BURR FORMAN LLP

Businesses Should Consider How They are Impacted by the California Consumer Privacy Acts

Article
11.14.2022

The CCPA – or the California Consumer Privacy Act – went into effect on January 1, 2020, followed by the CPRA, or California Privacy Rights Act. These laws have had a significant impact on the privacy and data security landscape in the U.S.

Many business owners not located in California are questioning if they should be concerned about the CCPA, and the answer is probably so. If your company collects the personal information of California consumers, then it needs to consider whether it otherwise qualifies as a business or other covered entity under the CCPA and CPRA, and if so, how the business will be impacted. The criteria to determine whether an entity qualifies as a business are:

- A for-profit legal entity doing business in California that collects consumers' personal information AND
- Meets one or more of the following criteria:
- Had annual gross revenues of more than $25M the preceding calendar year;
- Annually buys, sells, or shares the personal information of 50,000 or more consumers or households;
- Derives 50% or more of its annual revenues from selling (not sharing) consumers' personal information.

California Consumer Privacy Act

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Businesses Should Consider How They are Impacted by the California Consumer Privacy Acts

Businesses that meet the above qualifications must understand how to comply with the CCPA. The main requirements of the law are:

For “Disclosure and Transparency”businesses must --

- Provide notice about collection practices.
- Disclose and keep up-to-date at least once every 12 months a description of consumers’ rights, e.g., privacy policy.
- List separately the categories of private information (PI) collected, sold, and disclosed for a business purpose in the preceding 12 months.
- Provide notice about onward transfers of PI.
- And make available two or more designated methods for requesting PI held by a business.

If selling PI, they must:

- Provide the right to opt out via a clear and conspicuous link entitled: “Do Not Sell My Personal Information.”
- Seek opt-in consent from consumers between the ages of 13-16.
- Seek opt-in consent from parents if a consumer is under 13 years of age.
- Establish procedures for receiving and processing verifiable consumer requests.
- Amend contracts with third parties to clarify PI is not shared for value (if applicable).

As of January 1, 2023, the full scope of CCPA rights is set to extend to California employees. This date was extended from its original anticipated enactment date of January 1, 2022. Employees will have the right to know what PI is collected and how it is used.

Business owners should note there are penalties for not complying with the CCPA. The California Attorney General may institute actions that may result in a $2,500 fine for each unintentional violation and a $7,500 fine for each intentional violation. Additionally, for data security breach violations, consumers may bring private causes of action, with statutory damages between $100-$750 per consumer, per incident; OR actual damages, whichever is greater. This has resulted in plaintiffs filing numerous class actions under the CCPA since it was enacted on January 1, 2020.

California Rights and Enforcement Act

This act amends certain provisions of the CCPA or the California Consumer Privacy Act. The CPRA clarifies and amends the definition of what qualifies as a business and expands certain consumer privacy rights. Generally, it goes into effect January 1, 2023.

Businesses Should Consider How They are Impacted by the California Consumer Privacy Acts

The CPRA includes various new rights for consumers concerning their management and the treatment of their personal information. For example, the CPRA includes the following additional rights:

(1) Businesses must disclose the consumer's right to request the correction of inaccurate personal information, and the consumer has the right to request a business correct such inaccurate personal information.

(2) The CPRA creates a new category of "sensitive personal information," which includes personal information revealing a consumer's:

(a) Social security number, driver's license number, state identification card, or passport number

(b) Account log-in, financial account, debit card number, or credit card number – in combination with a required security or access code, password, or credentials allowing access to the account

(c) Precise geolocation data – which is a radius of 1,850 feet around the consumer or less

(d) Racial or ethnic origin, religious or philosophical belief, or union membership

(e) Mail, email, and text message content – unless the business is the intended recipient of the correspondence

(f) Genetic data

(g) Businesses must notify consumers of (i) the collection of sensitive personal information, (ii) the purposes for which it is being collected or used, and (iii) whether it is being sold or shared;

(h) Consumers have the right to limit the use of their sensitive personal information to only as necessary to perform services or provide goods reasonably expected based on the transaction with the business.

(3) In addition to displaying the link "Do Not Sell or Share My Personal Information" on the business's homepage, businesses must also post a link for "Limit the Use of My Sensitive Personal Information." In the alternative to these 2 links, businesses may: (i) use a single, clearly labeled link on the business's homepage, or (ii) recognize an opt-out preference signal sent with the consumer's consent by the consumer's technology or platform. However, the specific guidelines as to this technical procedure are still evolving.

(4) Consumers have a right to know the length of time the business intends to retain each category of personal information and sensitive personal information.

(5) The CPRA implements data minimization and purpose limitations principles, similar to those found in GDPR (the EU General Data Protection Regulation). In sum, a business shall not retain a consumer's personal information or sensitive personal information for longer thanreasonably necessary for the

disclosed purpose for which the data was collected. Additionally, a business's collection, use, retention, and sharing of personal information shall be reasonably necessary and proportionate to the purpose for which it was collected.

(6) Businesses must implement and maintain reasonable security procedures and practices, which are not specifically defined.

(7) And finally, the CPRA sets out certain requirements for contracts between a business and a third-party, service provider, or contractor, and they generally involve vendor management provisions.

Conclusion

It should be noted that a privacy policy must include operational elements, as well as an accessible link for individuals to request their personal information not be sold. There must be a method to request personal information maintained by the business. In addition, the privacy policy should be reviewed and updated as appropriate every 12 months. Businesses must also implement reasonable security methods, appropriate in the context of the types and sensitivity of PI they collect and consistent with the industry in which they operate.

In conclusion, while businesses may be able to conduct a general assessment as to whether they are subject to compliance with CCPA and CPRA. It is recommended they consult with a data privacy/ cybersecurity attorney regarding how to implement compliance and, importantly, how to monitor and ensure ongoing compliance. Although various provisions of the CPRA do not go into effect until January 1, 2023, businesses should not wait until the last minute to comply with it, as a rush job may lead to mistakes, unexpected obstacles, or inadequate funding for the effort.

If your business needs assistance navigating the CCPA and CRPA, visit our website at www.burrcyber.com.