Step Three: What Do I Have to Do to Meet My CCPA or CPRA Obligations?

California Consumer Privacy Act
California Privacy Rights Act

The following is provided solely as information that a company should consider when attempting to determine whether it can generally comply with the California Consumer Privacy Act ("CCPA"). This is not intended as an exhaustive compliance checklist, it should not be considered legal advice and should not be used to determine if a business is "compliant." It is intended to assist a company in determining what the company must consider to meet applicable requirements.

NOTE: In November, 2020, California voters approved the California Privacy Rights Act (the "CPRA"), which amends the CCPA. The CPRA is set to become effective on January 1, 2023. Until then, the CCPA will remain in full force and effect. Below, you will find what a business, service provider or contractor should consider under both the CCPA and the CPRA.
For ease of comparison, the CPRA additions or changes are shown in red text.

A. What should you be able to do if the CCPA or CPRA applies to your business and its collecting, sharing or selling of personal information?

I. Consumer Rights. Each of the following rights are available to applicable California consumers with respect to any personal information your business may process about them. Assuming each request is authentic, validated, and an exemption or exception doesn't apply, your business will need to be able to do the following:

□	**Right to Know** You must be able to determine if you are collecting or have collected personal information on the qualified consumer making the request.
□	**Right to Request to Disclosure** You must be able to determine what categories and specific pieces of personal information is collected and for what purpose the information is used.

□	**Right to Delete** You must be able to delete a qualified consumer's personal information from your own records and also direct service providers to do the same.
□	**Right to Opt-Out - CCPA** If you sell consumers' personal data and receive an opt-out request from a qualified consumer, you must be able to cease selling that customer's personal information.
□	**Right to Opt-Out – CPRA (January 1, 2023)** If you sell *or share** consumers' personal information and receive an opt-out request from a qualified consumer, you must be able to cease selling *or sharing* that customer's personal information.
□	**Right to Correct Inaccurate Personal Information – CPRA (January 1, 2023)** Upon request from a qualified consumer, you must be able to correct any inaccurate personal information that you maintain about that consumer.
□	**Right to Limit the Use and Disclosure of Sensitive Information – CPRA (January 1, 2023)** Upon request from a qualified consumer, you must be able to limit your use and disclosure of that customer's *sensitive personal information*** to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer.

	• "Sharing" means your use of personal information when you share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate personal information to a third party for "cross-context behavioral advertising," whether or not for monetary or other valuable consideration.
	
	"Cross-context behavioral advertising" is the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses or other services, other than the business or services in which the consumer intentionally interacts with.
	
	• **"**Sensitive Personal Information" includes:
	
	  • Social Security, driver's license, state identification card or passport number;
	  • Account log-in, financial account, debit card, credit card number with security or access code or password;
	  • Precise geolocation;
	  • Racial or ethnic origin, religious/philosophical beliefs or union membership;
	  • Contents of mail, email and text messages;
	  • Genetic data and processing of biometric information; or

- Health and sexual orientation.

II. Procedural Requirements for Business.

a. Notice to Consumers. The CCPA requires covered businesses to inform consumers of the following information in its online privacy policy, which is easy to read, clearly understandable and does not contain dense legal jargon:

- **Rights.** A list of consumers' rights under CCPA. (See above)

- **Categories of Personal Information.**

    - **Collected.** A list of categories of personal information (11 specific categories of PI are to be used) **collected** in the preceding 12 months and the purposes (business and commercial) for collection; use for any other purposes requires further notice prior to different use.

    - **Sold.** A list of categories of personal information sold in the preceding 12 months (or if the covered business has not sold consumers' personal information in the preceding 12 months, the covered business must inform the consumer of that fact).

    - **Disclosed**. A list of categories of personal information disclosed for a business purpose in the preceding 12 months (or if the covered business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the covered business must state that).

- **Financial Incentive**. If the business provides a financial incentive or a price or service difference based on the consumer's data choices, the business must provide a Notice of Financial Incentive. This notice must include:

    - **Summary.** A succinct summary of the financial incentive or price or service difference offered; and

    - **Material Summary**. A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data.

- **Opt-in.** How the consumer can opt-in to the financial incentive or price or service difference.

- **Right of Withdrawal.** A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right.

- **Explanation of Value.** An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

    - A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

    - A description of the method the business used to calculate the value of the consumer's data.

b. Privacy Policy Updates. Building on the CCPA's requirements from 2020, the CPRA requires the following additional information to be included in the online privacy policy:

- **Categories of Sharing.** Adds "Sharing" of personal information to the required lists of categories described above under the CCPA.

- **Categories of Sources.** The categories of sources from which consumers' personal information is collected.

- **Purpose.** The business or commercial purpose for collecting, selling or sharing consumers' personal information.

- **Categories of Third Parties.** The categories of third parties to whom the covered business discloses consumers' personal information.

- **Retention Period**. The length of time the business intends to retain each category of personal information. If not possible, must disclose the criteria the business uses to determine the retention periods for each category, provided that it will not be longer than is reasonably necessary for the specified purpose.

c. Sale of Information. Covered businesses should determine whether or not they plan to sell the personal information of California consumers to third parties. If a covered business decides to sell, then it should implement processes to account for the following:

- **"Do Not Sell My Personal Information Link."** Under the CCPA, if a business sells the personal information of California consumers, it must provide two

methods to opt out, including clearly and conspicuously posting a link entitled "Do Not Sell My Personal Information," which directs visitors to a webpage where the visitor can opt-out of their personal information being sold. The link must be placed on both the internet home page and in the online privacy policy.

- The second method can include, but is not necessarily limited to: a toll-free; phone number; a designated email address; a form submitted in person; a form submitted through the mail and user-enabled global privacy controls.

- The CPRA requires the same process, but the link must be titled "Do Not Sell *or Share* My Personal Information."

- The CPRA also requires businesses to provide a clear and conspicuous link on the business's internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to only those uses authorized.

- The CPRA also allows a single, clearly labeled, link to be used on the business's internet homepages (rather than the two separate links described above) to allow a consumer to easily opt out of the sale or sharing of the consumer's personal information AND to limit the use or disclosure of the consumer's sensitive personal information.

- The CPRA requires that a consumer not be forced to create an account or otherwise provide any information beyond what is necessary to instruct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

- The CPRA requires that businesses ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CPRA are informed of all requirements in Sections 1798.120, 1798.121, and 1798.135 of the CPRA and how to direct consumers to exercise their rights under those sections.

- **Opt-In and Parental Consent.** Businesses must seek opt-in consent from California children between the ages of 13 and 15. If selling personal information from children under the age of 13, the business must receive parental consent.

- **Refrain from Seeking Opt-In Consent.** A business must refrain for following up with any consumer that has opted out for 12 months after receipt of the consumer's opt out.

d. Responding To Consumer Requests. Under the CCPA, businesses have to acknowledge and respond to authenticated requests from any consumer.

- **10 days.** A business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response.

- **45 days.** Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request.

- **90 days.** If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

e. No Discrimination. Under the CCPA and CPRA, consumers have the right to equal service and price, meaning that a covered business cannot discriminate against a consumer because the consumer exercised any of his or her rights under the CCPA or CPRA. Covered businesses must have processes in place to ensure they do not inadvertently discriminate under CCPA or CPRA. Discrimination, for purposes of CCPA and CPRA, includes:

- Denying goods or services to the consumer;
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits of imposing penalties;
- Providing a different level or quality of goods or services to the consumer, if the consumer exercises his or her rights under CCPA or CPRA; and
- Suggesting that the consumer will receive a different price or rate for goods or services, or a different level or quality of goods or services.

The CPRA adds one additional example of what constitutes discrimination:

- Retaliating against an employee, applicant for employment, or independent contractor.

B. What should you be able to do if you are a "service provider" under the CCPA?

Essential to the role as a service provider is a written contract between the covered business and your business in which the covered business prohibits your business from retaining, using or disclosing personal information for:

- Any purpose other than performing the services specified in the contract or that the CCPA otherwise permits a service provider to take; and

- A commercial purpose other than providing the services specified in the contract.

A service provider generally shall not retain, use or disclose personal information obtained while performing its services except:

- To process or maintain personal information on behalf of the covered business that provided the personal information in compliance with the written contract;
- To retain and employ another service provider;
- For internal use to build or improve the quality of your services; or
- To detect data security incidents or protect against fraudulent or illegal activity.

Additionally, if a consumer has opted-out of the sale of his/her information, a service provider cannot sell their data on behalf of the covered business. Moreover, if a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the covered business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

C. What should you be able to do if you are a "service provider" OR a "contractor" under the CPRA (January 1, 2023)?

I. Service Provider. A written contract between the covered business and your business (as a service provider) in which the covered business prohibits your business from:

- Selling or sharing the personal information.
- Retaining, using or disclosing personal information for any purpose other than for the business purposes specified in the contract or as specified in the CPRA.
- Retaining, using or disclosing personal information outside the direct business relationship with the covered business.
- Combining the personal information with personal information retained from another business relationship or that you collect on your own.

II. Third Party. A written contract between the covered business and your business (as a third party) in which the covered business:

- Prohibits you from retaining, using, or disclosing the personal information for any purpose except performing the services specified in the contract, including prohibiting use for a different commercial purpose (similar to service providers).
- Prohibits you from selling the personal information and retaining, using, or disclosing the information outside of the direct business relationship between the recipient and the business.
- Must include a certification that you understand the restrictions and intends to comply with them.

III. Contractor. Contractors are also required to have a written agreement with covered businesses. In addition to the requirements listed above for service providers, contractors must also have the following in its agreement with covered businesses:

- A certification that the contractor understands the restrictions listed under the CPRA; and
- A process in which the business is able to monitor the contractor's compliance with the contract through manual reviews or other methods.

Additionally, service providers and contractors are required to cooperate with covered businesses in complying with any data subject requests, such as deleting or enabling the covered businesses to delete any personal information upon a consumer request.