

ManageEngine[®]
Log360

A simple guide to the
**CALIFORNIA
CONSUMER
PRIVACY
ACT 2018**



Table of Contents

The need for a strong privacy law in the United States	1
Applicability of the CCPA	2
Personal information under the CCPA	3
The rights of consumers	4
Non-compliance leads to penalties	5
Action plans for adhering to the CCPA	6
Meeting CCPA compliance requirements with ManageEngine Log360	8
About ManageEngine	10
Endnotes	11

The need for a strong privacy law in the **United States**

As things stand today, companies are well within their rights to monitor Americans' online and offline behavior, collect data, translate this data into insightful information, and use this information for turning a profit. And they can do all of this without the consumers' permission or knowledge.

This means that consumers in the United States have no control over their personal data, and there is no repercussions for companies that misuse this data. This is why many US citizens want to know how their data is being used.

As if this wasn't bad enough, with the evolution of the digital age, people's online footprints are everywhere. Companies want information on consumers and numerous organizations with that information are more than willing to provide it at a cost. At the same time, attackers are keen to intercept or steal this data for their own financial gain. There were a record 447 million exposed records from 1,244 data breaches in the United States in 2018.¹ This figure has been steadily rising over the years, leaving consumers feeling wary about sharing their data with companies. Businesses need to take strong measures to safeguard both themselves and their customers.

Apple CEO Tim Cook wrote in an article in Time Magazine about four principles that should drive legislation.²

"First, the right to have personal data minimized. Companies should challenge themselves to strip identifying information from customer data or avoid collecting it in the first place. Second, the right to knowledge—to know what data is being collected and why. Third, the right to access. Companies should make it easy for you to access, correct and delete your personal data. And fourth, the right to data security, without which trust is impossible."

- **Tim Cook, CEO of Apple, January 2019**

Americans need a law that will provide transparency into how their data is being used and what for. In addition, this law needs to hold businesses accountable when they fail to protect themselves from data breaches and their consumers from identity theft.

The California Consumer Privacy Act (CCPA), which will go into effect on January 1, 2020, aims to do just this within the state of California. It's the first law of its kind in the US, and it may lead to other states following suit quickly. It could even be a precursor to a federal law.

This guide will detail the main requirements of the CCPA, and what these mean for organizations. Furthermore, the guide will also look at steps that organizations should take to comply with the CCPA. And finally, we'll take a look at how Log360—ManageEngine's integrated SIEM solution—can help companies become compliant.

Disclaimer: Please note that this guide is for informational purposes only, and do not constitute any legal advice. ManageEngine does not provide any legal advice. All information provided in this guide should be used at your own risk, and we do not provide any warranty on the legal effect or completeness of the information. Please also note that more updates to the CCPA may happen in the months ahead, and this could lead to amendments of the various clauses.

Applicability of the CCPA

The CCPA applies to all for-profit organizations that do business in California and satisfy any of the following three criteria:

1. The organization has an annual revenue of \$25 million or more.
2. The organization buys, receives, sells, or shares personal information of 50,000 or more consumers, households, or devices in California annually.
3. The organization derives at least 50 percent of its annual revenue from selling California consumers' personal information.

Organizations that already need to adhere to regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Driver's Privacy Protection Act (DPPA) are exempt from the CCPA. However, there could be divisions within these companies that do not need to comply with these regulations and are therefore required to adhere to the CCPA. Figure 1 below shows the types of organizations the CCPA applies to.

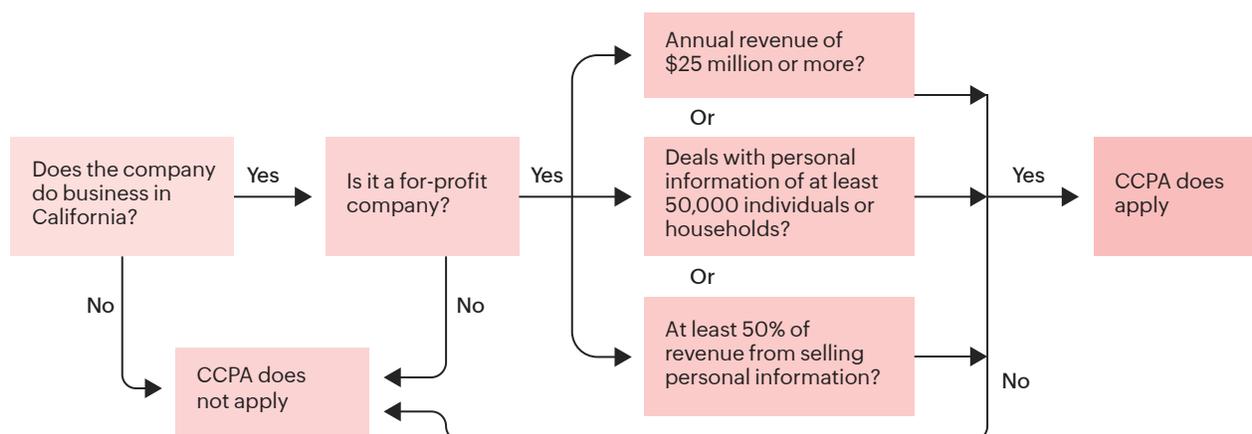


Figure 1: Applicability of the CCPA

Personal information under the **CCPA**

According to Clause 1798.140(o)(1) of the CCPA, personal information is information that can be used directly or indirectly to identify any consumer or household. It includes the following:

1. Identifiers such as name, alias, postal address, unique personal identifier, IP address, email address, account name, Social Security number, drivers license number, and passport number.
2. Commercial information, such as records of personal property, products or services purchased, or other purchase histories or tendencies.
3. Biometric information such as fingerprint, palm print, face recognition, and DNA.
4. Internet activity information such as browsing history, search history, online advertisement interaction history, and geolocation.
5. Audio, electronic, visual, thermal, olfactory, or other information that could be obtained from surveillance cameras and other devices.
6. Profession and education-related information that is not publically available.
7. Inferences drawn from any of the above to create a profile about a consumer reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Organizations required to adhere to the CCPA have to ensure that no personal information gets into the wrong hands. Furthermore, they have to strictly enforce measures to safeguard the rights of consumers to whom the data belongs.

The rights of consumers

Consumers will have several new privacy rights under the CCPA.³ These rights will give people control over their own data.

-  **1. Right to information security:** Consumers will have the right to sue a company if their data was stolen from the company due to a data breach. The company will be held liable if it's unable to prove that adequate measures were put in place to protect the stolen data.
-  **2. Right to access:** Consumers will have the right to know all the data collected about them by a business. They can request this information from companies up to twice a year, free of charge.
-  **3. Right to say no:** They will have the right to say “no” to the sale of their information.
-  **4. Right to delete:** Consumers can ask companies to delete all or part of the data they have collected. This is often referred to as the “right to be forgotten.”
-  **5. Right to non-discrimination:** A company cannot discriminate against consumers on the basis of data (or lack thereof) collected on them. This also holds true if a consumer asks the company to not sell their personal information to a third party. The same prices and levels of services must be provided by companies to consumers who demand these restrictions.
-  **6. Right to be informed:** Prior to data collection, consumers have the right to know the business purpose of data collection and what data will be collected. They also have the right to know about any third party that receives or might receive any shared data.
-  **7. Right to opt out or opt in:** Consumers aged 16 years and above have the right to opt out of the sale of personal information. Consumers aged between 13 and 16 years have the right to opt in for this. And consumers who are below 13 years of age need parental consent to opt in.

Figure 2 shows the different rights consumers have under the CCPA.



Figure 2: Rights of consumers under the CCPA

Failure to protect the rights of consumers will make a company liable for penalties. Consumers can sue the defaulting company, and the California Attorney General can levy fines.

Non-compliance leads to **penalties**

If any organization fails to adhere to the CCPA, penalties may be imposed on them. Let's take a look at some sample scenarios under the CCPA:

1. In case of a data breach where a consumer's information is stolen, the consumer can sue the company that collected the data. However, it must be proved that the company did not have adequate measures in place to stop such an attack. According to Clause 1798.150(a)(1):

"If a consumer's data 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."

The consumer can sue the company for an amount of at least \$100 and no greater than \$750 per incident; or for actual damages, whichever is greater.

2. For violations other than a data breach (i.e., their data has not been stolen or leaked into the wrong hands), consumers can issue a 30-day written notice identifying the specific provisions of the CCPA that have allegedly been or are being violated; after 30 days, if no action is taken to rectify the situation, the consumer can sue the company.

For example, if a consumer requests a list of all the data a company has stored on them, and the company fails to provide it within 30 days, the consumer can proceed with civil action. Consumers may also take civil action if they request that a company delete the stored data it has on them, and it fails to do so.

If within 30 days the business addresses the violation and provides the consumer with a written statement that the violations have been fixed and that no further violations shall occur, no action for damages may be initiated against the company (1798.150(b)(1)).

3. The California Attorney General can enforce the CCPA on any company that violates the rules with civil fines up to \$7,500 for each willful violation (1798.155(b)).

Action plans for adhering to the **CCPA**

By January 1, 2020, companies that need to adhere to the CCPA need several measures in place:

1. **Develop a privacy notice:** Draft a proper privacy notice that can be used to obtain explicit consent from consumers to process their personal data. This notice should clearly explain what data is collected, for what purpose it's collected, and how it will be used. The notice should be shared with consumers at the time of data collection.
2. **Respond quickly to access requests:** Document data processing techniques so that consumers can be provided with information as and when they exercise their right to access their own data. Companies should also have procedures in place to receive, respond to, and process access requests efficiently.
3. **Make consumer data portable:** Consumers may need the data they request to be easily transferable from one environment to another. They may also want to move or copy their data, and organizations have to support this.
4. **Respond quickly to deletion requests:** If a consumer requests that their personal data be deleted for whatever reason (i.e., they are exercising their right to be forgotten), the

company must quickly comply with this request. For this, they need to have a mechanism in place to identify and isolate the data, and subsequently delete it. Procedures should also be in place to ensure deletion requests are responded to efficiently. Figure 3 shows how a company could do this.

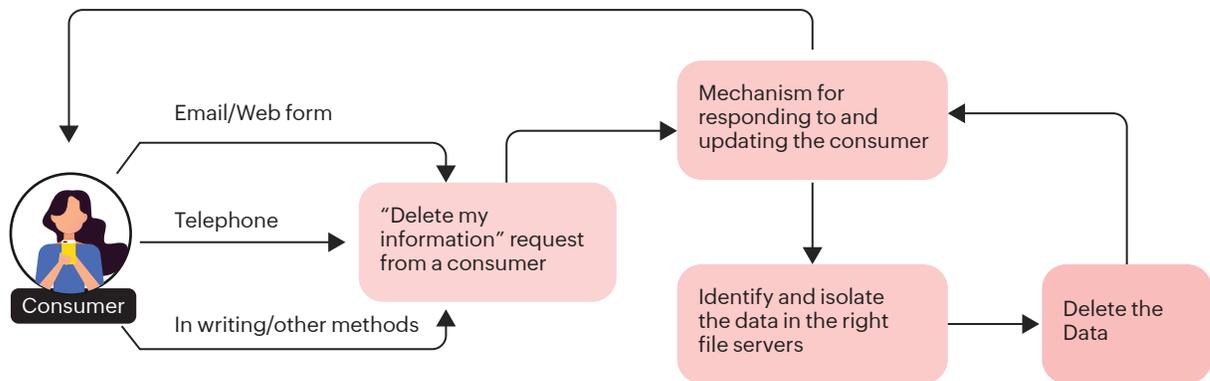


Figure 3: Responding to a "right to be forgotten" request

5. **Ensure compliance to opt-out and opt-in conditions:** Companies need to be aware that children below 13 years of age need parental consent for the sale of any personal information. Children between 13 and 16 years of age have the right to opt in for the sale of any personal information. People aged 16 and above have the right to opt out of the sale of their personal information. All of this must be made clear to consumers at the time of data collection itself. Consent and web forms need to be designed in a way that can meet all these conditions.
6. **Appoint people responsible for data security:** If necessary, companies need to appoint officials who can monitor the data processes and who are accountable for the security of personal and sensitive data.
7. **Document all information related to data processing:** Companies need to clearly document what kind of personal data is being collected; how it is collected, used, transmitted, and stored; and how the collected data is protected from disclosure at each step.
8. **Constantly monitor data access:** Companies should continuously monitor the files and folders where the data is stored. They should be able to identify who accessed the data, when they accessed the data, and who has access to the data at any given time. They should also be able to detect any unauthorized access attempt. Furthermore, the stored data should be encrypted and tamperproof.
9. **Store data only for the required time:** Companies need to maintain a record of how long data is to be stored. When data has served its purpose, companies will be required to delete it.

9. **Frame tight security policies to defend against data breaches:** Companies need to monitor their networks to detect any anomalies, track user behaviors (especially those of privileged users), audit sensitive files and folders, and be alerted in real time upon a breach or warning signs of a breach.
10. **Prove that tight security is in place:** Companies will be held liable if they fail to put adequate security measures in place to defend themselves against breaches. Therefore, companies need to have the right reports, audit trails, and log history to prove that security was always in place.

Meeting CCPA compliance requirements with **ManageEngine Log360**

Log360 is a comprehensive SIEM solution that helps enterprises detect data breaches, ensure the security of stored personal data, and track each and every access to personal data. It also tracks critical changes to the files and folders where personal data is stored

Let's take a closer look at some of Log360's features that can help organizations adhere to CCPA regulations:

Real-time Active Directory auditing:

Log360 aggregates security log data from different domain controllers to centralize Active Directory audit information, placing it all in a single location. Administrators can track important changes made to AD objects, including users, computers, groups, OUs, and GPOs, and get real-time alerts about critical changes. If access permissions are changed and privileges are escalated in Active Directory, administrators will receive real-time notifications and can investigate if it's a threat.

Real-time network device auditing:

Log360 can analyze syslogs generated by your network perimeter devices, including routers, switches, firewalls, and IDS/IPS, in real-time. Administrators can track configuration changes—such as rule modifications, links that are up or down, denied and accepted firewall connections, and IDS/IPS alerts—all from a single console. This helps with mitigating data breach risks that originate outside the business' network.

Discover data:

With Log360, administrators can find, analyze, and track sensitive personal data—also known as personally identifiable information (PII)—stored in files, folders, or shares. This will prove beneficial when dealing with requests from consumers on data deletion and data access.

Audit file servers:

Companies can monitor, report on, and receive real-time alerts for changes made to files and folders in file servers. This is how Log360 maintains the integrity of data and ensures it's not being misused. In addition to this, Log360 can thoroughly audit activities on your files and folders in Windows and Linux devices. Every access, creation, deletion, modification, and permission change made to files and folders can be tracked to ensure the security of confidential data. Figure 4 shows the file integrity monitoring report available in Log360. Using this report, administrators can quickly investigate if sensitive data has leaked.

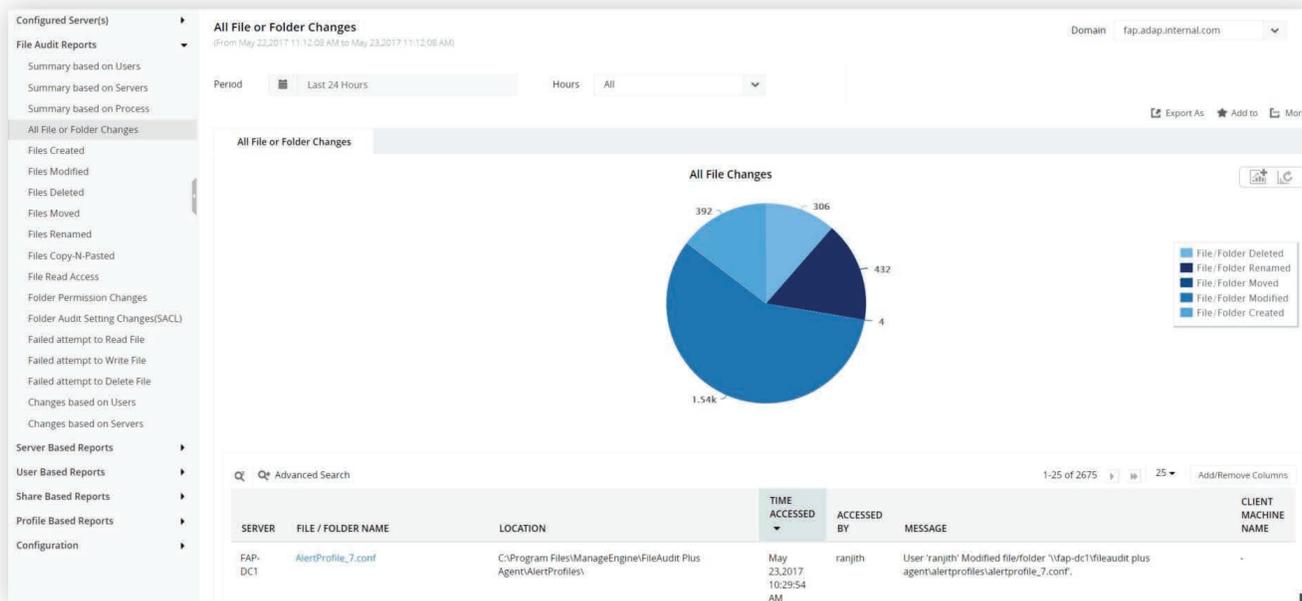


Figure 4: File integrity monitoring in Log360

Conduct audit trails:

Log360's log search capability makes forensic analysis easy (Figure 5 shows the ElasticSearch module of Log360). One of the requirements of the CCPA is to quickly stop a breach or a breach attempt. This can be accomplished by finding the root cause of any security issue. Log360 can help find the root cause of a data breach by searching terabytes of log data within minutes. The solution also provides an option to export the search results as a forensic report.



Figure 5: ElasticSearch in Log360

ManageEngine

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

[\\$ Get Quote](#)

[Download](#)



Toll Free: +1 844 649 7766

Direct Dialing Number: US : +1-408-352-9254



log360-support@manageengine.com



www.manageengine.com/log360

Endnotes



1. Statista, "Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)," 2019,

<https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed>.



2. Tim Cook, "You deserve privacy online. Here's how you could actually get it," Time Magazine, January 17, 2019,

<https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/>.



3. Californians for consumer privacy, "About the California Consumer Privacy Act," Californians for consumer privacy, <https://www.caprivacy.org/about>.