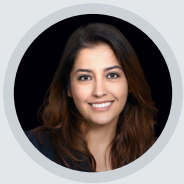
California Broadens Data Privacy Protections with the Passage of Privacy Rights Act

April 2021

LOCKTON®

AUTHOR



Maryam Rad
Vice President
Insurance & Claims Counsel
213.689.0504
mrad@lockton.com

On Nov. 3, 2020, California voters approved the California Privacy Rights Act ("CPRA"), which is another step forward in California's expansion of data protection. The CPRA expands privacy rights under the California Consumer Privacy Act ("CCPA"), which went into effect on Jan. 1, 2020. With the CPRA's detailed and extensive provisions, its passage appears to move California's data privacy protections closer to the ones afforded by the European Union's General Data Protection Regulation ("GDPR").

The CPRA becomes operative on Jan. 1, 2023, and will apply to personal information collected after Jan. 1, 2022. Civil and administrative enforcement will commence on July 1, 2023. The law is lengthy, expansive, nuanced and subject to further regulations, but some of its critical provisions are highlighted below.

Business impact highlights

Covered business

The CCPA applies to businesses that: (1) have $25 million in annual revenue; (2) annually buy, sell, receive or share for business commercial purposes, personal information of 50,000 California consumers, households, or devices; or (3) derive at least 50% of its annual revenue from selling California consumers' personal information.

The CPRA will apply to businesses that: (1) in the preceding calendar year had an annual gross revenue of $25 million; (2) annually buy, sell or share the personal information of 100,000 consumers or households; or (3) derive 50% or more of its annual revenue from selling or sharing consumers' personal information.

While the annual revenue of $25 million is the same under both the CCPA and CPRA, there are two notable differences regarding covered businesses. First, the annual buy, sell or share threshold under CCPA is currently 50,000 and includes devices, but under the CPRA that number has been increased to 100,000 and does not include devices, which may alleviate some of the burden on small businesses when the CPRA goes into effect. Second, the CPRA expands the CCPA by including businesses deriving at least 50% of their annual revenue from selling or sharing information, thereby potentially expanding the scope to include more businesses.

Service providers, contractors & third parties

In addition to covering "businesses," the CCPA also regulates "service providers" and "third parties." A "service provider" is an entity that processes consumer personal information on behalf of a business pursuant to a written contact. By contrast, "third party" is defined in the negative by the CCPA. A "third party" is not the business that collects consumer personal information nor is it a person to whom the business discloses a consumer's personal information pursuant to a written contract which is to contain very specific provisions regarding the handling of personal information.

The CPRA adds a new category of regulated entities — contractors. A "contractor" is "a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contact." The distinction between "service provider" and "contractor" is nuanced, but important because the new "contractor" category includes those person to whom the business makes available a consumer's personal information whereas "service provider" only included entities which process consumer personal information.

Under the CPRA, contracts with a third party, service provider, or contractor must have the following provisions: (1) specify that the personal information is sold or disclosed only for limited and specified purposes; (2) obligate the third party, service provider, or contractor to comply with applicable obligations under the CPRA and obligate those persons to provide the same level of privacy protection as required by the CPRA; (3) grant the business rights to take reasonable and appropriate steps to help to ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business's obligations under the CPRA; (4) require the third party, service provider or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA; and (5) grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

Data protection requirements

The CPRA expressly addresses the principles of purpose limitation, data minimization and storage limitation.

Specifically, the CPRA provides that the "collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." The CPRA provides that "a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose ... for longer than is reasonably necessary" but does not state a specific retention period.

Accordingly, organizations subject to the CPRA must: (1) have a specific and legitimate business purpose for collecting, using, retaining or sharing the personal information and the processing must not be inconsistent with the stated purpose, i.e., purpose limitation; (2) limit the personal data to information which is reasonably necessary for the stated business purpose, i.e., data minimization; and (3) store the data no longer than reasonably necessary, i.e., storage limitation.

30-day cure period

The CPRA eliminates the automatic 30-day cure period created by the CCPA for alleged noncompliance before being subject to potential State enforcement and makes granting a cure period discretionary. As to private actions, the cure period will remain; however, the new law makes clear that the "implementation and maintenance of reasonable security procedures and practices…following a breach does not constitute a cure with respect to that breach."

Digital advertising

The CPRA's broad definition of "share" means the disclosure of personal information for "cross-context behavioral advertising" that benefits the business, even if no money is exchanged. "Cross-context behavioral advertising" is defined as targeted advertising based on a consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications or services, other than those that the consumer intentionally interacts. Therefore, under the new law the sharing of personal information for "cross-context behavioral advertising" will be expressly regulated.

Children's Data

The CCPA imposes fines of $2,500 for a non-intentional violation, and $7,500 for an intentional violation. Under the new law, the $7,500 fine will apply to each intentional violation and each violation involving the personal information of a minor.

California Privacy Protection Agency ("CPPA")

The CPRA will establish the CPPA, which becomes the first privacy protection enforcement agency of its kind in the United States. It will serve as California's privacy enforcement regulator and replace the State Attorney General's rulemaking authority on the later of July 1, 2021, or six months after notifying the Attorney General that is ready to begin rulemaking. The CPPA will have an initial $5 million budget for fiscal year 2020-2021, with $10 million every fiscal year thereafter.

Audits & risk assessments

The CPRA requires the issuance of regulations regarding: (1) annual cybersecurity audits; and (2) risk assessments on a regular basis, for businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy or security. Under the CPRA, factors to determine when processing may result in significant risk include the size and complexity of the business and the nature and scope of the processing activities. Further, the CPPA will appoint a Chief Privacy Auditor to conduct audits to ensure compliance.

Consumer rights highlights

Sensitive personal information

The CPRA creates a new category of data called "sensitive personal information," which is defined as personal information that reveals a consumer's: (1) Social Security, driver's license, state identification card, passport number; (2) account login, financial account, debit card or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (3) precise geolocation; (4) race, ethnicity, religion, philosophical beliefs, union membership; (5) content of private communications, including mail, email and text messages, unless the business is the intended recipient of the communication; and (6) genetic data.

Sensitive personal information also includes: the processing of biometric information to uniquely identify a consumer; personal information collected and analyzed concerning a consumer's health; or personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Expansion of consumer rights

The CPRA expands upon the CCPA's consumer rights provisions in addition to creating new protections. Each of the consumer rights noted in the following chart have specific nuances within both the CCPA and CPRA, is meant to be illustrative of the general concepts. The CPRA provides that regulations will follow regarding consumer rights related to automated decision-making and profiling.[1]

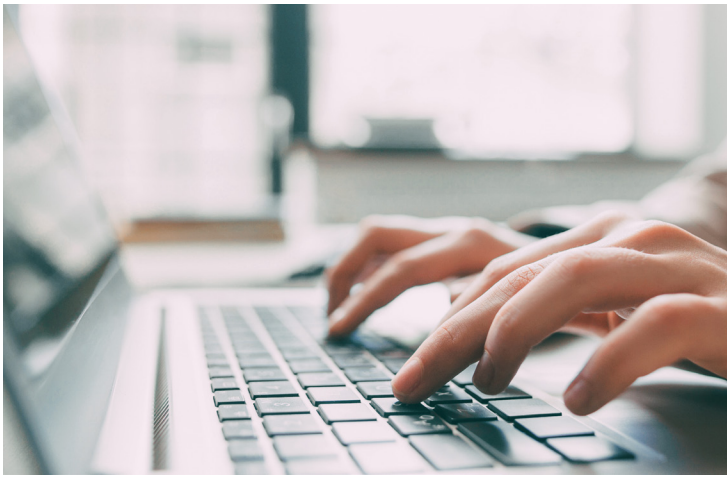
[1]Generally, automated decision-making involves using algorithms, computers and/or artificial intelligence to make decisions automatically, without human involvement. Profiling uses personal data about an individual in the decision-making process.

The following chart summarizes the key consumer rights created by or addressed in the CCPA and CPRA:

Consumer right	CCPA	CPRA
RIGHT TO DELETE — Consumers may request that their personal information be deleted	✓	✓ Businesses receiving deletion requests must notify third parties who have received the information to do the same, subject to some exceptions.
RIGHT TO CORRECT INACCURATE INFORMATION — Consumers may request that a business correct inaccurate personal information		✓
RIGHT TO KNOW WHAT INFORMATION IS BEING COLLECTED — Consumers have the right to know about the personal information that a business collects about them	✓	✓ For personal information collected after Jan. 1, 2022, consumers may request to know what personal information is collected beyond the previous 12 months as long as it is not "impossible" or require a "disproportionate" effort.
RIGHT TO ACCESS — Consumers have the right to access their personal information collected by a business	✓	✓
RIGHT TO KNOW IF PERSONAL INFORMATION IS SOLD — Consumers may request that a business disclose what personal information is being sold	✓	✓
RIGHT TO KNOW IF PERSONAL INFORMATION IS SHARED — Consumers may request that a business disclose what personal information is being shared		✓ The definition of "sharing" applies here to include the transfer or making available of a "consumer's personal information by the business to a third party for cross-context behavioral advertising whether or not for monetary or other valuable consideration."
OPT-OUT OF SALE OF PERSONAL INFORMATION — Consumers have the right to opt out of a business selling their personal information to others	✓	✓
OPT-OUT OF SHARING OF PERSONAL INFORMATION — Consumers have the right to opt out of a business sharing their personal information to others		✓ Based on the CPRA's "sharing" definition, consumer's opt-out rights have been expanded.
LIMIT USE AND DISCLOSURE OF SENSITIVE PERSONAL INFORMATION — Consumers may limit the use and disclosure of sensitive personal information		✓
RIGHT OF NON-DISCRIMINATION — Businesses cannot discriminate against consumers for exercising their data privacy rights	✓	✓

Private right of action

Under the CCPA, consumers can bring a private right of action whose nonencrypted and non-redacted personal information is subject to compromise because of "the business's violation of the duty to implement and maintain reasonable security procedures and practices." The CPRA expands the bases for data breach liability to also include compromises of a consumer's email address in combination with a password or security question that give access to personal information.



Compliance and best practices considerations

Organizations subject to California's laws, including those outside of state, need to ensure that they undertake a thorough and comprehensive evaluation of California's consumer privacy protection laws and implement a robust compliance strategy. Below are some considerations:

- Consult with legal counsel to determine whether your organization is subject to the CPRA's compliance obligations, i.e., whether the organization is considered a covered business under the law.
- Ensure that your compliance strategy includes consideration of all potentially applicable privacy protection laws, including international, federal, state and local regulations.
- Establish a team within your organization, including members from legal, IT, operations and finance to evaluate your data collection, use, and retention practices and create a course of action specific to your organization's needs and its compliance obligations. Some practices to consider may include:
  - Conducting a data mapping exercise inventorying all data created and collected, and track its entire information flow path and life cycle, both internally and externally;
  - Implementing a subject access request ("SAR") process to include verification processes for all individuals requesting a SAR; and
  - Applying a data classification policy to all sensitive and personally identifiable information and protecting that data appropriately.
- Evaluate contracts with entities that have access to data and are performing services for your organization, as well as contracts with customers to whom you are providing services.
- Plan for and establish a budget dedicated to compliance efforts, including allocations for implementing risk transfer mechanisms such as cyber insurance.

It is clear that California continues to be a leader in its consumer privacy protection efforts, and organizations must stay abreast of regulations that impact their consumers and operations.

UNCOMMONLY INDEPENDENT

KC: 79106