NOW + NEXT

DATA PRIVACY & CYBERSECURITY ALERT | NIXON PEABODY LLP

JUNE 11, 2021

Colorado General Assembly passed the Colorado Privacy Act

By Tracy Ickes

Colorado is set to become the third state to enact comprehensive privacy regulation. On June 8, the Colorado General Assembly passed the Colorado Privacy Act (the "CPA"). Once the CPA is transmitted to Governor Jared Polis, he will have ten days to sign or veto it. If signed, the effective date will be July 1, 2023.

Protections for consumers

Similar to California and Virginia's privacy laws, the bill creates personal data privacy rights. Consumers have the right to opt out of processing of personal data for targeted advertising, the sale of personal data, or "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer." Consumers also have the right to authorize another to opt out of processing such data, including through preferences in web browsers. Of particular interest though, is that the attorney general is authorized to establish technical specifications for a user-selected universal opt-out mechanism.

Consumers also have the right to access their personal data, correct inaccuracies in personal data, and delete personal data. Additionally, up to two times per year, a consumer may obtain personal data in a portable format that allows transfer to another entity.[1]

Affected entities

The CPA applies to controllers that conduct business in Colorado, or deliver commercial products or services intentionally targeted to Colorado residents, and:

- Control or process personal data of more than 100,000 consumers per year, regardless of whether they derive revenue from it; or
- Derive revenue from the sale of personal data and control or process the personal data of at least

[1] Note that these rights do not apply to pseudonymous data if the information necessary to identify the consumer is kept separately and is subject to both technical and organizational controls that prevent a controller from accessing the information. In addition, the CPA does not impose any obligation to maintain data in an identifiable form, or to re-identify data in order to respond to requests.

25,000 consumers.

Data controller obligations

The CPA also imposes a number of requirements on "controllers," defined broadly as a person, alone or jointly with others, that determines "the purposes for and means of processing personal data." Some of the obligations—such as responding to requests and providing privacy notices—are unremarkable. However, the CPA still warrants a careful look.

First, the act requires controllers to limit collection of personal data to what is "adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." The purpose for which data is processed must be stated in the privacy notices. Thus, controllers should pay close attention to how they identify the purpose for which data is processed, and ensure that it is consistent with their actual practices.

Second, the act requires controllers to take reasonable measures to secure data, taking into account the volume, scope, and nature of the data processed and the nature of the business. While the CPA itself does not create a private right of action (as discussed below), victims of data breaches may rely on this to allege negligence per se.

Third, the act requires controllers to conduct a "data protection assessment" of each processing activity that "presents a heightened risk of harm to a consumer," including selling personal data, processing sensitive data, or targeted advertising that presents a reasonably foreseeable risk of unfair or deceptive treatment, financial or physical injury, intrusion, or other "substantive injury." These data protection assessments must be made available to the attorney general upon request, and the attorney general may evaluate them for compliance with other laws. This may permit broad inquiries, particularly in light of the FTC's recent announcement that certain practices relating to artificial intelligence could violate the Fair Credit Reporting Act and the Equal Credit Opportunity Act.

Enforcement

Enforcement mechanisms under the CPA are limited. There is no private right of action, and only the attorney general and district attorneys have authority to enforce the act. The attorney general and district attorneys may seek injunctive relief, and violations of the act—after notice and an opportunity to cure—are deemed deceptive trade practices. However, no other form of relief or monetary penalty is specified.

Looking ahead

A patchwork of state-level privacy acts is emerging nationwide, with Colorado now joining California and Virginia, and each has unique features. Companies should be aware of the applicable laws, and their individual nuances, in each state in which they operate.

Nixon Peabody's Privacy & Cybersecurity Team will continue to monitor the changing landscape of state privacy laws.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Tracy Ickes at **tickes@nixonpeabody.com** or 415-984-8372
- Jason C. Kravitz at **jkravitz@nixonpeabody.com** or 617-345-1318