BCLP. Client Intelligent

Insights

CALIFORNIA PASSES NEW CPRA PRIVACY REGULATION

Nov 06, 2020

On November 3, 2020, the state of California voted to pass Proposition 24, also known as The California Privacy Rights and Enforcement Act of 2020 ("CPRA"). As a result of this vote, businesses dealing with personal information related to California consumers will have to initiate efforts to shore up their privacy practices in order to comply with the CPRA. The bulk of the law will go into effect on January 1, 2023, with some provisions requiring a 12-month lookback period that would start January 1, 2022. Nevertheless, businesses will likely need to identify and begin addressing potential compliance gaps in the near term, including those businesses that have already been dealing with CCPA and/or GDPR compliance efforts.

Expansion of Employment Exemption

The CPRA will now extend the CCPA's exemption of employee data until January 1, 2023. Governor Gavin Newsom had already signed into law AB 1281 on September 29, 2020, which extended the employee information exemption to January 1, 2021, but this will now be superseded by the CPRA.

Under the CPRA's employee information exemption, the requirements of the CPRA do not apply to personal information that is collected by a business about a person in the context of an employment relationship (*e.g.* the person is a job applicant, employee, owner, director, officer, medical staff member, or independent contractor of that business) to the extent that the personal information is collected and used by the business with the context of said employment relationship, as emergency contact information of the person in the employment relationship, or for purposes of administering benefits. Importantly for businesses, employee information will not be subject to the various rights afforded to consumers under the CPRA until January 1, 2023.

It is worth noting that a business will still need to comply with certain aspects of the CPRA as it relates to employee information immediately. A business is still required to provide employees with a notice of privacy practices (*i.e.* a privacy policy) related to their personal information. In addition, a business will still be required to meet its obligations related to a security breach if an employee's information is subject to said breach.

Creation of Enforcement Agency

The CPRA will usher in the California Privacy Protection Agency (the "Protection Agency"), a five-member board to govern the administration and enforcement of the CPRA. It will assume rulemaking responsibilities on the earlier of July 1, 2021, or within six months of providing the Attorney General with notice that the Protection Agency is prepared to assume such responsibilities. Notably, both the rulemaking authority and enforcement under the CCPA are presently handled by the Attorney General's Office.

The primary responsibilities of the Protection Agency will be to investigate possible violations of the CPRA and to determine whether additional action is required against a business deemed to have violated the CPRA. If the Protection Agency determines there is probable cause for believing the CPRA has been violated, actions will be brought through Administrative Law Court (as opposed to state court, which is the current enforcement mechanism under CCPA), with potential administrative fines up to $2,500 for each violation, or up to $7,500 for each intentional violation or each violation involving the personal information of minor consumers. The Protection Agency will have the power to subpoena witnesses, compel testimony, and to take evidence as necessary to audit a business's compliance with the CPRA.

The Protection Agency will be independently funded, receiving at least $10 million in annual funding, beginning in 2021 with $5 million. The Protection Agency will appoint an executive director that will then be tasked with staffing the Agency.

Expanded Consumer Rights

In addition to the rights already afforded under CCPA, CPRA will grant California consumers the right to correct inaccurate personal information about them that is held by a business. It is worth noting that this particular right will not be available for consumers until the CPRA fully goes into effect on January 1, 2023. For a business that already has a process in place to receive and verify requests, this may be less difficult to operationalize.

Enhanced Fines for Violations of Children's Data

The CPRA will triple fines for instances in which a business violates the requirements under CPRA related to children's data, totaling a maximum of $7,500 per violation as opposed to $2,500 for other, non-intentional violations. In addition, a business must obtain opt-in consent prior to selling *or sharing* personal information of a child under 16.

Inclusion of "Sensitive Personal Information"

The CPRA adds a new definition for "sensitive personal information," which will be expansive and includes data elements such as government-issued identifiers (*e.g.* Social Security Number, driver's license number, or passport number), financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information about sex life or sexual orientation. The CPRA will also provide

consumers the right to limit a business' use of their sensitive personal information to that use "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services." Notably, a business that uses or shares sensitive personal information for purposes other than to perform services or provide goods will have to include a link on its homepage titled, "Limit the Use of My Sensitive Personal Information" that allows consumers to exercise their limitation rights. Businesses will not have to implement these features until January 1, 2023, although they will want to start understanding what types of sensitive personal information (if any) are being processed in preparation of these changes.

Expansion of Breach Liability

The CPRA provides for a private right of action where a business that suffers a data breach that results in the compromise of a consumer's email address in combination with a password or security question (and answer that security question) that would permit access to the account. Furthermore, unlike the CCPA, there will no longer be a 30-day cure period wherein a business has an opportunity to remedy the damages caused by a data breach. The expansion of the private right of action will mean it is even more important for a business to ensure it has appropriate indemnification language related to data breaches in agreements with third parties and/or service providers who are receiving personal information from the business. This expansion also goes into effect January 1, 2023.

Risk Assessments for "High-Risk Processing"

The newly created Protection Agency will also be issuing regulations, including a requirement that "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" will be required to perform annual cybersecurity audits as well as regular risk assessments with respect to their processing of personal information. The extent of this requirement will become clearer once the Protection Agency issues its regulations.

Storage Limitation and Data Minimization

The CPRA will now also restrict a business from retaining personal information for longer than reasonably necessary for the purpose for which it was collected. Further, businesses would be barred from collecting more personal information than necessary to accomplish the disclosed purpose. This will be a familiar restriction for businesses already in compliance with the GDPR's data minimization principle. For those businesses, procedures implemented for GDPR compliance measures will need to be extended to personal information of California consumers as well. For businesses that have not addressed the data minimization principle under GDPR, this may be a cumbersome requirement. The business will need to ensure it has a comprehensive data inventory, record retention policy, and will need to analyze and be able to justify how long it is retaining various data elements.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
