wiley

NEWSLETTER

California Votes 'Yes' on the California Privacy Rights and Enforcement Act of 2020

November 2020

Privacy in Focus®

On November 3, 2020, mere months after the California Consumer Protection Act (CCPA) took effect, California voters approved a ballot initiative that will significantly change that law and the privacy obligations for entities that do business in California that flow from it. The ballot initiative, known as California Privacy Rights and Enforcement Act of 2020 (CPRA), will in large part become operative on January 1, 2023, with enforcement beginning no earlier than July 1, 2023. Even though implementation of the CPRA's expanded obligations is two years away, businesses should become familiar with the new framework now, as it may require fundamental shifts in privacy practices. Importantly, the new law does not take away from a business's current obligation to comply with the CCPA.

The CPRA moves California privacy law closer to the European Union's landmark privacy regulation – the General Data Protection Regulation (GDPR). Specifically, the CPRA expands consumer rights, requires specific protections for sensitive personal information, imposes a requirement for data minimization and retention policies, establishes a data security obligation, and redefines the framework for sharing information with service providers, contractors, and third parties. The CPRA also creates a new privacy enforcement agency, changes the cure period for businesses that are not in compliance with the law, and expands the private right of action in the case of breaches.

Specifically, key changes in the CPRA include:

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

State Privacy Laws

Expanded Consumer Rights: The CPRA will expand the consumer rights of California residents to include the right to correct information a business has about a person. The law also expands an individual's right to opt out of having their information "shared" for "cross-context behavioral advertising." Under the current CCPA, there is no right to correction, and the right to opt out is limited to "selling" information.

Sensitive Personal Information: CPRA defines a new category of data – "Sensitive Personal Information" – and creates new obligations related to that data. Specifically, there are heightened notice requirements for businesses that collect "Sensitive Personal Information," and consumers will be allowed to limit the use or disclosure of this information in certain circumstances. Sensitive Personal Information is broadly defined to include: a consumer's Social Security, driver's license, state identification card, or passport number; 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; a consumer's precise geolocation; a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; the contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication; a consumer's genetic data; the processing of biometric information for the purpose of uniquely identifying 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.

Data Minimization/Data Retention: Similar to the GDPR, the CPRA expands the baseline obligations of a business to include requirements that the collection, use, retention, and sharing of personal information be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." A business will also have to create and publicly disclose a data retention policy. Businesses are prohibited from "retain[ing] a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose."

Data Security: CPRA also includes a data security obligation that requires a business to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure."

Service Providers/Contractors/Third Parties: In another nod to the GPDR, CPRA imposes several additional obligations on businesses that share personal information with service providers, contractors, and third parties. Among other things, it requires that a business contractually obligate service providers, contractors, and third parties to process personal information with the level of protection required by the CPRA.

New Privacy Agency: The CPRA would create a new state agency – the California Privacy Protection Agency (CPPA) – to implement and enforce the CPRA – removing enforcement obligations from the Attorney General.

Modifications to the Cure Period: The CPRA removes the 30-day cure period for enforcement actions brought by the AG, while granting the CPPA authority to provide a business a time period in which it may cure alleged violations – but not defining that specific period. The law retains the 30-day cure period for private claims related to data breaches, although the CPRA clarifies that "implementation and maintenance of reasonable security procedures and practices … following a breach" does not constitute a cure with respect to such breaches.

Expanded Private Right of Action: The CPRA expands the private right of action currently in the CCPA to apply to the unauthorized access or disclosure of an "email address in combination with a password or security question and answer that would permit access to an account" if the business failed to maintain reasonable security.

While the majority of the CPRA will not be operative until 2023, some provisions will become operative sooner. These nearer-term provisions include extension of the employee and B2B exemptions until 2023 and the requirement for the California AG to initiate new rulemakings to transfer regulatory authority to the CPPA. The deadline to adopt final regulations required by the CPRA is July 1, 2022.

It is critical for businesses subject to the new law to examine their current CCPA compliance efforts and begin preparing for the modifications and additions that will be needed to comply with the CPRA.

Now more than ever, it is crucial that businesses keep their fingers on the pulse of emerging privacy laws in the United States. Our team has helped entities of all sizes from various sectors parse through complicated CCPA issues – from determining whether the CCPA applies to developing compliance programs. If your organization has questions about the CPRA or the potential impact of this new law on your business, do not hesitate to reach out.