PUBLICATION

Privacy Reset in 2023: Effective January 1: What Employers Need to Know About Additional Rights in the California Privacy Rights Act

Authors: Alisa L. Chestler, Vivien F. Peaden
January 03, 2023

For most companies, human resource departments handle one of their most valuable and sensitive information assets: the personal data of their employees and job candidates. While this dataset provides employers a goldmine of information and intelligence, state legislatures have remained largely silent on the data privacy aspects of these HR operations. Effective January 1, 2023, this will change with the California Privacy Rights Act (CPRA), which will provide California employees additional rights when it comes to how certain employers collect, disclose, use, share, and store their personal data. Previously, business-to-business and HR data were universally exempt in states that have passed comprehensive privacy laws, i.e., Virginia, Colorado, Utah, and Connecticut.

The CPRA heralds a new era of data protection for California residents, and extends protections to California employees, independent contractors, and job applicants (California Personnel). The CPRA imposes penalties up to $7,500 *per violation*. Some claims can turn into class actions, exposing a company to enormous potential liabilities. Therefore, employers with any personnel residing in California must review the law and consider their obligations and the following:

1. How does the CPRA apply if an employer has no or limited business operations in California?

For most companies, the CPRA applies when it generates more than $25 million in global revenue in the previous calendar year (Revenue Threshold). The CPRA also governs smaller entities that commercialize a substantial amount of California personal data by volume or revenue, when they buy, sell, or share 100,000 Californians' personal data, or derive 50 percent or more of their revenue from selling or sharing California personal data (Data Commercialization Threshold). Once a business meets either threshold, it must comply with the CPRA even if it engages only one Californian employee and even if they have no other physical presence in the state.

2. What notice should an employer provide to California personnel?

The CPRA gives California residents more transparency on how their employer handles their personal data. Employers should update privacy policies and provide a notice at the point of data collection with the following disclosure involving its California personnel, including:

(i) ***What*** types of data it has collected during the last 12 months (i.e., name, address, employment and professional history, and other sensitive personal information);

(ii) ***Why*** it collects the data (for business or other commercial purposes);

(iii) ***Where*** it collects the data (either directly from the individuals or indirectly through a third party);

(iv) ***To whom*** it transfers the data and whether it sells or shares the data;

(v) ***How long*** it stores and retains the data (or applicable criteria for retention period); and

(vi) ***How*** individuals can exercise their rights under the CPRA.

3. What rights do California personnel have under the CPRA?

Under the CPRA, California residents have the rights, under certain circumstances, to delete their personal data, correct any inaccurate personal data, suspend sales or sharing of personal data for commercial purposes, to restrict use and disclosure of sensitive personal information, and to not be retaliated against by an employer for making a request to exercise their CPRA rights. A company must respond to a CPRA consumer request within 45 calendar days following its receipt but may extend the response period by another 45 days.

Note that some CPRA consumer rights may conflict with an employer's legitimate HR operations, such as employee benefit enrollment, EEO-1 report filing, and HR files' retention to defend against legal claims, among other circumstances. Employers should consult their privacy counsel before responding to these requests within the required 45-day period.

4. What other contractual and operational measures should an employer implement?

Companies invest substantial resources in privacy operations, yet often overlook amending vendor contracts with CPRA-specific clauses. The onus is on every company to monitor vendors within the supply chain. For the HR team to contribute to CPRA compliance, they should:

- **Create a vendor list**: Companies rely on various technology and professional service providers to support HR operations, including payroll processing and time management providers, applicant tracking technology (ATS) providers, benefit enrollment partners, learning and development providers, external recruiters, and other vendors that access their personnel personal data.
- **Pay attention to HR-tech vendors with cutting edge features**: Some vendors deliver cutting-edge tools to accelerate HR operations through AI-assisted screening, text-messaging outreach, and automated personality assessment. Before deploying any AI-enabled or text-messaging solutions, employers should consult their employment and privacy counsel to assess the risks under both U.S. and foreign privacy laws.
- **Amend contracts to bridge any gaps**: The CPRA has specific requirements for setting appropriate data protection terms with service providers. Companies should set up processes to quickly amend these HR vendors' contracts to comply with the CPRA.
- **Refer HR vendors for security assessment**: Employers should allocate resources to enable information security teams to conduct security assessment, insurance coverage review, and other due diligence on existing vendors and potential vendors in the RFP processes.
- **Update privacy policies accordingly**: The obligation to maintain policies and procedures should not be overlooked or forgotten. Companies should determine what policies exist, what policies are needed and how to implement the procedures. These determinations are a team effort. Companies need to ensure all stakeholders are aware of the need to document and implement appropriate policies and procedures.

Bottom line

Investment in California privacy readiness should be a top priority. The CPRA's enforcement agency has announced that it is ready to take disciplinary action against companies that do not protect consumer data in compliance with the regulations. By adopting CPRA-compliant privacy practices, employers will not only mitigate risks but also build consumer trust as a competitive advantage in improving talent acquisition and retention. If you have questions or want to know more about how the CPRA affects your HR operations, please

contact Alisa Chestler, Vivien Peaden, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity team.