NOW & NEXT

Cybersecurity & Privacy Alert

DECEMBER 1, 2022

Prepare now — California Privacy Rights Act effective January 1, 2023

By Jenny L. Holmes and Jason C. Kravitz

Employers must have data collection and privacy protocols in place by the new year.

What's the Impact?

- If the CPRA applies to your organization, you should prepare by reviewing your existing policies and implement needed changes now

On January 1, 2023, the California Privacy Rights Act becomes effective, amending the California Consumer Privacy Act. Like the CCPA, the CPRA requires a privacy notice be given to employees and job applicants at the time of collection of their personal information. Importantly, however, the CPRA ends the moratorium on extending the CCPA's consumer privacy rights to employees. This means that employers need to have mechanisms in place to respond to data subject requests from employees, like the right to access or to correct personal information.

Here are some other key parts of the CPRA:

A compliance runway

- While the CPRA comes into effect January 1, 2023, actual government enforcement of the CPRA's provisions will not begin until July 1, 2023.

Additional consumer substantive rights

- The law imposes heightened protections for "sensitive personal information," which includes social security, driver's license, passport, and financial account numbers, and other highly private information. Consumers will have the right to limit businesses' ability to collect, use, and share this information.
- Consumers will have the right to request that businesses correct inaccurate information about the consumer.
- Consumers can limit a business's ability to collect and use geolocation data that has a level of precision within 1,850 feet.
- Businesses must inform consumers of their data retention policies, and are not allowed to keep data longer than is "reasonably necessary."
- Consumers have the ability to prohibit businesses from sharing data with others for the purposes of cross-context behavioral advertising.

Strengthened enforcement

- The CPRA creates a "California Privacy Protection Agency" tasked with enforcement and promulgation of regulations.
- The CCPA's 30-day "cure" period is eliminated for government enforcement actions, replaced with a provision allowing the government the discretion to abstain from enforcement actions depending on the circumstances.
- The penalties for mishandling children's information are tripled from $2,500 per incident to $7,500, dramatically increasing the consequences of violating the statute.
- The scope of potential data breach claims is increased by the CPRA's clarification that leaks of email accounts combined with a password or security question information can support a cause of action for statutory damages.

Audits and risk assessments

- While the CPRA itself does not impose a requirement that a business conduct data privacy audits and risk assessments, it does task the attorney general with issuing regulations that create such a requirement for businesses whose processing "presents a significant risk to consumers' privacy or security."

What hasn't changed? As an amendment to the CCPA, the CPRA leaves many of the current statutory provisions untouched. Generally speaking, the overall statutory scheme requiring that consumers are accurately notified of their rights pursuant to a privacy policy; that data collection, sharing, and usage is generally limited to that which is disclosed to the consumer; differing obligations for "businesses" and "service providers" (although the CPRA imposes some additional contractual requirements); and that businesses promptly respond to consumer requests, all remains essentially the same.

What employers need to do to prepare

- Assess the thresholds to see if the CPRA applies to your organization—the CPRA is triggered if your organization collects the personal information of any California consumers and in the past 12 months your organization:
  - has at least $25 million of annual gross revenue
  - buys, sells, shares, or receives personal data or the personal information of 100,000 or more California residents
  - receives over half of its revenue from the sale of personal data of California residents
- Identify the personal information your organization collects about its employees
- Develop an employee and job applicant privacy notice
- Review contracts with service providers that receive and/or process employee personal information
- Establish internal procedures to receive, analyze, and honor employee data requests

Our Cybersecurity & Privacy team can help you prepare for the changes the CPRA will bring.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Jason C. Kravitz
617.345.1318
jkravitz@nixonpeabody.com