The CPRA Will Soon Amend And Supplement The CCPA, Adding New Requirements Applicable To Covered Businesses With California Employees.

Is Your Organization Prepared?

Eliza T. Davis

Martin T. Tully

The landmark California Consumer Privacy Act ("CCPA") remains one of the most expansive and comprehensive consumer privacy laws in the United States. The CCPA, which became effective January 1, 2020, placed new restrictions on the collection, use, and sale of a consumer's personal information. In addition, the CCPA provided consumers with certain rights regarding their personal information collected by a covered business, such as the right to know, access, and delete such information. But as groundbreaking as the CCPA was, it still was not enough. Less than a year after the CCPA went into effect, California voted in favor of Proposition 24, which included the California Privacy Rights Act ("CPRA"). Effective on January 1, 2023, the CPRA replaces and amends parts of the CCPA in various important ways.

For example, last-minute amendments to the CCPA have provided employers with temporary exemptions regarding the collection and handling of employee personal data. Unlike other consumers, California employees of covered employers have not had the right to make data subject access requests (DSARs). However, these "Workforce Exemptions" are scheduled to sunset at the end of the year when the CPRA goes into effect. While the California legislature could still extend or adopt new Workforce Exemptions, it has not done so to date. Accordingly, covered employers with employees in California should be proactive and start implementing changes to their privacy practices and overall data governance to prepare for the expiration of the Workforce Exemptions.

Extraterritorial Reach

Preparing to comply with the CCPA and the CPRA's new requirements is not limited to California-based companies. It is important to remember that the CCPA and the CPRA can apply to employers who are not located in California. Rather, covered entities include businesses that:

- Are for profit and *do business* in the State of California;
- Collect personal information of California residents – including their employees, job applicants, and independent contractors;
- Determine the purposes or means of processing of personal information data; and
- Satisfy at least one of the following conditions:
    - Annual gross revenue of $25 million. Note that the California Attorney General has clarified in comments that the revenue threshold is not limited to revenue generated in California or from California residents;
    - Buys or receives for commercial purposes, sells, or shares the personal information of at least 50,000 consumers, households, or devices. The CPRA altered this requirement to apply to businesses that "alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households;" or

- Derives at least 50% of its annual revenue from selling consumers' personal information. The CPRA expanded this threshold requirement to "sharing" of personal information.

Moreover, businesses that conduct online transactions or simply have employees who are California residents must comply with the CCPA and CPRA despite having no physical presence in the state. This feature is important to note as the workforce becomes increasingly remote and mobile due to the global pandemic. Employees and independent contractors may start taking advantage of businesses' "work from anywhere" policies – and head West to seek sunshine and warmer weather in California. The trend towards a remote workforce also makes it all that more important to review current privacy and data governance policies to ensure compliance.

Employers' Current CCPA Obligations Will Change Under The CPRA

Employees are included within the definition of "consumer" under the CCPA, but they do not currently have all the same rights. The CCPA provides employees of and applicants for employment with a covered business with some limited rights, including (1) disclosure of a privacy notice at or before the point of personal information collection, and (2) a private right of action if their personal information is impacted by a data breach due to a failure of the employer to maintain reasonable safeguards. However, while the CCPA provides other consumers with rights related to accessing their personal information, employee and human resources data have been excluded from these requirements.

The CPRA expands the list of disclosures that employers must provide to employees and applicants at or before the time of collecting personal information. Under the CPRA, the privacy notice must include details about the types of personal information collected, the purpose for which the information is collected, and how long the personal information will be retained. In addition, businesses must indicate whether they will sell California residents' personal information and a notice of the right to opt-out of sales.

The CPRA Sunsets The Workforce Exemptions

If the CPRA is not amended, employees, applicants, and independent contractors will receive the same rights consumers have enjoyed under the CCPA beginning January 1st of next year. That means that employees, job candidates, and independent contractors who reside in California will have the right to request: (1) the deletion of their personal information; (2) the categories of personal information collected; (3) the purpose of collecting or selling personal information; (4) the sources from which personal information is collected; (5) to opt-out; and (6) the categories of third parties with whom the business shares their personal information. Notably, the current version of the CPRA would cover more information than what would typically be found in personnel files. The statute's broad definition of "personal information" would extend to email, spreadsheets, contracts, or other documents, all of which may have to be provided in response to an access request, free of charge. In addition, employees, job candidates, and independent contractors cannot be discriminated against by a business for the exercise of their CCPA privacy rights.

Consumer And Employee Personal Information Cannot Be Retained Indefinitely

Most organizations are familiar with the need to retain employee records and information for certain minimum time periods. Indeed, the temptation may be to retain employment information for great lengths of time, if not indefinitely. However, the CPRA does not permit indefinite retention of personal information of employees. In addition to expanding consumer privacy rights to employees and applicants residing in California, the CPRA explicitly includes a data minimization requirement. The CPRA provides that a business "shall not retain a consumer's personal information or sensitive personal information . . . for longer than is reasonably necessary."

Regulations To Be Promulgated Under The CPRA Are Unlikely To Defer Compliance Requirement

The CPRA also established a new agency, the California Privacy Protection Agency ("CPPA" or "Agency"), to implement and enforce the state's comprehensive privacy law. The Agency is the first of its kind in the country. As originally passed, the CPRA provides that the Agency is to finalize and publish regulations under the CPRA by July 1, 2022, to allow a six-month period for businesses to comply with the January 1, 2023 effective date. On May 26, 2022, the CPPA reiterated at its board meeting that completion of the rulemaking process will extend beyond July 1st, although draft proposed regulations will be on the CPPA's June 8, 2022 meeting agenda for consideration and potential action. Notably, however, there has been no indication that the CPRA's effective date will be pushed back commensurately.

Now Is The Time to Develop A Strategy for Compliance with the CPRA

The explicit data minimization requirement, coupled with expanded consumer rights, underscores the importance of having a comprehensive privacy policy and data governance program proactively in place. Covered businesses have little more than six months remaining to prepare for the CPRA. Under the CCPA, covered businesses were given 30 days to cure alleged violations before any administrative enforcement by the California Attorney General. Significantly, the CPRA eliminates that 30-day cure period permitted under the CCPA.

Therefore, businesses need to start developing a strategy now to be in compliance on January 1, 2023. Here are some key tips for an effective CCPA/CPRA compliance strategy:

Data Governance

California job applicants and employees will have rights to data access, portability, correction, and deletion, among others. Personal information includes emails, personnel files, HR data, spreadsheets, contracts, or any other document that can reasonably identify the employee. Without advance planning, businesses could be unprepared to deal with large amounts of data residing in multiple locations if employees request access.

Therefore, businesses should look now to tighten their data retention policies so they do not have to locate, gather, and produce large amounts of data in response to DSARs from their employees. In addition, businesses

should develop a defensible disposition procedure to regularly dispose of data that is past retention periods. Having carefully crafted data retention policies and deletion procedures will also ensure that businesses comply with the CPRA data minimization requirement by not retaining personal information beyond what is reasonably necessary.

Data Mapping

Another important step to building a comprehensive privacy program and data governance strategy is to know what personal information about employees, job applicants, and independent contractors your business collects, where it is stored, for what purpose it is collected and used, and to whom it is disclosed. Preparing a data map or inventory will allow businesses to make accurate representations in their privacy notices, timely, efficiently, and effectively fulfill DSARs, and comply with their own data retention program.

Implement Data Subject Access Request Protocols

As discussed, employees, job candidates, and independent contractors may request data access, deletion, correction, and to opt-out of the sharing of their personal information effective January 1, 2023. Businesses should develop efficient procedures for accepting and executing on DSARs. This process will include notifying employees, job applicants, and independent contractors of the actions the business takes to ensure compliance as well as documenting the same.

Update Privacy Policy & Privacy Notices

Employers should review and analyze their current privacy policy and privacy notices with an eye toward ensuring compliance with the CPRA. Currently, covered businesses must disclose certain required information in an online privacy policy or on an internet website, as applicable. This information includes an explanation of the rights consumers have under the CCPA and how they may exercise those rights. These disclosures must be updated, as applicable, every twelve (12) months.

Under the CPRA, privacy policies will have to be updated to include the new and modified consumer rights highlighted above. In addition, the CPRA requires that privacy notices include (1) the business or commercial purpose of "sharing" personal information and (2) a description of the new consumer right to limit the use of sensitive personal information and a link that will allow consumers to exercise that right. An employer's privacy policy and privacy notices that comply with the CCPA most likely will not be sufficient under the CPRA.

Employee Training

Businesses should consider implementing annual training regarding their retention policies, defensible disposition procedures, and data rights requests. Employee education is key to ensuring that any privacy and data governance program is effective.

Key Takeaway: Time Is Of The Essence

Covered businesses need to be proactive and not wait until the CPPA's regulations are published and finalized. Now is the time to craft or refresh a privacy and data governance program to ensure compliance with the CPRA when it goes into effect in little more than six months from now. Doing so is even more important now that the "right to cure" afforded under the CCPA will no longer be available under the CPRA.

Redgrave LLP will continue to monitor CPRA developments and provide guidance to ensure covered businesses can effectively comply with the CCPA/CPRA and its impending new requirements.

For additional information on this topic or further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*