Published on *The National Law Review* https://natlawreview.com

California's Proposition 24 – CCPA 2.0 Meets the California GDPR

Article By:

Data Privacy & Cybersecurity Robinson Cole

Proposition 24 is known as the California Privacy Rights Act of 2020 (CPRA). It is on the ballot in California on November 3, and if it passes it will amend and expand certain provisions of the California Consumer Privacy Act (CCPA). Some say it's CCPA 2.0, however, there are some provisions that make the CPRA look more like the General Data Protection Regulation (GDPR) – the European data regulation that reshaped privacy rights in the European Union. Two provisions in particular are very GDPR-like; specifically, the creation of the California Privacy Protection Agency (CPPA), which will become the regulator charged with implementing and enforcing both the CCPA and CPRA, and the expanded definition of sensitive personal information. CPRA would become effective Jan. 1, 2023, with an enforcement date of July 1, 2023. Here are some key highlights of Proposition 24.

What's new for California consumers in CPRA? CPRA creates a new category of data, similar to GDPR, for sensitive personal information. CPRA also adds several new rights for consumers:

- to restrict the use of sensitive personal information;
- to correct inaccurate personal information;
- to prevent businesses from storing data longer than necessary;
- to limit businesses from collecting more data than necessary;
- to know what personal information is sold or shared and to whom, and to opt out of that sale or sharing of personal information;
- CPRA expands the non-discrimination provision to prevent retaliation against an employee, applicant for employment, or independent contractor for exercising their privacy rights.

What do businesses need to know regarding CPRA? It creates a new data protection agency with regulatory authority for enforcement of both CCPA and CPRA. Some new key provisions for businesses are:

- the CPRA creates a Chief Auditor, who will have the authority to audit businesses data practices;
- the CPRA also requires high risk data processors to perform regular cybersecurity audits and regular risk assessments;
- the CPRA adds provisions regarding profiling and automated decision making;
- the CPRA adds restrictions on transfer of personal information;
- the CPRA requires businesses that sell or share personal information to provide notice to consumers and a separate link to the “Do Not Sell or Share My Personal Information” webpage and a separate link to the “Limit the Use of My Sensitive Personal Information” webpage or a single link to both choices;
- the CPRA triples the fines set forth in CCPA for collecting and selling children’s private information and requires opt-in consent to sell personal information of consumers under the age of 16;
- the CPRA expands the consumer’s private right of action to include a breach of a consumer’s email address and password/security question and answer.

The CPRA also changes the definition of “business” to more clearly define the annual period of time to determine annual gross revenues, which specifies that a business must comply with CPRA if, “as of January 1 of the calendar year,” the business had annual gross revenues in excess of twenty-five million dollars “in the preceding calendar year,” or alone or in combination annually buys or sells or shares the personal information of 100,000 or more consumers or households, or derives 50 percent or more of its annual revenues from selling or sharing consumers’ personal information.

In addition to these criteria, CPRA adds somewhat puzzling language that states that a business would also be defined in the CPRA as a person that does business in California, that is not covered by one of the criteria described above, who may voluntarily certify to the California Privacy Protection Agency that it is in compliance with and agrees to be bound by CPRA.

The CPRA adds the new term “contractor” in addition to service provider. A contractor is a person to whom the business makes available a consumer’s personal information for a business purpose pursuant to a written contract with the business. The CPRA contains specific provisions to be included in the contract terms, and the contract must include a certification that the contractor understands the restrictions and will comply with them. The CPRA adds several new definitions, including definitions for cross-context behavioral advertising, dark pattern, non-personalized advertising, and profiling, and makes some changes to the definition of personal information. The CPRA eliminates some of the CCPA language regarding the “categories” of personal information.

The CPRA also adds “sensitive personal information” as a defined term which means:

(l) personal information that reveals: (A) a consumer’s social security, driver’s license, state identification card, or passport number; (B) a consumer’s account log-in, 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; (C) a consumer’s precise geolocation; (D) a consumer’s

racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2) (A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

The CPRA retains the CCPA exemptions for medical information governed by the California Confidentiality of Medical Information Act or protected health information collected by a covered entity or business associate under HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act), personal information collected as part of a clinical trial or other biomedical research study, activity involving the collection of personal information bearing on a consumer's credit worthiness, and personal information collected, processed, sold or disclosed subject to the Gramm-Leach-Bliley Act or the federal Driver's Privacy Protection Act of 1994.

The CCPA's limited exemptions for employment information and so-called business-to-business information are also continued in the CPRA, however these provisions shall expire on January 1, 2023.

The CPRA provides authority for the CPPA to create extensive regulations, including a requirement for regulation of businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to: (A) perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent; and (B) to submit to the CPPA on a regular basis a risk assessment with respect to the processing of personal information.

The private right of action under CPRA is expanded to include that consumers whose email address in combination with a password or security question and answer that would permit access to the account be able to institute a civil action and to recover damages or other injunctive relief. The CCPA 30-day cure period after notice of a breach is eliminated and administrative fines for violation of the CPRA increase to not more than $2,500 for each violation or $7,500 for each intentional violation or violations involving the personal information of consumers that the business has actual knowledge is under 16 years of age. The CPPA will have broad powers of investigation and enforcement for violations of the CPRA.

We will follow the progress of Proposition 24 on election day and provide an update here next week.

National Law Review, Volume X, Number 303