

## California Privacy Rights Act (CPRA) Regulations Push Forward

By Thomas J. DeMayo, Partner

The California Privacy Protection Agency approved the final draft of the “[Regulations](#)” declared under the California Privacy Rights Act of 2020 (CPRA). The Regulations provide enhanced interpretation and expand upon the CPRA. Now approved, the Regulations will go into a 30-day review period and will likely take effect April of 2023. Enforcement of the CPRA will not occur until July of 2023; as such, the amount of time to fully adopt some of the revisions noted in the Regulations is limited.

Companies doing business with California residents must be aware of both the new and existing privacy rules to maintain compliance. What leadership team doesn't want to avoid financial penalties and unnecessary litigation? Especially if that could have been avoided by timely, prudent action. So, read on if your company is affected.

### Important Stipulations

Key provisions to be aware of are as follow:

- **Purpose Limitations** – Consumers' personal information that is collected, used, stored, retained, or shared (collectively “processed”) by a business must be necessary and proportionate to achieve the purpose for which the personal information was processed and compatible with the context in which it was collected. An example described in the Regulation is the consumer of a business' mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.
- **Submitting Requests and Obtaining Consent** – Methods for submitting California Consumer Privacy Act (CCPA) requests and obtaining consumer consent must be easy to understand and provide symmetry in choice. An example provided in the Regulation is a website banner that provides only the two choices when seeking the consumer's consent to use their personal information, “Accept All” and “More Information.” For symmetry in choice, a reject or deny all option would also need to be provided.
- **Alternative Opt-Out Link** – Instead of posting the two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links, a business may opt for a single, clearly-labeled link allowing consumers to exercise both their right to opt-out of sale/sharing and right to limit.
- **Opt-Out Preference Signals** – A consumer can elect to automatically opt-out of all sharing and the sale of their personal information with all businesses they interact with online and not be required to make individual requests. As such, the business must be able to recognize and process the opt-out signals.
- **Agency Audit** – The Agency may audit a business, service provider, contractor, or person to ensure compliance with any announced or unannounced provision of the CCPA.

### General Recap on CPRA

CPRA is the latest amendment to California's existing consumer privacy law, the California Consumer Privacy Act (CCPA). The CPRA expands individuals' data privacy protections, including rights of

employees who live in California. This legislation further dictates how organizations operate when it comes to collecting, utilizing and sharing privacy related data.

The CPRA defines different types of "personal information" and the rights California-based consumers (and employees) have when it comes to how their data is managed. The CPRA's ancillary rights also include the ability for California residents to limit the use and disclosure of personal data and forces businesses to correct personal information inaccuracies upon request. There are several additional requirements beyond these that will also impact businesses both large and small.

The CPRA applies to businesses with annual global revenues over U.S. \$25 million, those that buy, sell, or share personal data for at least 100,000 California consumers/households and who receive 50% or more of their annual revenue from sharing or selling personal data. While some believe that this is merely a California issue, it extends beyond that. The reality is, it is widely anticipated that this is just the tip of the iceberg and many states are going to follow suit by adopting their own privacy legislation in the not-so-distant future. The CPRA is also more far reaching since it applies to businesses in any U.S. state that may have employees who live and work remotely in California. It's also worth noting that fines are tripled for infractions involving the personal information of minors (under the age of 16).

The CPRA also distinctly designates certain types of information as "sensitive personal information," some of which includes:

- driver's license numbers
- social security numbers
- state ID cards
- authentication (login) information
- financial account information
- debit and credit card numbers

In addition, geolocation, race, religion and ethnic information also fall into these categories.

## Wrap-Up

Privacy rights and regulations are not something to take lightly. Technology teams, in conjunction with Legal and HR divisions, are scrambling to adjust privacy policies and processes to overhaul existing (and in some cases, non-existent) privacy programs. Having the right people, policies and security in place is an essential first step to protecting your business. Knowledge and experience some could argue is equally as important.

## Contact Us

PKF O'Connor Davies is here to help you. If you have concerns about the new privacy rules, reach out to your engagement team or to our Cybersecurity and Privacy Advisory specialists:

[Thomas J. DeMayo](#), CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

Principal

Cybersecurity and Privacy Advisory

[tdemayo@pkfod.com](mailto:tdemayo@pkfod.com) | 646.449.6353

Our Firm provides the information in this e-newsletter for general guidance only and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.