Last Reviewed: May 21, 2024

A Primer on the CCPA/CPRA

Introduction

The California Consumer Privacy Act (CCPA) became law on January 1, 2020 and was the first comprehensive data privacy legislation to be enacted in the U.S. The CCPA introduces requirements for businesses handling personal data for California residents. The California Privacy Rights Act (CPRA) was a ballot initiative approved by voters in November 2020 that amended the CCPA with additional privacy protections for consumers and came into effect on January 1, 2023. This primer provides practical tips to help sales and marketing teams navigate these regulations while using a go-to-market platform like ZoomInfo.

For simplicity within this document, we will refer to the CCPA as amended by the CPRA as "the CPRA."

Which companies are governed by the CPRA?

These laws apply to any for-profit organization that does business in California, collects, shares or sells California residents' personal data, and meets one or more of the following three criteria:

- Has an annual gross revenue of $25m or more
- Annually buys, sells, or shares the personal information of 100K or more California consumers, households or devices, or
- Earns more than half its annual revenue by selling or sharing personal information

If your organization does not meet this threshold, the law does not apply to you.

What does the CPRA require of companies?

If the law does apply to you, the CPRA imposes several key obligations with regard to the collection and use of personal information of California consumers. In general, the CPRA is an opt-out statute, meaning you can collect and use personal information, but must provide notice and respect the rights of consumers to opt out of the sale or sharing of their information, to know what data you have about them, to have their data corrected or deleted, or to limit the use and disclosure of their sensitive personal data. Notable scenarios that require consent include when collecting data on minors, or when asking individuals who have previously opted out of your processing to opt back in after one year has passed from their opt-out request.

Can a business be liable for its service provider's misconduct under CPRA?

If a service provider uses personal information in violation of the CPRA, a business is not liable if the business: (i) has a written contract with the service provider that complies with the CPRA; and (ii) at the time it discloses the personal information, does not have actual knowledge or reason to believe that the service provider intends to violate CPRA.

More simply, any customer seeking to purchase third-party data for sales and marketing purposes from a data broker cannot be held liable for any of the data vendor's actions provided there is a legal agreement and the customer was not aware of any violations at the time the data vendor disclosed data to the customer.

What is ZoomInfo doing about its own compliance with CPRA?

As a data broker, we are required to register with the state and provide consumers with clear and conspicuous notice regarding what data we collect, how it is used, and the rights consumers have, including the right to opt out of our database. On top of this registration, we extended our direct notice program across California contacts. Addressable contacts are provided with a notice directly by email which informs them of our processing and provides them easy mechanisms to opt-out.

In addition, we have taken affirmative steps to ensure our ongoing commitment to privacy, including:

- **Product Enhancements:** We have enhanced our products to help our customers address CPRA obligations, including publishing notice dates for all California-based contacts, and making a list of our CPRA opt-outs available to customers. Additionally, improvements to our consumer location data, Compliance API product, and the addition of our customer master suppression feature to propagate opt outs from your CRM and MAT systems directly in the ZoomInfo platform serve to support our customers in their CPRA compliance efforts.
- **Trust Center Enhancements:** We have fortified our Trust Center so individuals can proactively manage their data preferences and profiles with much greater ease.
- **Privacy Policy and Website Update:** We regularly update our privacy policy

and website assets to ensure transparency

- **Expansion of Privacy Communication Options:** We have expanded the number of ways that data subjects are able to reach our privacy team, including the provisioning of a toll-free number to leave inquiries.
- **Data Team Expansion:** We have enhanced our data team to ensure proactive management of our data with comprehensive project management reviews.
- **Employee Training and Awareness:** We conduct employee awareness and training to help ensure ongoing compliance with our legal obligations.

What MUST my company consider regarding CPRA compliance?

You should always consult qualified legal counsel for advice on your organization's specific legal compliance obligations. Below are some general items that you should consider when implementing a CPRA compliance program:

- **Update Your Privacy Policy:** This is the one-stop shop document to communicate on how you run your business. Be transparent in your practices and policies.

- **Data Vendor Selection:** When evaluating data providers, confirm that your data provider employs CPRA-compliant data practices. Data providers that do not register as a data broker, post and provide notice to data subjects, or honor data subject access requests may be in violation of the CPRA. Remember, customers may be liable for the actions of their service providers if they are aware of provider policies that violate the CPRA.

- **Data Inventory:** As data fuels the marketing economy, it is important to know what you have, how it's managed and where it's located. All data has a shelf life and you should create policies and procedures for the off-boarding of these assets.

- **Investigate Potential Data Selling:** Determine whether your company sells or shares personal information in any manner. Some companies may have little-known data sharing partnerships with third-parties. If so, there are several requirements imposed upon companies selling data.

- **Establish a Privacy Rights Management Program:** The CPRA affords rights to consumers, including but not limited to opting-out of sale, and requesting access to their records. Having a team prepared to manage these requests is a crucial part of ensuring compliance.

What SHOULD my company consider regarding CPRA compliance?

In addition to tasks that minimize or eliminate liability under the CPRA, there are additional best practices you can adopt to position your organization for success, including:

- **Review Your Compliance Obligations:** Check with your legal team or outside counsel for CPRA or other legislation that may be applicable to your business.

- **Appoint a Data Privacy Officer:** Having someone on point for all things compliance related is a great resource for your organization and demonstrates your commitment to transparency and privacy.

Please visit our Trust Center for more information on our policies: https://www.zoominfo.com/trust-center

Notice: This is for informational purposes only and is not intended to constitute legal advice. ZoomInfo is not qualified to provide legal advice of any kind and is not an authority on the interpretation of the CPRA or any other rule or regulation. To understand how the CPRA or any other law impacts you or your business, you should seek independent advice from qualified legal counsel.