BURR FORMAN LLP

Overview of Applicability and Updated Privacy Provisions in the California Privacy Rights and Enforcement Act of 2020 (CPRA)

Articles / Publications
06.10.2021

The CPRA – or the California Privacy Rights and Enforcement Act of 2020 – amends certain provisions of the CCPA (California Consumer Privacy Act) that went into effect on January 1, 2020. The CPRA narrows the definition of what qualifies as a business while expanding consumers' privacy rights. It goes into effect as of January 1, 2023.

If your company collects personal information of California consumers, then it needs to consider whether it otherwise qualifies as a business or other covered entity under the CPRA. The criteria to determine whether an entity is a business are:

(1) A for-profit legal entity doing business in California that collects consumers' personal information AND

(2) Meets one or more of the following criteria:

(a) Has annual gross revenues of more than $25M the preceding calendar year. (CPRA clarifies that determinative time frame is preceding calendar year);

(b) Annually buys, sells, or shares the personal information of 100,000 or more consumers or households. (The CCPA provides for the lower threshold of 50,000.)

(c) Derives 50% or more of its annual revenues from selling or sharing consumers' personal information. (The CPRA broadens this element, as the CCPA only considers selling, not sharing personal

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

information.)

The CCPA and CPRA define a "consumer" as a "natural person who is a California resident," referencing the definition of a "resident" in California's tax code, 18 CCR § 17014. California's tax code defines a resident as:

(1) Individuals living in California for other than a temporary or transitory purpose; and

(2) Individuals who are domiciled in California and are outside the State for a temporary or transitory purpose.

The phrase "doing business in California" is not specifically defined. During the CCPA rule-making process, the Office of the Attorney General took the position that the phrase should be given meaning according to the plain language of the words and other California laws. Other California laws, such as its tax code, define this phrase broadly, to include actively engaging in any transaction for the purpose of financial or monetary gain or profit. Accordingly, it may be safe to assume that if a company collects, sells, or shares personal information of California consumers and obtains a monetary benefit as a result – particularly on a regular basis – that may be considered doing business in California.

The CPRA includes various new rights for consumers with regard to 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 that a business correct such inaccurate personal information.

(2) The CPRA creates a new category of "sensitive personal information," which includes personal information that reveals 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;

Overview of Applicability and Updated Privacy Provisions in the California Privacy Rights and Enforcement Act of 2020 (CPRA)

(g) Additionally, 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 the services or provide the 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 on the homepage, businesses may: (i) use a single, clearly labeled link on the business's homepage, or (ii) respect 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 (EU General Data Protection Regulation). In sum, a business shall not retain a consumer's personal information or sensitive personal information for longer than is reasonably 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) 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.

There are a number of exemptions set out in the CPRA. For example:

(1) If every aspect of the business's commercial conduct takes place wholly outside of California, then the CPRA does not apply to the business's collection, selling, or sharing of the consumer's personal information.

(2) Other exemptions are based on compliance with a federal, state, or local law, court order, or subpoena to provide information, as well as for the business to exercise or defend legal claims.

(3) There are exemptions for compliance with other potentially applicable laws, including compliance with HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act); FCRA (Fair Credit Reporting Act); GLBA (Gramm-Leach-Bliley Act); and

Overview of Applicability and Updated Privacy Provisions in the California Privacy Rights and Enforcement Act of 2020 (CPRA)

other similar federal and California industry-specific statutes that include privacy and data security protections.

(4) The CPRA extends the exemption in the CCPA for collecting personal information of employees, owners, directors, officers, independent contractors, and job applicants from January 1, 2022, to January 1, 2023. The exemption concerning personal information collected in the course of B2B communications and transactions is also extended generally until January 1, 2023.

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

Burr & Forman's Cybersecurity and Data Privacy team offers these services, and we are happy to assist.