BARNES & THORNBURG LLP

ALERTS

California Voters Pass Proposition 24, The California Privacy Rights And Enforcement Act

November 10, 2020

Highlights

Ballot initiative resulted in California Privacy Rights and Enforcement Act of 2020 (CPRA), effective Jan. 1, 2023, with enforcement beginning July 1, 2023

CPRA will enhance protection of "sensitive personal information"

The new act will establish a new state agency, the California Privacy Protection Agency, to regulate and enforce these new privacy laws once they go into effect

On Nov. 3, 2020, California voters passed Proposition 24, paving the way for the California Privacy Rights and Enforcement Act of 2020 (CPRA) and its amendments to consumer privacy rights enacted under the California Consumer Privacy Act of 2018 (CCPA). The new law will impose additional restrictions and requirements on businesses.

Among the most notable changes, CPRA – set to take effect on Jan. 1, 2023 – will create a new privacy enforcement agency, provide new definitions and protection for sensitive consumer data, expand and clarify

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Scott N. Godes
Partner
Washington, D.C.

P 202-408-6928
F 202-289-1330
scott.godes@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy

limits on the use and sharing of this data, and expand liability for breaches of the security of this data.

More specifically, CPRA, a voter-initiated amendment to the 2018 act, provides even more restrictions on businesses sharing personal information and gives consumers greater control over their personal information. It also establishes and provides funding for a new California state agency to oversee implementation and enforcement of state privacy laws, taking over many CCPA regulatory duties from the state's Attorney General.

In light of the population of California, CPRA continues California's de facto role as a privacy regulator beyond its borders by adding to an increasingly complex regulatory compliance environment for businesses across the world, operating across any number of industries. It is a further indication such privacy regulations are only going to increase, whether at the state or federal level.

Businesses, many of which are still working toward full compliance with CCPA and the European Union's General Data Protection Regulation (GDPR), will now need to act before Jan. 1, 2023, to further update their privacy and data protection policies and procedures to ensure compliance with this new law, which applies to data collected beginning Jan. 1, 2022. The CCPA remains in effect until the CPRA takes over.

Certainly, best practices dictate understanding and responding to these new requirements well before the law's effective date.

CPRA Key Takeaways

- Effective date Jan. 1, 2023 – Enforcement starts July, 1, 2023
    - Applicable to personal information collected beginning Jan. 1, 2022
    - CCPA remains in effect
    - CCPA applicability to employees and business-to-business personal information is delayed until Jan. 1, 2023
- Businesses may not retain personal information for longer than reasonably necessary
- Law enforcement may stay deletion of data for an approved investigation
- Consumers have greater control over the sharing and correction of personal information
- A new category of "sensitive personal information" is created
- Establishment of a California agency to regulate and enforce privacy laws
- 30-day right-to-cure violations grace period is eliminated
- Exemptions include some vehicle information, student grades in

some instances, written memorials of some verbal contracts, and certain consumer credit information

- Some provisions are more stringent for minors

Affect and Application

The CPRA does not impact, extend, or nullify the effectiveness of the CCPA except as specifically indicated in the proposition.

CCPA, as amended by CPRA, applies to “businesses” that conduct business in California and participate in the collection or direction of consumer personal information and either 1) have gross revenues of more than $25 million (now measured in the prior calendar year), 2) buy, sell or share the personal information of 100,000 consumers (up from 50,000), or 3) derive more than 50 percent of annual revenue from selling (and now sharing) personal information.

Like CCPA, CPRA will not apply to nonprofit organizations.

Employee and B2B Personal Information

Notably, CPRA extends CCPA exemptions related to data from a business’ employee, independent contractor, and business-to-business (B2B) relationships until Jan. 1, 2023. Since 2018 there have been questions about whether CCPA intended to apply to employee and B2B information, the California legislature has thus far chosen to extend deadlines for application of CCPA to these data types.

Collection and Retention of Consumer Data

In contrast to the CCPA requirement for businesses to disclose the categories of information collected only upon consumer request, CPRA explicitly requires:

- Disclosure prior to collection of the categories of personal information collected;
- The purpose of collection;
- Whether the information is sold or shared; andHow long the information will be retained prior to collecting the information.

Further, collection, use, retention, and sharing of personal information must be “reasonably necessary and proportionate” to achieve the disclosed purpose and may not be used in a manner inconsistent with the disclosed purpose. Personal data may only be retained for as long as “reasonably necessary” to fulfill the purposes for which the data was collected.

Businesses are exempt from compliance with CCPA if compliance would violate federal, state or local laws or when acting consistently with civil, criminal or regulatory investigations or summonses, court orders, and subpoenas. CPRA adds an exemption from compliance when a person’s life is in jeopardy and allows law enforcement to delay the deletion of

personal information for an approved investigation.

Data Processing Agreements with Vendors

CPRA continues the CCPA requirement that businesses obligate their vendors and third party service providers with whom they sell data to comply with statutory privacy protections – and expands that requirement to all third parties with whom they share consumer personal information. Data Processing Agreements (DPAs) are incorporated as part of agreements and are used to direct third-party handling of consumer personal information. DPAs have become one of the most visible impacts of laws like CCPA and GDPR for U.S. businesses and should be included in any agreement where personal information is being shared or accessed.

Under CPRA, businesses must notify third parties when a consumer requests personal information to be deleted, corrected, or limited. It also empowers businesses to act to stop violations by third parties, but does not make businesses liable for the violations of third parties.

Greater Consumer Control

The stated goal of CPRA is to provide consumers with increased control over their data. It does this by adding “sharing” of personal information to the list of actions covered by CCPA; that clarifies CCPA’s fluctuating determination of whether or not a “sale” of data has occurred. CPRA also allows consumers to correct inaccurate personal information and creates a new category of data called “sensitive personal information,” similar to the “special categories” data concept under GDPR.

“Sensitive personal information” as defined, includes Social Security numbers; state and driver identification cards; account log-ins with passwords; financial account information with passwords; precise geolocation; race; religion; ethnicity; union membership; mail, email and text content not intended to be sent to the business; genetic data; biometric data used to identify a person; or a consumer’s sex life or sexual orientation.

In addition to the protections given to other personal information, consumers can limit the use of sensitive data to only “that use which is necessary to perform the services or provide the goods reasonably expected.” Businesses may not discriminate against or charge more to consumers who elect to limit the use of sensitive personal information. Note that the scope of use of sensitive personal information is more limited than that of personal information as it relates to offering consumers financial incentives to utilize their data.

CPRA has some other noteworthy changes to the definitions of personal information and sensitive personal information, adding “reasonably” as a qualifier for the idea of associating data to individuals. The new definitions include qualifying language for certain information that was “lawfully obtained” or “truthful information that is a matter of public concern.”

Under CCPA, consumers can request access to their data for the prior 12 months. CPRA will allow consumers to request access to their data

beyond 12 months if the business has retained such data and it is practical for the business to provide the data. This provision will only apply to data collected after Jan. 1, 2022. Businesses are given up to 90 days to comply with consumer requests, up from 45 days under CCPA.

The required data collection and use disclosures and the opportunity to opt out of sharing and selling personal information must still be prominently and conspicuously posted on the business' website homepage. CPRA continues an opt-out approach to data collection (except for minors under age 16). However, consumers must be given at least two ways to exercise their rights, generally via email and a phone number. Internet-only businesses are permitted to only allow consumers to make requests via email. Businesses must wait 12 months from the date of the opt-out to ask the consumer to opt back in.

Establishment of the California Privacy Protection Agency (CPPA)

The California Department of Justice and the state attorney general are responsible for enforcement of the current CCPA. The CPRA establishes a separate state agency to regulate state privacy laws called the California Privacy Protection Agency (CPPA).

The agency will have a five-member board appointed by various government officials with qualifications in privacy, technology, and consumer rights. The agency will have broad powers encompassing administrative, legislative, and adjudicative responsibilities.

Right-to-Cure

Under the current regulations, a business has 30 days after receiving notice of a CCPA violation to cure the violation. If the business fails to cure during that period, civil penalties of up to $2,500 per violation, or $7,500 per intentional violation (or violation relating to a child under 16), can be assessed. Under CPRA, this grace period will be eliminated and administrative fines can be recovered for privacy law violations. The amount of the fines per violation under CPRA remains $2,500 and $7,500, respectively. The right of consumers to recover up to $750 per consumer, per incident or actual damages for violations also remains unchanged.

What to Do Now

In preparation for CPRA to go into effect, businesses should consider these best practices as next steps:

1. Evaluate the amended California law and how it applies to your business and data protection program
2. Evaluate your data collection and sharing policies and make adjustments for tracking shared information and sensitive personal information
3. Review third-party agreements to ensure their compliance with the new law
4. Establish or update data subject access request procedures and data retention policies to minimize liability

5. Assess your cyber liability insurance coverage to address increased regulatory risk

For more information, please contact the Barnes & Thornburg lawyer with whom you work, or Brian McGinnis at brian.mcginnis@btlaw.com or 317-231-6437, Jason Bernstein at jason.bernstein@btlaw.com or 404-264-4040, Scott Godes at scott.godes@btlaw.com or 202-408-6928, Michael Baumert at michael.baumert@btlaw.com or 312-214-4570, or Sahara Williams at sahara.williams@btlaw.com or 317-231-6407.