Checklist

7 Steps to CPRA Compliance

One of the biggest challenges with complying with data privacy regulations like the California Privacy Rights Act (CPRA) is simply knowing where to start. To track your journey to CPRA compliance, walk through this checklist. Here, we'll delve into the basics of CPRA, explore its key principles, and outline the essential steps to achieve compliance.

☐ 1. Map Your Data

Start by conducting a comprehensive data inventory and mapping exercise. This involves identifying all the personal information your business collects, where it is stored, how it is used, and who it is shared with. Consider all possible sources of personal information, including customer databases, website analytics, and third-party vendors.

Ultimately, mapping your data serves as the foundation for all your downstream compliance activities.

☐ 2. Implement Proper Security Measures

To comply with the CPRA, businesses must implement reasonable security measures to safeguard personal information. The law doesn't exactly give specific guidance about what "security procedures and practices" need to be implemented, which is why it's important to follow best practices, such as meeting SOC 2 standards.

One clear requirement in the CPRA is the need to protect personal information at an "appropriate" level based on its nature—that means businesses need to apply a higher standard of security around the sensitive personal information they process. If you effectively mapped your data in step one, then you'll know where to apply this higher standard.

☐ 3. Develop a Privacy Policy

A robust privacy policy is essential for CPRA compliance. The policy should clearly and accurately outline how your business collects, uses, and shares personal information as well as the rights of consumers under the CPRA.

If you've just started working toward CCPA compliance, you may not have all of this information at hand yet. For instance, you may not have implemented a means of handling subject rights requests. The reality is that your privacy policy should be a living document; as your compliance operations change in your organization, it will need to change as well. As you further develop your privacy program, remember to update your policy correspondingly.

4. Handle Consumer and Employee Requests

Under the CPRA, consumers and employees have the right to:

- Know about the personal information collected and used by a business.
- Request the deletion of their data.
- Correct inaccurate information.
- Opt out from the sharing or sale of their personal information.
- Request businesses to limit the use and disclosure of sensitive personal information.
- Not have their personal information sold or shared if they haven't first opted in if they are a child under the age of 16.
- Not have their personal information sold or shared if their parent or guardian hasn't first opted in if they are a child under the age of 13.
- Avoid discrimination upon exercising the rights granted by the CPRA.

Businesses need to make it easy for consumers to exercise these rights, such as through a DSAR form, toll-free phone number, and/or an email address. What's more, requests need to be fulfilled within 45 days. Businesses can request an extension of up to 90 days, but they must prove that the request is of a particularly high volume or complexity first.

5. Negotiate Data Processing Addenda and Establish Default Contractual Language

To ensure the organizations who receive your consumers' data give it the protection it deserves, the CPRA requires businesses to add data processing addenda to their contracts with vendors.

There are actually three entities under the CPRA we need to be aware of:

- Service providers, or organizations that process personal information for you.
- Contractors, or organizations that use personal information to provide a service for you.
- Third parties, which are defined as any organization that isn't a service provider or contractor.

Only service providers and contractors need data processing addenda under the CCPA. The important thing to know is that the personal data you share with service providers and contractors who have these contractual provisions in place is exempt from consumer opt-out requests.

Unfortunately, there is no prescribed format for a data processing addendum, so you'll need to work with legal counsel to determine what your preferred language should be.

6. Implement and Operationalize Opt-out Mechanisms

The CPRA requires you to provide consumers with two links: 1) a “Do Not Sell or Share My Personal Information” link, and 2) a “Limit the Use of My Sensitive Personal Information” link.

When a consumer requests that you do not sell or share their personal information, it needs to trigger the cessation of any data transfers to third parties (not to service providers or contractors, however).

The “Limit the Use of My Sensitive Personal Information” link functions in a similar way but is stricter. Not only must you cease any transfers of sensitive personal information, but you may only use sensitive personal information if it's necessary for delivering your core product or service and a way that a consumer would reasonably expect.

Lastly, the California Privacy Protection Agency has clarified that businesses must also accept universal opt-out signals, like the Global Privacy Control.

7. Review and Iterate

It can be tempting to think of data privacy compliance as a one-and-done activity, but the reality is that compliance is an ongoing process. Your organization and the way your organization processes personal data will change over time. It’s essential that you:

- Keep your data map updated.
- Improve upon your data protection and security efforts over time.
- Maintain your privacy policies and notices so that they accurately reflect the reality of your organization’s data processing activities.
- Iterate upon your DSAR workflow to reduce effort, risk, and cost.
- Manage your contract portfolio to ensure data processing language remains up to date and new contracts successfully incorporate that language.
- Maintain adequate staff and plan for associated costs.

Attending to all of these requirements at once can be exhausting, especially if you rely on manual, time-consuming processes to carry out your compliance activities. Businesses that rely on Osano for their data mapping, consent management, DSAR workflow, and other difficult but highly automatable compliance requirements regain much-needed time to maintain their CPRA compliance status.

Schedule a Demo of Osano!