Special Alert: Data Privacy Law Exemption for Businesses with California Workers Will Expire December 31, 2022

Traditionally, the focus in California at the end of the legislative session is on the numerous new laws that were actually enacted and impose new compliance obligations. This year, however, the biggest compliance challenge may flow from something the California legislature failed to do. Specifically, the California legislature ended this year's session without extending employers' partial exemption from certain requirements under the California Consumer Privacy Act of 2018 (CCPA) and California Privacy Rights Act of 2020 (CPRA), California's consumer privacy law.

Therefore, the exemption will expire December 31, 2022, making California the only state with such "consumer privacy laws" without an exemption for employment or human resource-related information. Equally concerning, California is heading towards applying the CCPA in the employment context – which most understood it was not intended to do in the first instance-- without providing essential notice and practical guidance. Accordingly, companies that do business in California and employ, interview, receive job applications from, or independently contract with California workers should take action to ensure that they comply with the CPRA or that they are exempt from the law.

Background: Confusion About the CCPA Results in an "Employment Exemption" that Will Soon Expire

Broadly speaking, the CCPA provided consumers rights to (1) notice of collection and sharing of their personally-identifiable non-public information, (2) disclosure of data collected, (3) right to opt-out of sale and sharing of data, (4) deletion on demand, with some exceptions, and (5) reasonable safeguarding of data collected about the consumer by the business. Effective January 1, 2023, consumers will also have the right to request correction of inaccurate information.

As originally enacted, the statute simply defined consumers as natural persons who are California residents, and did not explicitly address whether the CCPA applied in the workplace setting, including to employees and/or job applicants. It was generally understood it was not intended to apply in such settings, including since California already has more specific rules regulating the workplace, including Labor Code section 1198.5 permitting employees to review their personnel files.

Apparently recognizing that imposing these requirements on employers in connection with information related to their workers or applicants would interfere with or complicate employer compliance with existing labor, employment, health privacy, and other laws, the legislature enacted a temporary exemption to certain specified provisions of the CCPA/CPRA. Specifically, the legislature exempted employers from complying with workers' employment data disclosure and deletion demands related to information gathered about employees or job applicants within the normal employment relationship. The CPRA amended the CCPA and extended the employment exemption through the end of 2022.

With this exemption in place, employers subject to the CPRA have only had limited compliance requirements including providing notice to employees, applicants, independent contractors, and other workers (Workforce Members) at the time personally-identifiable non-public data is collected, and ensuring reasonable data security measures are in place.

Many employers understandably anticipated the workforce exemption would either be made permanent, or would be further extended until the privacy law was amended to take into account the challenges of implementing consumer rights in the highly regulated workplace setting. Instead, the exemption will expire, largely because labor groups conditioned further extensions upon further broad reaching employment law changes. Complicating matters further, the CCPA includes a one-year "look-back"

period, which means that employers must be prepared to disclose and respond to CCPA requests regarding data collected from January 1, 2022 forward.

This alert includes a broad overview of the expanded obligations of employers with respect to workplace data. However, the applicable laws and regulations are complex and include nuanced rules and exceptions that exceed the scope of this summary. Moreover, applicable regulations are still being prepared. Businesses with question about whether and how these laws apply to their operations are urged to consult legal counsel.

Which Businesses Are Covered?

The CCPA applies to businesses that satisfy all three of the following criteria:

1. The company does business in California; *and*
2. The company is a for-profit business; *and*
3. The company meets *any* of the following thresholds (effective January 1, 2023):
    a. Has gross annual revenues over $25 million; *or*
    b. Buys, receives, or shares the personally-identifiable information of 100,000 or more consumers or households; *or*
    c. Derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

The CCPA also imposes separate obligations on service providers (which process personal information on a business's behalf) and other recipients of personal information from businesses.

What Type Of Employee Information Will Be Covered?

The CCPA regulates collection and use of "personal information," which is defined as information that directly or indirectly identifies, relates to, or describes a particular consumer (including a Workforce Member), or a household; or is reasonably capable of being associated with or linked to a person or household. The CCPA lists categories and examples of personal information, including many types of information typically collected by employers from Workforce Members, including, for example:

- Identifiers, including name, home address, telephone number, email address, social security number, or driver's license number.
- Personal information including signature, education, employment history, bank account number, medical information, or health insurance information.
- Characteristics of protected classification under California or federal law, such as race, religion, gender, age, etc.; requests for family and medical leave, and requests for pregnancy disability leave.
- Biometric information, such as fingerprints, faceprints, and voice recordings.
- Internet or other similar network activity, including browsing or search history.
- Geolocation data, such as the location of company-issued laptops or mobile devices.
- Professional or employment-related information, sch as work history, prior employer, human recourses data.
- Non-publicly available educational information, such as grade point average and school transcript.

Personal information does *not* include publicly available information, and the CPRA exempts some personal non-public information that is already subject to state and federal privacy laws, such as HIPAAA and CMIA (California's Medical Information Act). However, the law is likely to be broadly applied to cover anything from IP addresses, background search results, and resumes from online applicants, to Covid 19 vaccination, temperature, or exemption status of employees and vendors on premise, to more traditional data such as employee files and non-public home contact information.

In addition, the CRPA adds a category of "Sensitive Personal Information," which is a subset of personal information subject to additional restrictions only if the business collects or processes that information with the purpose of inferring characteristics about the individual.

What New Obligations Will Covered Businesses Have as of January 1, 2023?

Even before January 1, 2023, covered businesses were required to provide collection notices to their Workforce Members before collecting personal information and were required to adequately protect collected personal information. The collection notices must contain the categories of personal information the business collects and the intended use purposes for the categories of personal information. The CPRA expands these pre-collection disclosure obligations. As of January 1, 2023, covered businesses will *also* need to include disclosures regarding sensitive personal information, information about whether any personal information is sold or shared, and the retention period for each category of personal information or sensitive personal information or the criteria used to determine the relevant retention period.

Additionally, as of January 1, 2023, Workforce Members will have *new rights* with respect to their personal information, including the rights to:

- Know what personal information the business collected, sold, shared or disclosed about them, including specific pieces of personal information held.
- Require the business to correct inaccurate personal information.
- Require the business to delete their personal information (with some exceptions).
- Opt-out of the sale or sharing of their personal information by their employer and employer's vendors.
- Restrict the use and disclosure of their sensitive personal information.
- Not be retaliated against for exercising these rights.

Covered businesses will have commensurate new obligations in connection with Workforce Members' personal information, including obligations to:

- Provide extensive privacy notices;
- Respond to data rights requests;
- Limit uses and disclosures of personal information;
- Obtain specific contractual commitments from third parties receiving personal information; and
- Refrain from discriminating or retaliating against Workforce Members for exercising their privacy rights.

Notably, even if the CPPA applies to a particular business, the CPPA includes exceptions that limit which data is subject to consumer privacy requests. California's newly minted Privacy Protection Agency provides some helpful guidance, noting:

- *A business may refuse to disclose personal information if:*
    - The business cannot verify the requester's identity to complete the request;
    - The request is manifestly unfounded or excessive, or the business has already provided personal information to the requester more than twice in a 12-month period;
    - Disclosure would restrict the business's ability to comply with legal obligations, exercise legal claims or rights, or defend legal claims; or
    - The information is publicly available information, certain medical information, consumer credit reporting information, or other types of information exempt from the CCPA.
    - Further, businesses cannot disclose certain sensitive information, such as social security numbers, financial account numbers, or account passwords, but must disclose if they're collecting that type of information.
- *A business may refuse to delete personal information if:*
    - The business cannot verify the requester's identity to complete the request;
    - The business needs the requester's information for employment purposes, such as for payroll, government data reporting, and health care;
    - The business needs the information to perform a contract between he business and the employee, such as to award stock options or pension benefits;
    - The information is contained in security logs to satisfy compliance requirements and litigation demands;
    - The business needs the information to comply with other laws applicable to the business, such as needing to retain employment records for the required data retention period;
    - Deleting the information prevents the business from exercising their legal rights, such as to retain the information to defend against possible legal claims; or
    - The information is publicly available information, certain medical information, consumer credit reporting information, or other types of information exempt from the CCPA

What Steps Should Covered Businesses Take?

Covered entities should plan and implement a reasonable compliance program by January 1, 2023, including:

- **Identify Which Data Is Subject to CPPA Requests**: Identify what personally-identifiable non-public data the business collects about Workforce Members, if the business has not already done so. Once workforce data collected is identified, the business must determine which data can be withheld from disclosure, correction, and deletion requests (as discussed above). This is also an opportune time for businesses to implement "data minimization" policies by choosing not to collect unnecessary data.

- **Update Privacy Policies.** The policy must include instructions explaining how Workforce Members can request disclosure or deletion of data**.**
- **Plan for Processing Privacy Requests:** Prepare forms and a plan for processing requests for disclosure, correction, and/or deletion of Workforce Members' personal information within specific time frames. The statute and regulations include limits on what consumers are entitled to, so thoughtfully comparing the data your business collects with the laws, and integrating those limits in this process may limit the burden and risk on your entity. Processing these requests also requires the business to determine how to authenticate each request to ensure that employee data is not inadvertently provided or deleted in response to a spoofed demand from hackers or estranged partners, for instance.
- **Train Employees and Vendors** who will be implementing this plan. Include the entities' IT and HR personnel in planning and training.
- **Update Existing Notices of collection and data security protocols** to ensure they remain compliant with the evolving privacy laws and advances in technology.
- **Review and update records retention policies** and update recordkeeping practices.
- **Update Terms with Service Providers** who handle employee/applicant data or whose employees' data are collected by your business.
- **Insurance:** Review and consider insurance policy coverage, for instance cybersecurity policies both to ensure adequate coverage and to ensure that the businesses reasonable safeguards satisfy any insurance prerequisites.

Covered employers may wish to continue monitoring the currently pending federal American Data Protection and Privacy Act (H.R. 8152), which potentially could preempt the CCPA and CPRA.

What are the Liability Risks?

Companies that fail to comply with these rules face the risk of private actions (individual or class actions) and agency enforcement including steep civil penalties and injunctions. In addition, employers may face claims for discrimination or retaliation from Workforce Members who exercise rights under the privacy laws.

If you have questions or would like assistance assessing your obligations under the CCPA/CPRA, please contact us.

- Jennifer Arnold (jarnold@wilsonturnerkosmo.com)
- Hugh Kim (hkim@wilsonturnerkosmo.com)
- Katie M. McCray (kmccray@wilsonturnerkosmo.com)