DAVIS GILBERT

Labor + Employment

California Employers: California Privacy Rights Act in Full Force on Jan. 1, 2023

The Bottom Line

- Employers' obligations will expand considerably as of Jan. 1, 2023, given the expiration of the CPRA employee-data exemption.
- California employers will need to comply with notice obligations and new individual rights, such as access and deletion.
- California employers should take steps now to get into compliance ahead of Jan. 1, 2023, including taking inventory of employee, applicant and independent contractor information collected, where it is stored and how it is used, and update their privacy policies.

When the California Privacy Rights Act (CPRA) takes effect on Jan. 1, 2023, covered businesses will be subject to the same rigorous requirements for the collection, retention and use of employee information as the CPRA requires for consumers. Covered companies will need to publish privacy policies applicable to employee data, provide certain notices and be prepared to respond to data access requests, among other requirements.

When the current California Consumer Privacy Act (CCPA) took effect on Jan. 1, 2020, it imposed numerous new privacy disclosure obligations on businesses that collect personal information from California consumers. It also provided those consumers with numerous rights, including the right to know what personal information about them has been collected, the right to delete such personal information and the right to opt-out of the sale of their personal information. Most obligations under the CCPA did not apply to personal information a business collects about job applicants, employees, officers or other individual's roles within the business. However, this so-called employee exemption is set to expire on Dec. 31, 2022 – which is why the employee data protection obligations will take effect at the beginning of the new year.

Covered Businesses

The CPRA applies to a covered business, which is defined as a company or other legal entity that collects consumers' personal information, does business

in California, **and** that (i) had annual gross revenues for the preceding calendar year of at least $25 million, (ii) annually buys, sells or shares the personal information of at least 100,000 consumers **or** (iii) derives at least 50% of its revenue from selling or sharing consumers' personal information. A "consumer" is any person who is a California resident, which includes California employees, independent contractors and employment applicants.

What is Personal Information and Sensitive Personal Information?

Under the CPRA, "personal information" is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." It includes, but is not limited to:

- real name
- postal address
- unique personal identifier
- Internet Protocol address
- email address
- Social Security number
- biometric information
- geolocation data
- inferences drawn from any of the personal information

It also includes "sensitive personal information," to which discrete requirements apply as outlined below. Examples of sensitive personal information include information that reveals an individual's Social Security, driver's license, state identification card or passport number, precise geolocation, the contents of the individual's mail, email and text messages (unless the business is the recipient of the communication), and racial or ethnic origin, religious or philosophical beliefs, or union membership, among others.

Pre-Collection Notice Requirement Expanded

In addition to being required to inform individuals (including job applicants and employees) of the personal information collected and the purposes for which the categories of personal information shall be used, businesses must inform individuals of whether the information is sold or shared (such as being provided to a payroll vendor or insurance company). Further,

if the business collects sensitive personal information, these same requirements apply to such information. Finally, businesses must include in the notice the length of time the business intends to retain each category of personal information, including sensitive personal information. Importantly, businesses cannot retain such information for longer than is "reasonably necessary" for the disclosed purpose that the information was collected.

Right to Delete Personal Information

Under the CPRA, individuals have the right to request that a business delete any personal information about them that the business has collected from the individual, and businesses must notify individuals of this right. A business that receives such a request must not only delete the individual's personal information from its records, but also notify any service providers or contractors to delete the individual's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the individual's personal information unless this proves impossible or involves disproportionate effort. Businesses can, however, maintain certain personal information despite a deletion request for a number of stated purposes, including to complete a transaction, to comply with a legal obligation and for internal uses that are reasonably aligned with the expectations of the data subject. These exceptions may be sufficient to cover much of the information and data collected about applicants and employees.

Right to Correct Inaccurate Personal Information

Individuals have the right to request that a business that maintains inaccurate personal information about the individual correct that inaccurate information, and businesses must notify individuals of this right and use commercially reasonable efforts to correct the inaccurate personal information.

Right to Know What Personal Information has Been Collected

An individual has the right to request that the business disclose to them:

1. the categories of personal information it has collected about that individual
2. the categories of sources from which the personal information is collected
3. the business or commercial purpose for collecting, selling or sharing personal information
4. the categories of third parties to whom the business discloses personal information and
5. the specific pieces of personal information it has collected about that individual.

Right to Opt-Out of Sale of Personal Information

Under the CPRA, the concept of "selling" is much broader than the word would intuitively imply. Selling "means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration."

While it's unlikely that many businesses will sell personal information about employees to third parties, such individuals have the right, at any time, to opt-out of the sale or sharing of such information. Such businesses must provide notice that information may be sold or shared, and individuals have the right to opt-out of the sale of their personal information. Such an opt-out must be adhered to, unless and until the individual subsequently consents to the sale of their personal information. Businesses cannot ask for such permission until at least 12 months after the initial opt-out.

Right to Limit Use and Disclosure of Sensitive Personal Information

Individuals also have the right to direct a business that collects sensitive personal information to limit the use of such information to

- "that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services"
- certain "business purposes" as defined under the CPRA and
- as authorized by forthcoming regulations.

Employees must be provided notice of this right. Note that the new California Privacy Protection Agency (CPPA), created by the CPRA and charged with enforcing the CPRA, is working on implementing regulations – but those regulations are still in draft form and not final.

Non-Retaliation

The CPRA specifically prohibits discrimination against an individual because the individual exercised any of their rights, including the right to opt-out, under the CPRA. Specifically, this prohibition includes retaliating against an employee, applicant or independent contractor for exercising their rights under the CPRA.

Notice, Disclosure, Correction and Deletion Requirements

Businesses must make available two or more designated methods for submitting requests for disclosure of personal information being collected, shared or sold and to whom, to delete personal information, or to correct inaccurate personal information, including at minimum through a toll-free telephone number. Businesses with an internet website must also make the website available for individuals to make these requests.

Once a request is received, a business must acknowledge receipt of the request within 10 business days and respond with the required information or action within 45 days free of charge to the individual. The required disclosure must be made in writing and delivered in accordance with CPRA requirements. The request can span a 12-month lookback period, or longer under the forthcoming regulations. In any event, such disclosures only need to be made for information collected on or after Jan. 1, 2022. Notably, businesses need not respond to an individual's request for personal information collected, or shared or sold and to whom, more than twice in a 12-month period.

Takeaways

Employers should take steps now to prepare for compliance with the CPRA. Measures to consider include data-mapping employee, applicant and independent contractor information and implementing policies and procedures to provide the requisite notices and respond to requests.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Gregg Brochin

Partner
212 468 4950
gbrochin@dglaw.com

Ryan Schneider

Associate
212 468 4817
rschneider@dglaw.com