Written and published for BrainSpire via SMB Advisors. Rewritten for portfolio presentation.

CCPA Compliance Checklist: Your Roadmap to Success

Arguably the biggest advantage of online marketing is the ability to truly understand your audience. Whether it's through your website, social media, or other digital channels, your interactions with leads and customers generate valuable data. When analyzed properly, that data helps you refine messaging, personalize outreach, and improve overall performance.

However, this advantage has also raised ethical and legal questions regarding consumer data privacy. California was one of the first states to address these concerns when it enacted the California Consumer Privacy Act (CCPA). The law was later expanded and strengthened by the California Privacy Rights Act (CPRA).

Businesses that fail to comply with the CCPA may face regulatory enforcement, civil penalties, and private lawsuits. With this in mind, we've put together a checklist to help you achieve and maintain compliance while conducting business in California.

What is the California Consumer Privacy Act (CCPA)?

CCPA was passed in 2018 after California residents petitioned for legal measures to protect their online privacy. The law was passed on January 1, 2020, requiring greater transparency from businesses that collect personal information from California residents.

Under the CCPA, businesses must inform consumers whether they are collecting, using, sharing, or selling personal data. They must also fulfill consumer requests to:

- Know what personal data is being collected
- Know how their personal data is being used
- Access their personal data
- Stop selling their personal data
- Stop collecting their personal data
- Delete all of their personal data

The California Privacy Rights Act (CPRA)

The CCPA was amended the same year it was enacted, with the intention that consumer protections would continue to grow over time. As part of this effort, the CPRA was passed in 2020 and went into effect in 2023.

One of the original limitations of the CCPA was that it treated all personal data the same, even though some types of data carry higher risks. To address this, the CPRA created a new category called sensitive personal information (SPI). This type of data is considered sensitive because it could expose consumers to identity theft or other harm. Examples of SPI include:

- The consumer's precise location
- Government IDs (such as Social Security numbers)
- Financial account information
- Racial or ethnic origin
- Religious beliefs
- Genetic or biometric data
- Private communications

The CPRA also expanded consumer rights under the CCPA, including the ability to:

- Prevent personal data from being shared
- Limit the use and disclosure of sensitive personal information
- Access personal information collected beyond 12 months

Does the CCPA Apply to You?

The first thing to understand is that the CCPA is a state law, not a federal one. While other states have their own privacy regulations, the CCPA specifically applies to personal information collected from California residents. If your business does not collect data from Californians, the law does not apply. However, if you do collect data from California residents, you are legally required to comply with the CCPA, even if your organization is located outside of the state.

It's also important to note that not every business is required to comply. There are specific criteria that determine whether a company falls under the scope of the law. If your company does not meet those thresholds, you are not legally obligated to follow the CCPA. Below is a checklist to determine whether your business is exempt from the CCPA or not:

1. Determine if Your Business Is Covered

There are three main criteria that determine whether a business must comply with the CCPA. Meeting any one of the following criteria means your company is legally required to achieve and maintain compliance.

- ❑ ***Does your annual gross revenue amount to $25 million?***

Any company that earns $25 million or more in profit per year must comply with the CCPA. If your revenue is currently just below this threshold, it's a good idea to start preparing for compliance, as you may soon meet the requirement.

- ❑ ***Do you receive or share personal information for 50,000 or more consumers, households, or devices?***

If your business collects personal information for 50,000 or more consumers, households, or devices, you must comply, whether you're selling or sharing that data or not.

- ❑ ***Is half of your annual revenue sourced from selling consumer data?***

If your company earns 50% or more of its annual revenue from selling personal information, you must comply, even if you don't meet the other revenue or data thresholds.

2. Identify if Your Business Is Exempt

In addition to companies that do not meet any of the three criteria established by the CCPA's guidelines, there are a few other exemptions in which you won't need to comply with the CCPA's regulations. These exemptions include the following:

- **Data Collected Outside of California**: If the user was outside of California at the time the data was collected, then the CCPA's regulations do not protect that user.

- **Transactional Data Needs**: Personal information necessary to fulfill a contract, complete a transaction, or maintain an ongoing business relationship does not have to be deleted immediately. For example, if a California customer purchases a product with a five-year warranty, their data cannot be deleted until the warranty period ends. However, one-time transactions are not covered by this exemption.

- **Employee Information:** Anyone who is employed or contracted by your company cannot request that you delete their personal data. However, they do have the right to access any personal information that you've collected from them.

- **Research on Behalf of Public Interest** - If you are collecting personal information for public or peer-reviewed scientific, statistical, or historical research, you do not have to delete that information even upon request. However, this depends on whether the research serves the public interest and whether deleting the data would hinder or prevent the study.

- **The Expected Internal Uses**: Personal data used solely for internal purposes, such as analyzing website traffic, may not need to be deleted, as long as the use aligns with reasonable consumer expectations.

- **Legal Compliance**: If a government agency requests personal information under laws like the California Electronic Communications Privacy Act (CalECPA), you do not have to delete it, even if a verified request is submitted. Regulatory investigations or court proceedings can also take priority over CCPA deletion requests.

- **Security Uses:** Certain personal data can be exempt from deletion if you're using it to maintain server logs or to detect and prevent cybersecurity or on-site security incidents.

Is Your Business Compliant?

Once you've determined whether your business meets one of the three CCPA criteria, the next step is to see if your company is actually compliant. There are three key components:

1. **Transparency**: Be clear about what personal data you collect, how you use it, and whether it's shared or sold.

2. **Consumer Requests**: Provide an easy way for consumers to access their data, request deletion, or opt out of the sale or sharing of their information.

3. **Ability to Fulfill Requests**: Make sure your data is organized and accessible, and that employees are trained to handle consumer privacy requests properly.

The following steps will help you determine whether your business is currently CCPA compliant and guide you on what to do if it isn't.

1. Take Stock of Your Data

- ❑ ***Do you have your data of California consumers mapped or inventoried?***

Many businesses collect personal data from various sources, but it's common for that data to be poorly organized. When data isn't well-structured, it can be difficult to trace all the information you have about a single consumer, making it harder to fulfill privacy requests.

Data mapping helps you take proper stock of your data. It makes it easier to track personal information and respond to access or deletion requests efficiently.

2. Update Your Policies and Notices

Although the CCPA doesn't require you to get consent to collect data—except for users aged 16 or younger—it does require transparency. You must clearly communicate whether you're collecting personal information and how it will be used.

To stay transparent and compliant, make sure you update the following website policies and notices:

Update Your Privacy Policies

- ❑ ***Have you updated your company's privacy policy and notices and incorporated them into all your procedures?***

Your privacy policy should clearly explain what information you collect and why. For instance, whether you're collecting data to improve your website experience or to share with third parties, you need to disclose it. Any time you change what data you collect or how you use it, update your policy to reflect those changes.

Your privacy policy should also be easy to find. A good practice is to provide a notice linking to it as soon as visitors arrive on your website.

Review and Strengthen Security Policies

- ❑ ***Can you assure your consumers of confidentiality and integrity?***

It's important to reassure users that the data you collect is secure and that their privacy will be respected. Without this assurance, users may be more likely to request deletion of their information. To build trust, post a clear and easy-to-understand security policy on your website.

Standardize Third-Party Agreements

- ❑ ***Are your agreements with third-party entities standardized and breach-proof?***

If you sell or share personal information with third parties, you need to ensure your agreements with them are clear and enforceable. They should specify what types of personal information are being shared and how the third party is allowed to use it. For example, you may not want them to resell the data without your permission.

3. Set Accessibility Procedures in Place

- ❑ ***Can you execute access or deletion requests accurately and seamlessly?***
- ❑ ***Can you respond to consumers promptly?***
- ❑ ***Can you correctly determine the requesting consumer's eligibility?***
- ❑ ***Can you evaluate which exceptions are available to your company in all instances?***

You're not only required to fulfill data privacy requests, but you must also make it easy for consumers to submit them. Provide a web form and a phone number so users can contact you directly. In addition to mapping all the personal information you've collected, remember to train your employees to handle requests correctly. Keep in mind that you have 45 days to respond once a request is received.

Before fulfilling a request, you must verify that the personal information belongs to the person making the request. If the request is for deletion, make sure the data isn't exempt under the CCPA.

Enable a Verification Process

- ***Can consumers verify their identities?***

Ensure that only the rightful owner can request access to their personal information. Without verification, you risk fraud or identity theft. To prevent this, implement a process that authenticates data privacy requests. There are many verification options available, including email confirmation, multiple-choice security questions, or verification using personal information.

4. Create an Opt-Out Button or Link

- ***Does your site allow consumers to opt out of sharing their information through a button or link?***

If your business sells or shares consumer information, you must provide an opt-out option. A clear button or link makes it easy for consumers to request that you stop selling or sharing their personal data.

5. Establish Consent Procedures for Minors

- ***Do you have a method in place for obtaining consent from the parents of children aged 13 or younger?***

- ***Do you have a method in place for obtaining consent from minors aged 13 to 16?***

As mentioned earlier, you don't need consent to collect data from users over the age of 16. However, for users aged 13 to 16, you must obtain their permission. Users under 13 need consent from a parent or guardian.

Plan Your CCPA Compliance Step by Step

The CCPA sets extensive rules for data transparency and use, and achieving compliance may seem challenging. However, with a systematic approach, it becomes much more manageable.

Start by understanding what the CCPA requires. Then, use the compliance checklist above to guide your actions step by step. Following this approach will not only help you achieve CCPA compliance but also maintain it over time.