## Services

Privacy & Data Security

# CCPA Employee and B2B Exemptions Set to Expire on Jan. 1, 2023: What Employers Should Do To Prepare

Up until now, employment data and business-to-business (B2B) data had been exempted from most of the California Consumer Privacy Act (CCPA) requirements. The California legislature had been considering multiple bills to extend the exemptions. Unfortunately, on August 31, the California legislature adjourned without extending the exemptions. This means that on Jan. 1, 2023, all the consumer rights that currently exist will apply equally to employee personal information collected by employers, as well as Personal Information collected in the context of "providing or receiving a product or service to or from" a business (B2B).

Currently the CCPA contains a limited exemption for personal information collected by a business about an individual who is a job applicant or employee, owner, director, or independent contractor of the business. The exemption is limited in that it only applies when such information is collected and used "solely within the context of [the individual's] role or former role" as a job applicant, employee, owner, director, or independent contractor. In the context of a B2B relationship, businesses are exempt from the requirement to provide notice of the collection, and the broadly defined "consumer" does not have a right to know or right to delete the information. With these exemptions set to expire, California will become the first state to apply comprehensive restrictions on the collection and use of these categories of information.

Concerns have been raised about the impact of this change on existing California employment law rights and obligations, as there is potential confusion because most of the rights under the CPRA are not easily applicable in the employment context. Notably, other state privacy laws (Colorado, Connecticut, Utah and Virginia) do not apply to employment data. These four states exclude individuals acting in an employment context from the definition of "consumer."

Businesses should assess how consumer rights apply to employees and to their B2B relationships, and prepare to provide each with CCPA or California Privacy Rights Act (CPRA) rights, including the right to know, the right to correct, the right to delete, the right to opt out of the sale or sharing of personal information, the right to limit use and disclosure of sensitive personal information, and the right to be free of retaliation following opt-out or exercise of their privacy rights.

We suggest businesses start reviewing and updating their internal processes and procedures and, at a minimum, perform these initial steps:

**Key Contacts**

**Jon Breyer**
*Minneapolis*
(612) 334-5057
jon.breyer@kutakrock.com

**Nicole Moriarty**
*Washington, D.C.*
(202) 828-2446
nicole.moriarty@kutakrock.com

### 1. Determine CCPA/CPRA Applicability

Determine whether your business is subject to the CCPA and CPRA. CCPA and CPRA only apply to for-profit organizations that do business in California that: (i) have annual gross revenue in excess of $25 million in the preceding calendar year; (ii) buy, sell, or share the personal information of 100,000 or more consumers or households per year; or (iii) generate 50% or more of their annual revenue from selling or sharing the personal information of consumers.

### 2. Data Inventory and Mapping

Start inventorying and mapping the employee and B2B data collected to determine what personal information the business collects, how it handles personal information, and whether the data is sold or shared with third-parties. Importantly, the CPRA includes a 12-month "look-back" provision that requires businesses to identify all information collected since January 1, 2022.

As it relates to employee data, the CCPA's definition of "personal information" is quite broad and extends beyond personnel files and payroll data to include usage data, photos, audio and video recordings, biometric data, key swipe records, network logs, geolocation data, insurance and benefits elections, bank and direct deposit information, emergency contacts, dependents, resume and employment history, performance evaluations, wage statements, time records, compensation history, and many other forms of data collected during the employment relationship. Moreover, the CPRA introduces a new concept of "sensitive personal information" (such as financial information, social security numbers, health information, and biometrics) that must be considered and inventoried by the employer.

### 3. Privacy Disclosures

Review the business's privacy policy to ensure it includes the required CCPA disclosures and notices. Certain disclosures must be made at or before the point of collection. Businesses will need to provide more detailed privacy disclosures to employees and B2B contacts that explain what personal information the business collects, how that information is handled and for what purpose, and what rights an employee has with respect to that information.

### 4. Employee Requests

Develop a mechanism for employees to make requests regarding their personal information. Businesses must develop internal and external policies and procedures for accepting, verifying, and responding to employee requests to access, correct, and delete personal information collected on the employee. Businesses also need to analyze whether they are "selling" or "sharing" employee personal information and, if so, allow employees to opt out. Finally, businesses will need to consider whether they are collecting sensitive personal information and, if so, whether they must provide employees with the right to limit the business's use of such sensitive personal information.

Access requests may also be precursors to litigation, especially from former employees. Thus, deciding how to respond to these requests will be an important consideration.

### 5. Data Agreements

Begin drafting addendums or amendments to data processing agreements for all transfers of personal information to other entities. This includes transfers to service providers, contractors and third parties.

For questions concerning how to implement any of these measures or for assistance with a CCPA/CPRA compliance program, contact Kutak Rock's Privacy and Data Security Group.