masuda funai

News & Types: Client Advisories

New Year, New Data Privacy Regulations: California Consumer Privacy Act Now Regulates HR Data

3/30/2023

By: Naureen Amjad, Riebana E. Sachs

Practices: Employment, Labor & Benefits

Executive Summary

On January 1, 2023, substantive amendments to the California Consumer Privacy Act ("CCPA") took effect and the temporary exemptions of certain employees and business-to-business ("B2B") personal information expired, providing employees, job applicants, independent contractors and B2B contacts with the same CCPA protection and rights as California consumers. The amendments have expanded coverage to include all personal information of employees, contractors, applicants and B2B contacts of California employers. While the amendments are effective, enforcement is expected to be delayed until July 1, 2023.

What Is The CCPA?

California was the first state to introduce data privacy protection regulation on par with the EU's General Data Protection Regulation when it enacted the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CPRA"). The CPRA amendments created the first state agency focused exclusively on privacy: the California Privacy Protection Agency ("CPPA"). The CCPA provides consumers, who are California residents, with strong individual rights around their personal information and imposes various data protection duties on certain entities conducting business in California.

Who Is Now Covered?

The CCPA's definition of consumers includes California-based (1) employees and job applicants; and (2) contacts of and from business customers, vendors, or independent contractors. However, the CCPA previously included the following two temporary exemptions:

- The workforce personal information exemption, which applied to personal information a business collected about job applicants, employees, owners, directors, officers, medical staff members, or contractors for the business; and
- The B2B exemption, which applied to written or verbal communications or transactions between a business and an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship,

non-profit, or government agency, and communications or transactions with a business which occurred solely within the context of the business conducting due diligence.

As of January 1, 2023, these two temporary exemptions have expired and employees, candidates, independent contractors, and B2B contacts alike are now provided with the same CCPA protections and rights as other California consumers.

Among the CCPA's definition of covered businesses are: (1) affiliates with common branding; (2) joint ventures or partnerships; and (3) any for-profit entity doing business in California that meets at least one of the following thresholds:

- had annual gross revenue in excess of $25 million for the prior calendar year;
- annually buys, sells, or shares the personal information of more than 100,000 California residents; or
- derives at least 50% of annual revenue from selling or sharing the personal information of California residents.

What Should Employers Do Now?

The CPPA is currently in the process of preparing regulations and guidance to implement the CPRA's substantive amendments to the CCPA, which are expected to be finalized in the next several months. Nevertheless, employers should start to evaluate and address their obligations under the amended CCPA. Specifically, employers should:

- Evaluate threshold matters to determine if their organization is subject to the CCPA.
- Understand how their organization collects, processes, uses, and discloses the personal data of California residents (e.g., names, dates of birth, governmental identification numbers, etc.). The CCPA imposes data minimization and purpose limitation requirements, as well as retention restrictions.
- Prepare or update notices to employees, job applicants, independent contractors, business customers and vendors.
- Audit data security practices and procedures. Covered employers must review their cybersecurity policies, incident response policies and other processes to minimize potential risk of data exposure.
- Determine how requests to exercise data privacy rights can be addressed. Covered employers must consider California labor rules regarding employee rights to access personnel files when establishing such a process. In addition, employers should examine the use and disclosure of certain sensitive personal information (e.g., race, health or medical conditions, sexual orientation, etc.) to ensure that such uses do not trigger employees' right to limit the use of such information.
- Review service provider agreements with third-party human resource service providers to ensure that they will be able to assist covered employers in meeting their obligations under the CCPA.

The recent amendments to the CCPA demonstrates a larger trend towards increased regulation in the area of privacy law. As a result, California employers must be cognizant of how their workplaces collect, manage and disclose data, revising existing policies and procedures, where necessary, in order to be compliant with the new law.

Please contact Naureen Amjad, Riebana E. Sachs or a member of the Employment, Labor and Benefit Group with any questions.