March 16, 2023

Not a California Company? You May Still Be Subject to the CPRA

The California Privacy Rights Act (CPRA) became effective January 1 and amends the 2018 California Consumer Protection Act (CCPA). The CPRA gives California consumers and employees more control over their personal data. It creates several obligations for California-based corporations and certain companies that conduct business in the state or that collect, use or share the data of California residents. While the CPRA went into effect on January 1, enforcement by the California Privacy Protection Agency (CPPA) will likely begin in *July*. Therefore, it is crucial to determine now whether your business is subject to the provisions of the CPRA. *Even entities that are not based in California or do not have facilities or offices in California can have obligations under the CPRA. In order for a business to be subject to the CPRA, it must be a for-profit entity doing business in California and must*

1. earn gross revenue in excess of $25 million in the preceding calendar year;
2. buy, sell or share the information of at least 100,000 consumers or households in California; or
3. earn 50 percent or more of its annual revenue from selling or sharing California consumers' personal information.

Importantly, "doing business in California" can mean a variety of things. Operating your California-based business is obvious, but the act would also include non-California companies that have just a single employee based in California. Additionally, if a company engages with a significant number of California residents, it may be subject to the CPRA. For example, if your website collects data from more than 100,000 California residents, you will be required to abide by the provisions of the CPRA. If your website sees traffic from California consumers, you may want to consider revision of your privacy policies to address the additional data privacy rights of these California consumers and to comply with the CPRA as a general matter. In the age of the virtual workforce, it is important to consider whether any of your employees (virtual or in the office) are located in California. The CPRA ended the CCPA's exemptions for employee data, meaning that all data collected from an employee within the scope of their employment or from an applicant for employment is subject to the CPRA. The CPRA also includes a "lookback period" for which entities must be able to produce information concerning the personal information they used, collected, shared, bought or sold January 1 through December 31, 2022. Additionally, the CPRA applies to service providers, and service providers can likely expect to see added language in their agreements with companies doing business in California that require higher data privacy standards. The CPRA defines a service provider as an entity that processes personal information on behalf of a business and receives from or on behalf of the business consumers' personal information for a business purpose pursuant to a written contract, provided the contract prohibits the person from selling or sharing data or engaging with data that otherwise violates the CPRA. This means that a service provider can be virtually any for-profit entity that is under contract with a main business to provide some form of service that requires the processing of data. For example, human resources or payroll software companies and other employee benefits administrators would likely be considered service providers under the CPRA. The CPRA will have a limited application to the healthcare industry because it specifically exempts "medical information" as defined by California's Confidentiality of Medical Information Act (CMIA) and protected health information (PHI) as defined by HIPAA. While healthcare providers and organizations benefit from CMIA and HIPAA exemptions, they remain subject to the vast obligations for non-HIPAA PHI. This includes the requirements involving employment-related personal information with respect to an organization's workforce (including medical staff). The situation concerning the CPRA is a fluid one, but final regulations from the CPPA are in the last steps of approval, with a potential effective date sometime in April. Despite an anticipated enforcement date beginning in July, the CPRA is active, and the CPPA can enforce against violations from any date after January 1. While it is too early to tell to what extent the CPPA will

pursue these "backdated" violations, entities should be taking active steps now to work toward compliance.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com



Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com



Colton J. Kopcik
Associate

Washington, D.C. | (203) 977-7362

ckopcik@daypitney.com