UNDERSTANDING THE CALIFORNIA PRIVACY RIGHTS ACT (CPRA): A BRIEF OVERVIEW WITH REGARDS TO EMPLOYEES

By Maureen M. Duffy and Christopher R. Nepacena

The California Privacy Rights Act (CPRA), often referred to as CCPA 2.0, is a significant modification of the California Consumer Privacy Act of 2018 (CCPA). The CPRA came into effect on January 1, 2023, and its enforcement is scheduled to begin on July 1, 2023. In addition to expanding the number of rights provided to consumers, the CPRA also ends the employee and the B2B exemptions provided under the original CCPA. This article provides a brief overview of the CPRA with regards to employees, its implications for businesses, and the key steps they should take to ensure compliance.

What is the CPRA?
The CPRA is an amendment to the CCPA, designed to strengthen privacy rights and protections for California residents. It introduces new requirements and expands upon the existing provisions of the CCPA.

New Requirements Under the CPRA
Companies that were compliant with the CCPA are not automatically compliant with the CPRA. Importantly, the original CCPA contained employee exemptions and B2B exemptions. The CPRA ends these exemptions and adds several new requirements, including:

- **Purpose Limitation:** Companies may only use personal data for the purpose for which it was originally collected;
- **Storage Limitation:** Personal data should be destroyed or deleted once the data has been used for its collected purpose;
- **Reasonable and Appropriate Security Measures:** Security for personal data must be appropriate for how sensitive the data is and the harm that would result because of unauthorized access; and
- **Additional Rights:** Right to correct, limit use, and protection against discrimination for exercising privacy rights.

The CPRA also introduces a new category of personal information called "Sensitive Personal Information," which entails specific compliance obligations.

Applicability of the CPRA
The CPRA applies to for-profit entities that conduct business in California and meet any one of the following conditions:

- Annual gross revenues (global) over $25 million, measured from January 1, 2022; or
- Annually buy, sell, or share personal information of 100,000 or more consumers or households. This threshold increased from 50,000 under the CCPA; or
- Derive 50% or more of their annual revenue from selling or sharing personal information.

CPRA and Employees
If the CPRA applies to a company, it also applies to the company's employees, remote employees, dependents of employees, job applicants, independent contractors, and board members ("Employees") who are also California residents. Remote Employees living in California are covered under the CPRA, irrespective of the employer's physical presence in California.

Requirements under the CPRA for Employers
The CPRA imposes obligations on employers to inform their Employees who are California residents about the collection and use of

employment-related Personal Information (PI). Employers must provide an Employee Privacy Notice ("Notice") at or before the time PI is collected (e.g., when a California resident applies for a job).

The Employee Privacy Notice is not the same as the original CCPA notice posted on a company's website. It is an additional notice that must be tailored to the company, including:

The Notice should include information on whether the employer sells or shares PI, the retention period for PI, and any third parties with whom PI is shared. It must also cover the categories of Sensitive Personal Information collected. The Notice should also inform employees about their Data Subject Rights (DSRs) and how to exercise them.

The difference between PI and Sensitive Personal Information.
PI is information that can reasonably be used to identify an individual but does not include information lawfully made available from a federal, state or local government or information that is deidentified or aggregated. An Employee's name, email address, photo, ID, address, and audio and video recordings are examples of PI.

Sensitive Personal Information is a subset of PI and includes the following:

- Financial information,
- Account log-in credentials,
- An Employee's identification number (e.g., Social Security number, driver's license number, etc.)
- Precise geolocation, racial and ethnic information,
- Personal communications (e.g., contents of an Employee's mail, email, and text messages unless the business is the intended recipient of the communication), and
- Information about an Employee's sexual orientation, genetic data, biometric, or health information.

DSRs under the CPRA
Consumers, including Employees, have various DSRs concerning their PI. These rights include the right to delete PI, correct inaccurate PI, Employers must provide an Employee Privacy know what PI is being collected, access PI, opt-out of selling or sharing PI, limit the use and disclosure of sensitive PI, and protection against retaliation following the exercise of their rights.

Best Practices for Responding to Employee DSR Requests
To effectively respond to Employee DSR requests, employers should:

- Create a "data map" to understand where data is stored. Data can be stored in many places such as HR systems or communication tools such as Slack or Teams.
- Verify the identity of the requester to ensure information is provided to the correct person.
- Respond promptly within 45 days of receiving the request.
- Provide clear and concise information in an easily accessible format.
- Maintain accurate records of DSR requests and actions taken including the request itself, any actions taken in response, and the date and time of the response. This will help businesses demonstrate its compliance with CPRA.
- Ensure data protection while providing PI.
- Train staff on responding to DSR requests to ensure compliance.

Exceptions and Enforcement of the CPRA
The CPRA includes exceptions to complying with DSR requests, such as legal compliance if your company is in pending litigation and is required to maintain evidence, access requests by government agencies, security or fraud prevention, internal business purposes where there's a legitimate business need to maintain information for business operation purposes, and excessive exercise of individual privacy rights. The CPRA grants enforcement authority to the California Privacy Protection Agency (CPPA) and the California Attorney General, with penalties for noncompliance starting from July 1, 2023. Penalties can range from $2,000 to $7,500 per offense, depending on the nature of the violation.

Conclusion
The CPRA introduces significant changes to

privacy rights and obligations in California, expanding upon the foundation laid by the CCPA. Businesses must understand the CPRA's requirements, including the new obligations for handling PI and Sensitive Personal Information, such as providing a notice to Employees at the time of collecting their PI, responding to DSR requests, and ensuring compliance to avoid penalties. By taking proactive steps and adhering to best practices, companies can meet the CPRA's standards while safeguarding privacy rights for their Employees and consumers alike.

Maureen D. Duffy
Partner
mduffy@donahue.com

Christopher R. Nepacena
Associate
cnepacena@donahue.com

DONAHUE FITZGERALD ATTORNEYS