How Cos. Can Prep For Enforcement Of Calif. Privacy Laws

By **Kendall Fisher-Wu** (January 26, 2023)

Kendall Fisher-Wu

By now, you have likely seen many posts about the California Privacy Rights Act, the changes it made to the California Consumer Privacy Act, and its general effect on the data privacy landscape in California.

But one of the biggest changes the CPRA brings to this landscape is the requirement that covered businesses provide their employees with the full scope of rights under the CCPA and CPRA.

This article provides an overview of how those changes affect the employer-employee relationship in California and some key takeaways for how your business can get up to speed.

Is your business subject to the CCPA and CPRA?

There are several ways for the CCPA and CPRA to apply to a business, most commonly the revenue threshold. If your business had annual gross revenues of more than $25 million in the previous year, the CCPA and CPRA apply to you.

Other ways a business might be covered by the laws include if the business shares common branding with and is controlled by another company that is directly subject to the laws.

In addition, if a business receives personal information from a covered business as a service provider, contractor or third party — such as a small company that runs background checks for a covered business — it too must comply with the CCPA and CPRA.

The CCPA and CPRA protect the personal information of consumers. A consumer is defined very broadly as a "natural person who is a California resident."

A business's employees and job applicants are covered by this broad definition. Personal information is any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with a particular consumer or household.

This is another very broad definition that includes most, if not all, of the information a business/employer receives from its employees and job applicants.

Why do businesses have to comply with the CCPA and CPRA now?

The CCPA, which was effective Jan. 1, 2020, always covered employees with its broad definition of "consumer," but it contained a temporary exception for employee information so that businesses largely did not need to comply with the law with respect to their employees.

The exception expired at the end of 2022, and the CPRA, which voters passed on the 2020 ballot, did not extend that exception.

So, as of Jan. 1, 2023, businesses need to fully comply with those laws and provide their employees with their complete scope of rights under the CCPA and CPRA.

What rights do employees and job applicants now have under the CCPA and CPRA?

Together, the CCPA and CPRA establish a plethora of rights for employees and job applicants regarding the personal information their employer collects and maintains about them. Below are the main rights under the data privacy laws:

- The right to request disclosure to them of the personal information that the employer has collected or stores about them;
- The right to request deletion of that personal information — with several exceptions laid out in the statute, such as information that an employer is required to maintain;
- The right to opt out from sharing of personal information — while this includes the sale of personal information, it also covers interest-based advertising;
- The right to opt out of certain uses and disclosures of sensitive personal information, a new category of personal information added by the CPRA that includes an employee or job applicant's social security number, passport number, union membership, genetic data, health data and a variety of other categories;
- The right to correct any inaccurate personal information the employer may have about the employee or job applicant; and
- The right to be free from discrimination by the employer for exercising any of the above rights.

If an employer receives one of the above verifiable requests, it must generally provide its response within 45 days. Employees and job applicants may submit up to two requests in a 12-month period.

Employers must provide at least two methods for submitting these requests, such as a dedicated email address and a toll-free phone number.

As noted above, the CCPA and CPRA provide several exceptions that a business might be able to invoke if an employee's request conflicts with other obligations or business needs, and these exceptions apply to the employment context in unique ways.

For example, the laws allow a business to retain information despite a request for deletion if the business is otherwise legally obligated to retain the information.

In the employment context, this could apply to employee records — the Labor Code obligates employers to maintain records about their employees for several years, so an employer may be able to invoke this exception and decline an employee's request for deletion of their payroll records.

The laws provide for several other exceptions that apply to a variety of employment situations, but employers should speak with counsel to determine if they can properly invoke any of those exceptions.

What needs to be in the notice at collection for employees and job applicants?

The CCPA already requires that a covered business provide its employees and job applicants with a notice at collection that informs them about the categories of personal information the employer collects and the reasons it collects each category.

This was just about the only thing employers had to do for their employees under the CCPA, and the requirement remains under the CPRA. This notice must be provided at or before the time of collection, which is the moment that the business acquires the personal information.

Typically, this means that the notice should be provided to employees during onboarding as part of the company's employee handbook and to job applicants alongside the job application.

For current employees, it is a good idea to circulate a standalone CCPA and CPRA notice at collection, and ask that employees sign a notice of acknowledgment and receipt of that notice.

The CPRA establishes a few additional requirements for the contents of the notice, including that the business must note the categories of sensitive personal information that it collects about employees or job applicants, the retention period for each category of data, and the reasoning behind each retention period.

In most circumstances, businesses should provide a different notice at collection to employees/job applicants than it does to customers.

The business likely collects different categories of information from employees, and for different purposes, than what it collects about its customers.

How can employers get in compliance with the CCPA and CPRA for employees and job applicants?

Any CCPA or CPRA compliance plan will be nuanced, especially when the peculiarities of California employment law are now in the mix.

An employment-focused CCPA or CPRA compliance plan will likely involve the following:

- Internally determining what categories of information the business collects about its employees and job applicants, the reasons that each category is collected, and the retention periods for each category — as well as the reasoning behind each retention category — and the systems by which it is collected or stored;

- Ensuring sensitive personal information or information that presents a high risk of harm to a consumer if disclosed — such as a Social Security number — is subject to a high level of data security and protection;

- Drafting or updating the business' privacy policy to inform employees of their rights established by the CCPA and CPRA;

- Establishing a procedure for responding to verifiable requests from employees and job applicants under the CCPA and CPRA in the required time frame;

- Drafting or updating the employee-facing notice of collection and making it available in a location accessible to both job applicants and employees, and disseminating the

notice to current employees, whether this is done via an update to the employee handbook or as a standalone policy; and

- Reviewing and updating contracts or data protection agreements with service providers, contractors or other third parties that receive employee personal information.

Conclusion

There is still some good news. Even though the new requirements went into effect Jan. 1, they will not be enforced until July 1, and enforcement will only look at violations that took place after July 1.

However, businesses should strive to get ahead with CCPA or CPRA compliance as soon as possible, particularly with regard to the new set of requirements that will apply to employees and job applicants.

Kendall Fisher-Wu is an associate at Hanson Bridgett LLP.