CARLTON FIELDS

California Privacy Rights Act Passes in California: What You Need to Know Now

November 05, 2020

California's Proposition 24, the California Privacy Rights Act, has passed with over 50% support of California voters. While votes continue to be tallied, it is highly likely that businesses will need to turn their attention immediately to the new obligations the CPRA puts into place.

The CPRA will have an effective date of January 1, 2023, and will, in large part, only apply to personal information collected after January 1, 2022. Those looking to the California State Legislature to amend the CPRA might want to think twice: the CPRA's language intentionally included text to limit the gutting of the law's key consumer protections.

The following highlights some key questions and considerations for businesses collecting, maintaining, and storing the personal information of California individuals and households.

Are there any immediate effective provisions?

- **A new sheriff is in town.** The CPRA creates the California Privacy Protection Agency (CPPA), a distinct privacy entity that will enforce California's consumer privacy laws. This agency has the power to levy fines, including increased fines for intentional violations or violations involving children's personal information (up to $7,500).

- **New rules on the horizon.** 2021 will likely kick off rulemaking for the new privacy regulator. The CPRA calls for the CPPA to begin a rulemaking process to address a variety of issues that have been left on the table with the California Consumer Privacy Act (CCPA). Businesses should expect changes to, as well as the creation of, new regulations that will guide compliance. If businesses thought changes were over with the latest round of modifications released to the CCPA regulations in October 2020, they need to keep their attention on the further changes to the California privacy compliance landscape to come.

Is the California Consumer Privacy Act (CCPA) a "lame duck" regulation?

Short answer: No.

The California Office of the Attorney General will continue to enforce the CCPA. Businesses who have thus far avoided or ignored CCPA obligations should immediately get in compliance for a few reasons:

1. It is the law in California and will be enforced.

2. The CCPA contains a private right of action—and plaintiff's lawyers are already actively filing suit.

3. The CPRA, if viewed in the context of augmenting a business's existing compliance framework or building a program from scratch, is a "CCPA+"—in some respects, it inches California closer to the European Union's General Data Protection Regulation (GDPR) and Brazil's LGPD. If your business has yet to undertake CCPA compliance, your business will not be in a position to shift effectively to adhere with the requirements of the CPRA.

How can a business get ahead of the curve?

While many provisions of the CPRA will not take effect until January 1, 2023, with an enforcement date of July 1, 2023, businesses would be prudent to start planning for the CPRA. Five reasons why (but, of course, there are more):

1. **The private right of action expands**. Individuals will have more latitude to bring suit. The "reasonable security" standard of the CCPA private right of action has been overlooked as many businesses have lasered in on the consumer privacy rights obligations of the CCPA. This puts businesses at risk should a data breach occur—and cyber security incidents are on the rise. The private right of action also would apply to individuals whose email address, along with a password or security question, is compromised if such information permits access to the account.

2. **Cure period for businesses canned to some extent**. Businesses who were looking to the 30-day cure period to quickly rectify their failure to comply with the CCPA have lost this perceived "safe harbor." The CPRA only provides for a cure period that will halt statutory damages if the violation is remedied, and only applies to a data breach and the private right of action.

3. **Challenges increase for behavioral advertising and digital marketing.** Individuals will be able to "opt out" from the sharing of their personal information related to "cross context behavioral advertising." Companies in the AdTech and related spaces, or those that use these marketing tools and technologies for revenue streams, need to start evaluating the impact to their business models now.

4. **New treatment for sensitive personal information.** "Sensitive personal information" must be treated as its own category for purposes of compliance. Practically, this means:

    - The use of "sensitive personal information" is restricted;

    - The data that qualifies as "sensitive personal information" includes:

    - Social Security numbers; driver's license information, passport information, financial account information; precise geolocation data; data related to race, ethnicity, and religion; union membership; personal communications (such as emails); genetic data; biometric data or health information; and information related to sex life or sexual orientation; and

    - Individuals get the right to "opt out" of the sale or sharing of this category of information.

5. **New consumer rights emerge.** The CPRA inches California closer to certain aspects of the EU's GDPR. These include:

    - *Right to correct*. Individuals can request to correct inaccurate personal information, and businesses must use commercially reasonable efforts to do so when they receive a verifiable consumer request.

- *Data minimization*. Businesses will be required to minimize the collection, use, retention, and sharing of an individual's personal information and apply a "necessity" and "proportionality" analysis with data, evaluating whether or not the data life cycle is reasonably necessary and proportionate to achieve the objectives for which the data was collected or processed.

While much is still to be determined in the wake of the CPRA, the time is now to create a holistic plan to address all California privacy requirements.

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology