BCLP. Client Intelligent

Insights

COLORADO PRIVACY ACT SIGNED INTO LAW

Jul 13, 2021

On July 7, 2021, Governor Jared Polis officially signed the Colorado Privacy Act ("CPA") into law, after the bill had passed both the Colorado House and Senate in June. The effective date of the CPA is July 1, 2023.

The CPA applies to organizations that conduct business in Colorado or produce commercial products or services that are intentionally targeted to Colorado residents and that either 1) control or process the personal data of more than 100,000 consumers per calendar year; or 2) derive revenue from the sale of personal data and control or process the personal data of 25,000 consumers.

Like similar laws, the CPA grants certain rights to consumers (subject to limited exceptions), which currently include:

- A Right to Opt-Out: The CPA allows Colorado consumers to opt-out of processing where the purpose is the sale of personal data, targeted advertising, or profiling in furtherance of *solely automated decisions* that have significant effects on the consumer. Notably, the CPA provides for a universal right of opt-out, meaning that consumers should be able to exercise their right of opt-out by clicking one button to opt-out of all activities subject to this right. As many organizations have learned in implementing the similar obligations of the CCPA and its implementing regulations, this requirement can be technically challenging in practice, particularly when trying to sync up opt-out rights for cookies and related technologies with other types of sharing.
- A Right to Correction: Colorado consumers can request that inaccuracies in their personal data be corrected, taking into account the nature of the personal data and purpose of the processing of the consumer's personal data.
- A Right to Deletion: Consumers have the right to request deletion of personal data about them.
- A Right to Consent to Processing of Sensitive Data: Controllers cannot process a consumer's sensitive data without first obtaining the consumer's consent. Sensitive data includes: 1) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; 2) genetic or

biometric data that may be processed for the purpose of uniquely identifying an individual; or 3) personal data from a known child (under 13 years of age).

Additional key features of the CPA include:

- Consumer is defined narrowly to include a Colorado resident acting only in an individual or household context. This means that data gathered from employees, job applications, B2B contacts and other individuals is out of scope for this law.
- The CPA defines "sale" as the "exchange of personal data for *monetary or other valuable consideration* by a controller to a third party." This definition confines the types of exchanges that could be considered sales to those exclusively for monetary or other valuable consideration.
- The CPA–like the VCDPA–excludes a private right of action for violations of the statute, a key distinction from the CCPA, which provides for a private right of action for certain data breaches.
- Like other consumer data privacy laws, the CPA imposes notice obligations on controllers of personal data and also requires that organizations prepare privacy risk assessments in certain circumstances that present a heightened risk of harm to the consumer.
- Prior to any enforcement action, the CPA provides that the Attorney General must issue a notice of violation to the controller if a cure is deemed possible. Organizations will have 60 days to cure the violation after receipt of the notice.

Now that the CPA has passed, organizations should begin preparing to address its requirements as part of their broader privacy compliance strategy. The good news for organizations seeking to understand how to adapt their privacy programs to yet another new law is that the provisions of this law are similar enough to that of the CCPA and the VCDPA that they should be able to build compliance with this new law into their ongoing efforts. The key will be to continue to build a privacy compliance program that allows for the inclusion of the requirements of new laws into the overall program rather than trying to build separate compliance models for each new state or law.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
