Blogs
April 20, 2023

The exemption for employment-related and business-to-business (B2B) data under California's privacy law expired on January 1, 2023. Without this exemption, information previously allowed to be excluded now falls within the scope of California's extensive privacy requirements, including notice and transparency, data minimization, and data subject rights requests.

In this blog post, we provide an overview of the now-expired exemptions and offer next steps on the requirements that now pertain to employment and B2B data.

What Was California's Exemption?

The California Consumer Privacy Act (CCPA) temporarily exempted employment-related and B2B data from all obligations imposed under the law other than the obligation to offer an opt-out for "sales" of personal information and the obligation to provide "notice at collection" until the effective date of amendments brought about by the California Privacy Rights Act (CPRA).

In particular, the temporary exemptions applied to: (1) personal data of job applicants, employees, owners, directors, officers, and independent contractors in the context of the individual's employment or application for employment and (2) personal information reflecting written and verbal communications or a transaction where the consumer is acting in a B2B commercial transaction (i.e., B2B data).

It was widely expected that the same exemptions would be carried forward to the CPRA amendments. However, the California legislative session closed last year without these exemptions being codified, making California the first state to apply comprehensive restrictions on the collection and use of such information. Because the chance that the law will be modified through implementing regulations or that a grace period will be added seems increasingly unlikely, employers and businesses should take action toward compliance given that there are less than six months until the contemplated July 1, 2023, enforcement deadline.

What Obligations Now Apply to Employment and B2B Data?

The expired exemption of employment and B2B data from the requirements of California's privacy law means that previously excluded information now falls within the scope of legal obligations that previously applied only to *consumers'* personal information. Below we outline these requirements with respect to employment and B2B data.

- **Notice and transparency.** Businesses must update their privacy policies and notice at collection to meet the requirements of the law to describe the collection, use, retention, and disclosure of employment and B2B data. For employment data, this typically entails a separate employee privacy policy and notice at collection. Note that terminology here is key, as applicants and independent contractors are covered by the scope of the CPRA, but they are *not* employees. Co-employment claims may arise if businesses refer to all groups as "employees." Thus, consider whether to have separate privacy notices for applicants and independent contractors.
- **Data minimization.** The collection, use, retention, and sharing of employment and B2B data must be "reasonably necessary and proportionate" to achieve the purposes for which it was collected or processed or for another disclosed purpose that is compatible with the context in which it was collected.
- **Data security.** To protect employment and B2B data from unauthorized or illegal access, destruction, use, modification, or disclosure, businesses must implement reasonable security procedures and practices appropriate to the nature of the data. While this may be a lighter lift in the case of B2B data, given that it generally consists of business contact information, companies should think carefully about the types of measures needed to secure potentially sensitive employee data (e.g., diversity, equity, and inclusion (DEI) data and health benefit information).
- **Contractual agreements**. Companies should ensure that their agreements with service providers, contractors, and third parties to whom employment and B2B data are disclosed include required contractual provisions detailing the nature, scope, and purpose(s) of the processing.
- **Individual rights.** Employees and individuals whose B2B data is collected (generally speaking, this will be business contact information) have new consumer rights, including rights to deletion, correction, access, and the right to opt out of certain processing activities. Businesses should evaluate whether these rights should be limited to California residents. Doing so may raise employee relations issues as team members may express concerns about the collection and usage of their personal information on a

perceived inequitable basis. This may be especially problematic for employers that are facing a historic surge of union-organizing campaigns.

California has yet to provide guidance on this topic, making it somewhat unclear as to how these traditionally consumer-facing rights and obligations now translate practically with regard to employee and B2B interactions. Nonetheless, companies should take steps now for what could be a significant undertaking to prepare for compliance. Below we outline key steps to take in this regard:

- **Data map.** The first step to prepare for compliance with the above obligations is to conduct data mapping of employment and B2B information. This step is essential for understanding what categories of information are collected, how that information is used, and where the information is stored. In the context of employment data, moreover, it is typical for the data to be stored throughout the enterprise, spread across human resources (HR) centers, off-site storage, and various human resources information systems (HRIS). It will take time and effort to interview key stakeholders to ensure all data is appropriately accounted for.
- **Determine if data is within scope.** Particularly for employers, once the data mapping is complete, companies must categorize that data as either "professional employment-related information," which is within the scope of CPRA, or "company" data not considered employee personal information (PI). In some cases, this decision may also require an update to company policies regarding the acceptable use of email, mobile devices, handbooks, and other data-containing entities. This is also a good time to reevaluate the company's document retention policies.
- **Determine if the data is being sold or shared.** Evaluate whether there is any "sale" or "sharing" of employment or B2B data. "Sale" refers to disclosing a consumer's personal information to a third party for monetary or other valuable consideration. Sales have been very broadly interpreted by the California Attorney General and cover any scenario that involves a business disclosing personal information to a third party, with a few limited exceptions. Generally, "sharing" occurs when a business discloses personal information to an external third party for the purpose of displaying ads to consumers on non-affiliated websites or apps. If the company engages in either or both of these processing activities, it needs to (1) prominently disclose such activity to employees and consumers through its privacy policy and other required notices, (2) offer individuals the ability to opt out of that activity via an opt-out link, and (3) effectuate opt-out requests.
- **Evaluate sensitive PI use.** Determine what "sensitive" PI is collected, evaluate how it is used, and determine if appropriate notice and ability to limit disclosure are needed. Sensitive PI includes information such as an individual's government identification (driver's license, passport numbers, state identification, and Social Security numbers); precise geolocation; ethnic or racial origins; biometric data and genetics; union membership; religious or philosophical beliefs; private communications content (text, mail, or email) where the company is not the intended recipient of such communications; and information about one's sexual orientation, sex life, or health. From an employment perspective, DEI data and certain geolocation data can be potentially problematic. A careful review is necessary to determine if the company is inferring characteristics about the employee based on the information. If so, special rules apply. With respect to B2B data, this is generally a nonissue for most companies, given that the types of B2B data collected generally do not rise to "sensitive" PI.
- **Determine who will handle data subject access requests (DSARs).** Consider whether to partner with an external vendor to verify the identity of requesting individuals, track requests, and respond to DSARs. Although it's difficult to gauge how many employee requests may initially come through, some employers are seeking to mitigate this risk by initially limiting DSARs to California residents. As for employment data, regardless of geographic scope picked by the employer, coordination with in-house human resources and legal teams will be needed, as the response deadlines for CPRA are typically within **45 days** of a request, with a one-time 45-day extension where "reasonably necessary." However, the California Labor Code typically requires the production of personnel files within **30 days** and payroll records within **21**

days. Ineffective coordination may lead to late production of documents, the imposition of fines and penalties, and may open the door to potential class-action risk. This is particularly concerning in that a failure to provide personnel files allows the plaintiff to receive attorneys' fees—making a violation of the CPRA a shoo-in claim to be tacked on to a variety of other claims in order to seek plaintiffs' fees and costs.

- **Be flexible.** Given the current state of the implementing regulations and the lack of enforcement examples ahead of the July 1 enforcement date, flexibility is key, and companies will need to be nimble and potentially change course or modify compliance strategies.

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field. Subscribe ?

View the blog