STINSON

News & Insights

California Consumer Privacy Act's Employee and Business-to-Business Exemptions Expire Effective January 1, 2023 *How Should Employers Prepare?*

Alert
12.16.2022

By Steve Cosentino (CIPP), Carrie Francis, Abigail Flores and Lisa Rippey

The California Consumer Privacy Act (CCPA) took effect on January 1, 2020, providing rights and protections to California consumers regarding their personal information and how it may be processed by certain businesses. Initially, certain businesses were temporarily and partially exempt from some CCPA requirements if the personal information being processed (1) was human resource information regarding the business' past and current employees, job applicants and individuals in an otherwise-related position (e.g., owners, directors, officers, contractors and beneficiaries/dependents) (workforce members); or (2) was collected in a business-to-business (B2B) context. The exemptions are set to expire on the effective date of the California Privacy Rights Act (CPRA), which is January 1, 2023, unless they are otherwise extended by the California legislature.

The exemptions were not extended during the 2022 legislative session. The employee and B2B exemptions will expire effective January 1, 2023. This means that personal information collected in certain employee contexts and in a B2B context will be subject to a number of additional data privacy requirements under the CCPA, as amended by the CPRA.

NEW DATA PRIVACY RIGHTS FOR WORKFORCE MEMBERS

Below is a sampling of the workforce members' new data privacy rights under the CCPA, as amended by the CPRA:

California Consumer Privacy Act's Employee and Business-to-Business Exemptions Expire Effective January 1, 2023 *How Should Employers Prepare?*

Right to Know

The CPRA grants workforce members the right to know about the personal information a business collects about them. While the California Labor Code already provides workforce members the right to know about certain information an employer has collected, such as payroll records (Labor Code § 226), signed documents (Labor Code § 432), and personnel files (Labor Code § 1198.5), workforce members have a right to additional information under the CPRA, such as geolocation, biometric information, internet activity, and inferences drawn.

Right to Delete

Under the CPRA, workforce members have the right to delete personal information collected from them, subject to certain exceptions. For example, the CPRA does not require businesses to delete personal information that they need to comply with a legal obligation. Therefore, employers will need to assess federal, state and local retention requirements when responding to a workforce member's deletion request, including but not limited to the Family Medical Leave Act, the Fair Labor Standards Act, the Americans with Disabilities Act, the California Labor Code § 226, and the California Government Code § 12946.

Right to Correct Inaccurate Information

The CPRA gives workforce members the right to correct inaccurate personal information. The employer must use "commercially reasonable efforts" to correct the inaccurate personal information upon the workforce member's request.

Right to Limit Use and Disclosure of Sensitive Personal Information

Workforce members will now have the right to limit the use and disclosure of "sensitive personal information." Sensitive personal information includes precise geolocation data, racial or ethnic origin, union membership, biometric information, and a workforce member's email and text message content. However, employers can collect sensitive personal information if it is being used for diversity and inclusion purposes.

NEW DEFINITION OF CONTRACTOR

The CPRA also adds a new definition for a "contractor." Companies would typically understand a contractor to be a service provider, providing services to the company for the company's business purpose. However, for CPRA/CCPA purposes a "contractor" is a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business. The distinction here is that the business purpose can be the contractor's business purpose, as opposed to

solely the company's business purpose. Examples include ancillary human resources benefits where the benefit is not being provided by the company but is instead offered as a perk and once the person engages with the contractor, they become the contractor's client. This would occur if a company offered employees a discounted service with a consulting company or a company that provides software for individuals. Once the employee signs up, they become the customer of the contractor operating under the contractor's business purpose. This differs from a vendor hired to administer a company sponsored benefit plan. In the latter case, the vendor would be a service provider under the CCPA.

WHAT EMPLOYERS SHOULD DO TO COMPLY WITH THE CCPA AND CPRA

In addition to updating the CCPA privacy notice to incorporate the new rights provided to the workforce members, employers should also take the following steps to comply with the CCPA and the CPRA:

- Review the personal information that the employer collects from workforce members
  To ensure that the privacy notice accurately describes the categories of personal information that the employer collects, uses and distributes, and to identify sensitive personal information, employers should first take an inventory of what type of personal information it collects from the workforce members.

- Review and update existing employee policies and procedures
  In light of the CPRA, employers should review their existing employee policies and procedures, including human resource-related privacy policies and internal data retention procedures, to consider whether they comply with the collection, use, retention and sharing standards set forth in the CPRA. If they do not, such policies and procedures should be updated.

- Update job applications and other privacy notices
  Employers should incorporate personal information collected in an employment context into their job applications and privacy notices.

- Enter into data processing agreements
  Employers should assess the personal information collected by service providers and then implement a Data Processing Agreement or Addendum (DPA) to be included in service provider relationships involving a workforce member's data. DPAs are important to ensure that vendors are deemed "service

providers" under the CCPA as opposed to "third parties." The CCPA's requirement to permit individuals to opt-out of data sales and sharing with third parties could make some HR services impossible to perform. The definition of "sale" under the CCPA is much more broad than simply an exchange for monetary consideration.

- Review and catalogue any vendors that fall in the contractor category
  The CCPA requires a business to enter into a contract with the contractor that contains three additional terms: (1) to refrain from selling the personal information, (2) to refrain from retaining, using or disclosing the information outside the direct business relationship between the recipient and the business, and (3) to certify that the contractor understands the above contractual restrictions. This can take the form of a modified version of the company's DPA.

- Develop a process for workforce member requests
  Employers should develop a process for accepting and making determinations on workforce member requests regarding their personal information. This process should include identifying a mechanism for workforce members to make such requests, identifying the person who will receive the requests, and training staff on how to respond to such requests.

While the employee and B2B exemptions expire on January 1, 2023, enforcement of the new CPRA requirements will not begin until July 1, 2023. Employers who have not yet done so should consult legal counsel to ensure their policies, processes, notices, contracts and job applications comply with the stringent requirements of the CPRA. The California Privacy Protection Agency is currently working on regulations to implement some of the basics of the CPRA. Those regulations have yet to be finalized so further revisions to policies and procedures may be required when the new regulations go into effect.

CONTACTS

Stephen J. Cosentino, CIPP

Lisa M. Rippey

RELATED CAPABILITIES

Business Litigation

Cybersecurity & Data Privacy

Intellectual Property & Technology

California Consumer Privacy Act's Employee and Business-to-Business Exemptions Expire Effective January 1, 2023 *How Should Employers Prepare?*

Labor, Employment & Benefits