5 Steps You Must Take to Prepare for CCPA

Caitlin Fennessy, CIPP/US

iapp

Effective Jan. 1, 2020, the California Consumer Privacy Act creates new protections for the personal data of California residents and new requirements for the businesses that process it. To comply with the CCPA, some critical action is needed now.

Here are five concrete action items privacy professionals can tackle and considerations that underpin each step.

1.) Determine who you are under the CCPA

As a starter, you should determine whether and how the CCPA applies to your organization. Is your organization a covered business? If so, is it "selling" personal data? Is it or are your vendors service providers or third parties? Might your organization be multiple of these at once?

Your organization is a **covered business** if it is a for-profit entity that does business in California, collects the personal information of California residents, determines the purposes and means of processing that information, and at least one of the following applies.

- It has annual gross revenues in excess of $25 million.
- It annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices.
- It derives 50% or more of its annual revenues from selling consumers' personal information.

Your organization is **"selling" personal data** under the CCPA if it is "communicating … a consumer's personal information to another business or a third party for monetary or other valuable consideration" … unless it is sharing it with a "service provider" and has provided notice in its terms and conditions that personal information is being shared (or a listed exemption applies). Notice that under the CCPA, the term "sell" is defined broadly to include many actions that your business may not have regarded as sales. For example, placement of a third-party cookie on your website to enable advertising could fall within scope. Allowing vendors to analyze data for their own purposes might also be considered a sale. Moreover, the CCPA definition of personal information is broad — even broader than that under the EU General Data Protection Regulation — and includes cookies, a device identifier, pixel tags, customer number, information linked to a household and more.

Your organization or your vendor is a **"service provider"** if it is a for-profit entity "that processes information on behalf of a [covered] business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business."

Your organization or your vendor is a **"third party"** if it is neither a covered business nor a service provider, as defined above. A third party may still be subject to CCPA obligations through contractual arrangements with business partners sharing personal information of California residents.

> **For a deeper dive on determining who you are under the CCPA, check out these articles:**
>
> - **Determining if you're a business "collecting" or "selling" consumers' personal information**
> - **Are there joint controllers under the CCPA?**
> - **A starting point for CCPA compliance, despite the unknowns**

2.) Update your vendor contracts

If you determine that the CCPA applies to your organization, updating your vendor or customer contracts is a critical action item to comply with the law, as well as to limit your organization's liability. In fact, for a vendor to be classified as a service provider under the law, a contract must be in place.

The first step is determining which of your vendors is a service provider and which is a third party, as those terms are delineated above. Check out this how-to article to guide you through the more detailed nuances of determining whether your vendors are service providers or third parties: How to know if your vendor is a service provider under CCPA.

The process of sorting vendors into third parties and service providers can be approached in tandem with contract updates. Some lawyers are recommending that as the best approach, suggesting that to avoid the requirements associated with the "sale" of personal information, the stated expectation in contracts and other communication with vendors going forward should be that vendors have not been and will not "sell" personal information. Regardless of how your organization decides which of its vendors is a service provider and which is a third party, contract updates are needed.

Service provider contracts

To comply with the CCPA, contracts with service providers must:

- Specify the business purposes for which shared personal information will be processed.
- Prohibit the service provider from "selling" the personal information.
- Prohibit the service provider from retaining, using or disclosing the personal information outside of the direct business relationship between the person and the business and for any purpose other than what is specified in the contract.

Third-party contracts

Covered businesses should also consider updating contracts with "third parties." The CCPA provides that "[a] third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." The law also envisions the business communicating a consumer's opt-out to third parties with which it has shared such information. Businesses should consider whether to delineate responsibility or processes for meeting these requirements in updates of contracts with third parties.

Separately, businesses could make clear in contracts with third parties when they are sharing personal information pursuant to an exception to the term "sell." For instance, when "a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party," that does not constitute a sale, provided the third party itself does not sell the information. If the business is relying on this exception, it should update relevant contracts to state that the third party may not sell the information provided.

Those already in compliance with the GDPR may be able to leverage work done previously on data mapping, records of processing and data processing addendum for CCPA compliance efforts.

> **For more information on vendor and third-party contracts, check out these additional resources:**
>
> - **Aiming for CCPA compliance? Define those vendor relationships**
> - **CCPA: Answers to the most frequently asked questions concerning service providers**

3.) Update your privacy policy

Covered businesses need to update privacy policies and other relevant disclosures to ensure consumers are provided the information required by the CCPA at the appropriate time. It is important to note that information regarding the categories of personal information to be collected and the purposes for which the categories of personal information shall be used must be provided to the consumer at or before the point of collection.

With regard to privacy policies, businesses must disclose the following:

- Descriptions of the rights to access and delete personal data, obtain information about disclosures, opt out of sales, and not be discriminated against.
- Methods for submitting requests for information, including a toll-free telephone number and a website address (where the business has a website).
- Categories of personal information collected in the past 12 months (which may need to be mapped to the following three elements).
    - Categories of sources of personal information.
    - Business or commercial purpose for collecting personal information.
    - Categories of third parties with which the business shares personal information.

- Categories of personal information sold or disclosed for a business purpose in the past 12 months or a statement that personal information is not sold or disclosed for a business purpose.
- If personal information is sold, a link to the separate "Do Not Sell My Personal Information" webpage, which enables consumers to opt out of the sale of their personal information.

> **For an illustration of how CCPA requirements could impact privacy notices in practice, take a look at this piece:**
>
> - **TheScore's privacy notice analyzed against the CCPA**

4.) Enable consumer requests, engagement and opt out of data sales

To comply with the CCPA, businesses need to create or confirm availability of processes to enable consumer requests. Many may be able to leverage processes developed to comply with the GDPR. An important consideration at the outset is whether to adopt a global approach to consumer access requests or segment individuals depending on their location and the relevant legal requirements.

Immediate areas to focus on include enabling:

- Access to and deletion of personal data. This may require companies to:
  - Map their personal data repositories (or leverage existing mapping).
  - Develop processes to verify the identity of requestors (aligned with the California attorney general's regulations).
  - Determine whether access requests will be fulfilled in an automated or manual fashion.
  - Ensure data can be provided in a portable and readily useable format (where feasible).
  - Create a process to direct service providers to delete information from their records.
- Opt out of sales of personal information. Organizations that "sell" personal information, as that term is broadly defined in the law, must:
  - Post a "Do Not Sell My Personal Information" button on the business's homepage and any webpage where it collects personal information, as well as in its privacy policy.
  - Link the above button to a page that 1) explains how a consumer or a consumer's agent can opt out of the sale of their personal information; and 2) enables them to do so.
  - Develop internal processes to ensure that consumers' opt-out requests will be respected for at least 12 months before any new request to sell their personal information is made.
- Opt in to sales of personal information. Organizations that sell personal information must create processes to enable opt-in consent for the sale of personal information of consumers between 13 and 16 years old and parental opt-in consent for those under 13.

The following two web conferences offer useful insights on fulfilling consumer requests:

- **CCPA Compliance: Automating the Intake and Fulfillment of Consumer Requests**
- **How to Modify Your GDPR DSAR Practices for CCPA Requests**

5.) Implement employee training

Ensuring that a business's employees have the training to make sense of this evolving new law is critical to ensure compliance. It is also required by law.

The CCPA requires that all individuals responsible for handling consumer inquiries about the business's privacy practices or compliance with the law are informed of its requirements and how to direct consumers to exercise their rights.

Training on the law's overall requirements, how they align with GDPR requirements, handling of access and deletion requests, and verification processes, as well as reasonable security practices (given the risk of harm caused by and private right of action associated with data breaches) are key areas to target.

Check out the following sites to access a wide variety of CCPA resources, including legal analysis, guidance and new employee training:

- **IAPP's consolidated CCPA Resources**
- **New and continually updated CCPA training**

Clearly, the CCPA is complex. To add to this complexity, the attorney general's regulations and CCPA 2.0 have the potential to change or significantly add to existing requirements. Ensuring that your organization understands CCPA requirements and tracking future developments in the law will be a key action item for companies well into the future.

Published 10/28/2019