to ensure they make the right access decisions

SailPoint makes it easy to ensure that you retain only the data required by regulation or policy. SailPoint also empowers your organization to implement workflows to ensure appropriate business stakeholders review, assess and approve access. Removing unwanted or unneeded access to systems, applications, and data minimizes potential abuse of account privileges.

Automate: Maintain Complince While Improving Efficiency

As you secure your customers' personal data, automated provisioning and deprovisioning of access enables you to tighten your security controls to maintain CCPA compliance without impacting your overall business operations. Automated provisioning ensures that access to personal data is granted on a need-to-know basis and provides approval workflow, policy checking, and auditing – all in an efficient manner.

Leveraging artificial intelligence (AI) and machine learning can also help your organization better manage risk while scaling to keep up with a growing and increasingly complex set of applications, data, and users. With AI and machine learning, you can make intelligent automated business decisions based on recommendations of whether or not a user should be granted access. In addition, these insights can help anticipate user access needs, identify risky access, and support continuous compliance.

SailPoint improves compliance with policies designed to strengthen security through the ability to:

- Get AI-driven recommendations to help you decide if access should be added or taken away
- Log all access requests and actions by approvers, providing a complete, auditable record of who requested access to which systems and who approved or denied the request
- Create detailed reports to assess and provide proof of CCPA compliance
- Automatically trigger a validation of access for risky users and access
- Get automatic notifications of unusual access patterns that might signal a breach or potential risk

Your organization can improve the efficiency with which you implement compliance by using SailPoint to:

- Flag high-risk access requests to managers and automate low risk requests
- Rapidly respond to auditor requests using historical identity data to investigate and diagnose user access
- React to risk in real-time with machine learning that evolves access recommendations in accordance with changing compliance and security needs
- Assign the rightful data owner (with the most knowledge about the data) to manage access, removing the burden from IT
- Automatically detect job changes such as transfers or terminations and launch the appropriate workflow to remove or change access privileges

Your Call to Action

CCPA creates an enormous challenge for any organization that conducts business with California consumers in any capacity. Placing identity governance at the core of your security strategy can give your organization the means to safeguard access to consumer data and mitigate the risks you face from a data breach. Solving CCPA challenges means organizations need to develop a complete picture of where their data resides, whether it is in a database or a spreadsheet, on a portal or in the cloud. With repositories such as file shares and Box, your organization can increase its visibility into what data you have, who has access to what, and how access is being utilized. Meeting the demands of CCPA requires a holistic approach that includes planning and process, as well as technology. SailPoint stands ready to provide your organization with the tools necessary to meet and solve the complex challenges CCPA compliance presents.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1313-1907