KFL KLUK FARBER LAW

hello@klukfarber.com
646.850.5009

California Privacy Rights Act: The New California Data Privacy Law You Need to Know About

December 2, 2020

Having already led the way in domestic data privacy regulation by passing the landmark California Consumer Privacy Act of 2018 (the "CCPA"), Californian citizens voted on November 3, 2020 to pass Proposition 24, the California Privacy Rights Act (the "CPRA"). The CPRA is additive to the CCPA, and is by far the most consumer-friendly privacy law passed to date in the United States, as it dramatically expands consumer protections, while imposing robust obligations on companies subject to the CPRA. In order to be in compliance with the CPRA before it goes into effect on January 1, 2023, companies will need to undertake significant changes to their existing privacy practices. In this Client Note, we summarize the key components of the CPRA and the changes companies should expect to make to comply with its terms.

The CPRA goes well beyond the CCPA in granting consumers rights over their personal information. The CPRA includes the following specific rights and obligations:

(i) Allows a consumer to prevent a company from *sharing* his or her personal information with third parties by opting out (as opposed to opting out of *selling* information under the CCPA);

(ii) Requires companies to provide a consumer the option to limit a company's use of his or her sensitive personal information (e.g., information relating to protected classes like ethnicity, religion, and sexual orientation or other sensitive information like social security information or genetic data) through a "Limit the Use of My Sensitive Personal Information" link on a website's homepage;

(iii) Grants a consumer the right to require companies to correct any inaccurate personal information upon request;

(iv) Requires that affirmative consent be given by a consumer who is younger than 16 years old or the parent or guardian of any consumer who is younger than 13 years old before a company collects any personal data from such consumers; and

(v) Requires data protection risk assessments for companies that present a significant risk to California residents' privacy or security.

The new law also substantially increases the penalties for privacy violations, by expanding the circumstances where the highest fine of $7,500 per violation is applicable and tripling penalties for violations involving minors under 16 years. To enforce these new penalties and California consumer data protection laws more generally, the CPRA requires the creation of a new state government agency that will act as an independent watchdog and educator, with a mission of vigorously enforcing the CPRA to ensure that businesses and consumers are well-informed about their rights and obligations.

hello@klukfarber.com
646.850.5009

While it can generally be characterized as very consumer-friendly, the CPRA does contain one unique feature that is more "company-friendly." Specifically, it authorizes companies to treat consumers differently based on whether a consumer does or does not allow the company to collect and/or sell their personal information. For example, a company can offer consumers financial incentives (e.g., payments to consumers or services at a different price, rate, level or quality) if the incentive reasonably relates to the value provided by the consumer's data. This provision of the law is vaguely drafted and leaves companies with no clear direction as to how to implement it. As a result, we expect that it will be the subject of much debate and may even be challenged in court.

While there may be amendments or further clarification on the CPRA before it goes into effect in January 2023, companies should take steps towards compliance well before that date and consider the following items:

Document / Process	Changes Necessary
Privacy Policy	Include (i) whether personal information is sold or shared based on the new definitions provided in the CPRA, (ii) disclosures for sensitive personal information, (iii) the new personal information correction right, and (iv) the retention period or retention criteria for each category of personal information collected.
External Process for Allowing Consumers to Opt-In or Opt-Out	Provide an affirmative opt-in option for consumers 16 years old and under and, separately, a "Limit the Use of My Sensitive Personal Information" opt-out link on the company's website homepage.
Internal Process for Handling Consumer Requests	Revise consumer request responses for opt-in and opt-out requests and create internal guidelines for service enhancements or downgrades.
Contracts with Service Providers or Other Third Parties	Consider including provisions that obligate the third party, service provider, or contractor to comply with the CPRA and grant the business rights to take reasonable and appropriate steps to ensure compliance with the CPRA, including the right to take reasonable and appropriate steps to stop and remediate the unauthorized use of personal information.

To the extent a company wants to differentiate the quality or cost of services provided to consumers who opt-out of the collection, sale or sharing of their personal, the company will need to establish fee schedules or policies for service downgrades for such consumers. In doing so, a company will need to ensure that the increased cost or downgraded service is "reasonably related" to the value to the company of the consumer's data. As noted above, we expect this area to be one of the most difficult to navigate

hello@klukfarber.com
646.850.5009

until guidance is issued or regulations are passed providing color around what "reasonably related" means.

We will continue to monitor CPRA developments, as there are likely to be additional guidance and regulations released prior to the legislation's effectiveness. For more information on the CPRA, please visit the Official Title and Summary prepared by the California Attorney General.

We encourage you to contact us at hello@klukfarber.com or (646) 850–5009 with any questions about the CPRA or to discuss other data privacy compliance considerations that you may have.