zoominfo

A Primer on CCPA and Marketing Data Protection Best Practices

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 on California residents.

Which companies are governed by the CCPA?

The CCPA applies to any for-profit organization that collects, shares or sells California residents' personal data and meets any one of the following three criteria:

- Has an annual gross revenue of $25m or more,
- Processes the personal information of 50K or more California consumers, households or devices,
- Earns more than half its annual revenue by selling personal information

If your organization does not meet one of these thresholds, the law does not apply to you.

What does the CCPA require of companies?

If the CCPA does apply to you, CCPA imposes several key obligations with regard to the collection and use of personal information on California consumers. In general, CCPA is an opt-out statute, meaning you can collect and use consumer personal information, but must provide notice and respect the rights of consumers to opt out of collection, to know what data you have about them, or have their data deleted.

What types of data are exempted from CCPA?

The above requirements come with numerous exceptions, including exceptions for data on employees, data needed to perform a contract with the consumer or a legal obligation, and a limited exception for publicly available information.

Important: After CCPA was enacted, there were many efforts to amend and clarify various provisions, including the passage of Assembly Bill 1355. AB1355 exempts certain B2B information from most of the CCPA's core requirements. In a nutshell,

the CCPA's notice, access, and deletion requirements do not apply to information in business-to-business communications, i.e. information you have about someone because you have communicated with them as an employee of a company for the purposes of providing a service or product to the company, buying something from the company, or performing due diligence on a transaction.

The introduction of the CPRA expands the publicly-available exception to cover information available online.

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

If a service provider uses personal information in violation of the Act, a business is not liable if the business: (i) has a written contract with the service provider that complies with the Act; 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 Act.

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 of contract signing.

What is ZoomInfo doing about its own compliance with CCPA?

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. We have implemented a comprehensive notice and choice program, and we will not include anyone in the database unless they have received notice from us. So you can be confident the data you get from us is CCPA compliant.

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 CCPA obligations, including publishing notice dates for all California-based contacts, and making a list of our CCPA 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.

- **Privacy Center Implementation:** We have developed a Privacy Center so consumers can proactively manage their data preferences and profiles
- **Privacy Policy and Website Update:** We have updated 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 the data with comprehensive project management reviews.
- **Data Inventory Accuracy Analysis:** We have increased the accuracy and integrity of all data we host, by leveraging the resources of our internal and external data sources.
- **Employee Training and Awareness:** We conduct employee awareness and training to ensure ongoing compliance.

What MUST my company consider regarding CCPA compliance?

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

- **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: create policies for the off-boarding of these assets. Most notably, look for any potential non-business personal information residing on your systems. Any personal data that is not considered business data or covered by any other exemption will be subject to CCPA. If a data subject asks that you remove their personal (non-business) data from your systems, you are required to comply with the deletion request.

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

What SHOULD my company consider regarding CCPA compliance?

In addition to tasks that minimize or eliminate liability under the CCPA, 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 CCPA or other legislation that may be applicable to your business.

- **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.

- **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 for transparency and privacy.

- **Consider Industry Codes or Advisories:** Proactive privacy management is now available to businesses, consider these solutions to publicly demonstrate your privacy commitments.

Please visit our privacy page for more information on our policies at: https://www.zoominfo.com/about-zoominfo/privacy-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 CCPA or any other rule or regulation. To understand how the CCPA or any other law impacts you or your business, you should seek independent advice from qualified legal counsel.