



JUNE 19, 2020

PRIVACY DEVELOPMENTS IN CALIFORNIA

The State of California continues its longstanding tradition of implementing unprecedented changes to the data protection landscape within the United States. The California Consumer Privacy Act (“CCPA”) went into effect on January 1. In May, Californians for Consumer Privacy announced that it has secured sufficient signatures to ensure that the California Privacy Rights Act (“CPRA”) is included within the November 2020 ballot. This June, California Attorney General Becerra announced that the proposed final CCPA regulations have been submitted to California’s Office of Administrative Law for expedited review.

The CPRA Initiative:

Commonly referred to as CCPA 2.0, the CPRA is designed to expand privacy rights for Californian residents. It is expected that the CPRA will be included in the November 2020 ballot, and if passed would become effective on January 1, 2023. Notably, the CPRA will apply to businesses that maintain the personal information of 100,000 or more consumers or households.

In line with the European Union’s General Data Protection Regulation (“GDPR”), the CPRA seeks to:

- Establish a “sensitive personal information” category, which goes beyond the scope of the GDPR counterpart to include geolocation data, racial or ethnic origin, religion or philosophical beliefs, content of digital messages, sexual orientation, and health and biometric information. Consumers will obtain a right to limit the use of their sensitive personal information, including for any secondary purpose.
- Provide consumers with the right of correction for any personal information maintained by a business that is inaccurate.
- Permit businesses not to honor access requests if such information is used for security purposes or would expose trade secrets.
- Clarify the definition of “sale” of personal information in relation to permissible business purposes.
- Prohibit businesses from retaining personal information for longer than reasonably necessary for the disclosed purpose of collection, and require consumer notice about retention periods for each category of personal information collected.
- Establish a right to know, access, and receive personal information collected before a 12-month lookback period of data collected on or after January 1, 2022.
- Increase financial penalties for businesses engaging in the unauthorized collection, processing, and sale of personal information belonging to children under the age of 16.
- Include the breach of a consumer’s email address and either their password or a security question answer in the categories of personal information subject a private right of action under Section 1798.150(a).
- Place new obligations on services provided to include, assisting businesses comply with privacy obligations, requiring service providers to inform businesses when they use sub-processors, and requiring service providers to formalize any relations with sub-processor with a binding contract.
- Create a new privacy enforcement regulator called the California Privacy Protection Agency (“CPPA”). Revisions to the proposed CPRA text clarify how the CPPA will not be directly funded by regulatory fines.

While the initiative clarifies some key issues under the law, it is likely to be unwelcome by businesses as it potentially creates substantial new compliance costs and obligations.

Thankfully, the CPRA would extend the current employee and business-to-business moratoriums until the CPRA’s 2023 effective date. Our prior alert discussing the employee moratorium can be found [here](#).

Although a number of the proposed amendments would increase burdens on businesses, there are several amendments that would be beneficial by reducing ambiguity in the law and introducing more balanced compliance obligations. Despite this, the CPRA still leaves significant gaps in compliance details to be addressed through the rulemaking authority of the California Attorney General and the proposed California Privacy Protection Agency. As a result, CPRA will impact businesses' compliance with California privacy law, but the full extent of that impact will continue to evolve as this proposed ballot measure makes its way through the lawmaking process.

CCPA Final Regulations:

On June 1, 2020 the California Attorney General [submitted the CCPA final regulations](#) to the California Office of Administrative Law, which has 30 working days, plus an additional 60 calendar days, to review the final regulations for procedural compliance with the Administrative Procedure Act. It is reported that the Office of Administrative Law is experiencing a backlog and, consequently, they will likely consume the total amount of time allotted. The final regulations are materially the same as the draft regulations published in March 2020 and will be enforced from July 1, 2020 onward. Despite COVID-19-related concerns from various industries, the Attorney General has [indicated](#) that no delay in enforcement will be permitted.

The Attorney General rejected repeated requests to delay CCPA enforcement and the rollout of the finalized regulations, particularly from critics who insisted that businesses must focus on the COVID-19 pandemic and might face special burdens with much of their workforce working from home. The Attorney General explained that “[t]he proposed rules were released on October 11, 2019, with modifications made public on February 10, 2020 and March 11, 2020. Thus, businesses have been aware that these requirements could be imposed as part of the [Attorney General’s] regulations.” Despite this, the Attorney General also indicated that his office would exercise “prosecutorial discretion if warranted, depending on the particular facts at issue. Prosecutorial discretion permits [my office] to choose which entities to prosecute, whether to prosecute, and when to prosecute.” This suggests that the Attorney General will take a more flexible approach toward enforcement, even though there is no willingness to change the effective date. In response to the criticism that due to COVID-19 the time of these regulations is poor, the Attorney General argued that “any delays in implementation of the regulation will have a detrimental effect on consumer privacy as more and more Californians are using online resources to shop, work, and go to school.”

While the Attorney General may choose to be lenient in the prosecution of the law, this by no means should give businesses an excuse to pause their efforts in becoming CCPA compliant.

Kutak Rock’s [Privacy and Data Security Group](#) will continue to monitor the progress of the CPRA and all forthcoming CCPA enforcement action. Kutak Rock is strategically placed to help businesses across the nation engage with the legislative process at all stages.

| Contacts | | | |
|-----------------|------------------|----------------|--|
| Jon Breyer | Minneapolis | (612) 334-5057 | Jon.Breyer@KutakRock.com |
| Nicole Moriarty | Washington, D.C. | (202) 828-2446 | Nicole.Moriarty@KutakRock.com |
| Todd Kinney | Omaha | (402) 231-8968 | Todd.Kinney@KutakRock.com |
| Jacob Tewes | Omaha | (402) 661-8611 | Jacob.Tewes@KutakRock.com |

This Privacy and Data Security Client Alert is a publication of Kutak Rock LLP. This publication is intended to notify our clients and friends of current events and provide general information about privacy and data security issues. This Kutak Rock LLP Privacy and Data Security Client Alert is not intended, nor should it be used, as specific legal advice, and it does not create an attorney-client relationship.

©Kutak Rock LLP 2020 – All Rights Reserved

This communication could be considered advertising in some jurisdictions.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.