CARLTON FIELDS

California Privacy Rights Act: Compliance Objectives for 2021

December 15, 2020

While California has been characterized by some of the nation's most long-standing and aggressive privacy laws, businesses operating in the state have faced uncertainty over the last three years as to what a final omnibus privacy regulation would look like. While the California Consumer Privacy Act (CCPA) passed in 2018, several modifications from the California state legislature, a lengthy rulemaking process undertaken by the Office of the Attorney General, and a looming proposition – Proposition 24, the California Privacy Rights Act (CPRA) – created an environment of reticence on the part of businesses to go "all in" on compliance.

Now, the CPRA has passed, and its heightened requirements, in conjunction with the CCPA, set forth a trajectory of steps that must be taken as businesses contemplate compliance for 2021. While the effective date of CPRA's requirements is January 1, 2023, the groundwork for compliance should begin in 2021.

A Few Compliance Objectives for 2021

Invest in data mapping now

Cursory data mapping will no longer be sufficient. The CPRA requires cybersecurity audits and risk assessments, which are the necessary predicate to compliance with the law's other requirements, such as updates to privacy notices. Notices will need to include:

- Whether the business sells or discloses the specific categories of personal information it collects;
- What "sensitive personal information" the business collects, processes, and discloses; and
- How long the business intends to retain each specific category of personal information and the criteria that the business will use to determine the retention period.

Check human and technical ability to honor consumer rights requests

If a business' approach to complying with the CCPA was to make only a cosmetic policy update to its publicfacing website, that will not pass muster with the CPRA. In addition to the existing rights given to consumers under the CCPA, the CPRA has added a new right and expanded others, as described below. In practice, this means that a business must have the workflows, scripts, procedures, and requisite employee training in place to accept and honor a verifiable consumer request, plus the technical means to effectuate the request should it be necessary.

- **Right to correct:** Consumers will now have the right to make requests to have a business correct inaccurate personal information.
- **Right to delete:** Contractors, service providers, and other third parties must cooperate with a business to delete information related to a consumer request. In addition to the business' internal processes and procedures, they will need to verify these third parties' ability to honor consumer requests from a customer support and technical perspective. Contracts with third parties will need to be revised and updated.

Review and revise your existing agreements

Existing agreements should be reviewed and revised in light of the totality of the CPRA's requirements. Given the CPRA's additional responsibility for third parties to effectuate consumer requests, and the explicit requirement under the CPRA to amend agreements to reflect its requirements, this is a necessary compliance measure.

Prioritize security. Under the CCPA, "reasonable security" could have solely been tied to the act's private right of action, but under the CPRA, businesses must identify and implement practices and procedures tied directly to the risk posed by collecting a specific category of personal information. This process includes conducting security audits of businesses.

With the dedication of a new, specific enforcement agency, the California Privacy Protection Agency, the CPRA has teeth and resources behind its enforcement. Playing a "wait and see" game for rulemaking will leave businesses too short a time period to ensure full compliance, and risk an audit of their compliance practices.

Related Practices

Life, Annuity, and Retirement Litigation
Securities Transactions and Compliance
Cybersecurity and Privacy

Related Industries

Life, Annuity, and Retirement Solutions
Securities & Investment Companies