crownpeak

California Consumer Privacy Act (CCPA)

What is the CCPA?

The California Consumer Privacy Act (CCPA) is a new law designed to empower California residents to take control of their personal data. It takes effect on January 1, 2020.

Prepare Now

While the law goes into effect on January 1, 2020, companies will need to disclose what precautions they took in 2019 to be compliant starting in the new year. You need to start working on your CCPA plans now.

Solve the CCPA Challenge

Read on for 11 must-know facts about how you can prepare for the CCPA and provide the best consent experience for your customers.

What is the CCPA?

The California Consumer Privacy Act (CCPA) is a new law designed to empower California residents to take control of their personal data.

When does it go into effect?

January 1, 2020

Is my company affected?

You must comply with the CCPA when working with any California resident's information when **at least one** of the following three criteria apply to your business:

1. Annual gross revenue of $25 million or more
2. Buys, receives, sells, or shares the personal information of 50,000 or more consumers, households or devices per year
3. Earns 50% or more of its annual revenue from the selling of consumers' personal data

My company is not based in California. Does the CCPA still apply?

Similarly, to the GDPR, the CCPA protects the consumer's data regardless of where the business operates. If the consumer is a California resident, the law applies no matter where your business is located.

What does the CCPA require?

There are 5 major components to the CCPA. They give California residents the right to:

1. Know what personal information is being collected about them
2. Know whether their personal information is being shared and to whom
3. Opt-out of the sale of personal information
4. Access the personal information you've collected
5. Equality in service and price even if they've exercised their privacy rights

What does "personal information" mean?

In the context of CCPA, personal information is quite broadly defined and likely includes all data you've ever collected for a consumer or digital visitor. The CCPA specifically defines it as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly with a particular consumer or household.

This covers what's frequently thought of as Personally Identifiable Information (PII), such as name, address, social insurance number, etc. But it also includes any information about that consumer that can be linked to them. This would include geo-ip, page visits, purchase history, and so on. In other words, if you're collecting information and users and visitors, it would fall under this regulation.

What are my disclosure requirements?

Either before collecting or at the time of collecting personal information, your business has to provide the categories and specific pieces of information collected; the sources where that information was collected from; the purpose of the collection; which categories will be shared or sold; and a disclosure of the consumer's rights.

What constitutes compliant disclosure for collection is still being decided through public forums and will ultimately be decided by the California Attorney General. However, there are some basic requirements that always must be met:

- Clear and prominent link to your privacy policy
- The privacy policy must include the disclosure elements listed above, including all third parties who may receive the personal information
- A clear and conspicuous link titled "Do Not Sell My Personal Information" on the home page and privacy policy.

What does sharing personal information and with whom mean?

The CCPA discusses sharing data with third parties and the "sale" of personal information. The distinction between these two is still being defined. Selling personal information is held to a higher standard than sharing.

While the definition of "sale" under CCPA is broad, note that it's more than just a monetary exchange. A "sale" is any kind of consideration or benefit you get in the exchange of data, e.g., sharing data into a cookie pool gives your company benefits. This is also considered a "sale" of data.

In general, you're sharing and not selling when one of the following apply:

- Disclosing under the intentional direction of the consumer
- Using an identifier to indicate to a third-party that a consumer has opted-out of selling of their data

What does sharing personal information and with whom mean?

- Disclosed to a service provider. To qualify, the disclosure must be for a business purpose; pursuant to a written contract that prohibits the further disclosure of the personal information
- You've provided a compliant notification to the consumer that the information will be disclosed in this way
- The service provider doesn't further use the personal information except to accomplish the business purpose.

If the sharing of information doesn't meet the above criteria, you must enable the consumer to opt-out of the disclosure of information.

You will need to carefully consider the written contracts that you have with third parties that run on your website to ensure that you and they are CCPA compliant. Consider a tool such as Crownpeak TagControl to know all of the run-time third-party tags and cookies executing on your site. Consider a tool such as the Evidon Universal Consent Platform® to ensure that your consent notices are fully compliant.

What does opt-out of the sale of personal information mean?

The CCPA requirements for the sale of personal information has three components:

- Disclosure of any selling of personal information as defined by the Act. At minimum this must be in your Privacy Policy. Although not defined yet, it will likely also need to be disclosed more prominently at the point of data collection.
- A prominent and conspicuous link titled "Do Not Sell My Personal Information" on your home page and in your privacy policy.
- A place on your website where the consumer can exercise their various privacy rights under the Act including opting-out the sale of their personal information.

I'm already GDPR compliant. Am I CCPA compliant, too?

Maybe. In general, the GDPR goes further than CCPA in many regards, but the CCPA has very specific requirements around the sale of personal information. Make sure that your consent solution includes all of the CCPA requirements before assuming you are compliant.

What's the best way to become CCPA compliant?

The best solution to CCPA compliance is to have:

- An enterprise-grade notice-and-consent platform installed to ensure consent and notification compliance
- A tool to identify all daisy-chained third-party vendors that execute at run-time on your site to ensure that you know which third parties you're potentially sharing personal information with

Crownpeak offers the Evidon Universal Consent Platform and TagControl products to solve the CCPA challenge.

Find out how Crownpeak solutions can help you provide a consent experience your customers will trust. Request a demo today at crownpeak.com/about/demo-request.

