Colorado Privacy Act ("CPA")

On July 7, 2021, Colorado Governor Jared Polis signed S.B. 21-190, known as the Colorado Privacy Act ("CPA"), making Colorado the third U.S. state to enact comprehensive consumer data privacy legislation, following California and Virginia.

Taking effect on July 1, 2023, the CPA grants Colorado residents the right to access, correct, and delete their personal data, as well as opt-out of targeted advertising and the sale of their personal data.

The CPA applies to the personal data of "consumers," which are defined as "Colorado resident[s] acting only in an individual or household context; and does not include an individual acting in a commercial or employment context, [or] as a job applicant."

The CPA defines a "controller" as a person that, alone or jointly with others, determines the purposes and means of processing personal data, and a "processor" as a person that processes personal data on behalf of a controller.

The CPA applies to an entity that: (a) conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and (b) (i) during a calendar year, controls or processes the personal data of 100,000 or more Colorado residents, or (ii) derives revenue (or receives a discount on the price of goods or services) from the sale of personal data and processes or controls the personal data of 25,000 or more Colorado residents.

Unlike the data privacy laws of California and Virginia, Colorado's privacy law does not include a company revenue threshold, and thus, a business with few Colorado customers does not become subject to the CPA merely due to its annual revenue. Further, unlike its CA and VA counterparts, the CPA does not provide an exemption for non-profit entities.

The CPA contains several exemptions for entities or data that are subject to certain federal privacy laws and regulations. For example, the CPA exempts:

- consumer reporting agencies, furnishers, and users of consumer reports regulated and authorized by the FCRA;

- financial institutions and their affiliates, and data collected, processed, sold, or disclosed pursuant to the GLBA, as well as the DPPA;

- certain data that is subject to HIPAA, but does not exempt "covered entities" and "business associates" at the entity-level;

- certain processing involving federal substance abuse regulations, patient safety work product, and certain health research;

- data regulated by FERPA, and COPPA;

- air carriers and national securities associations; and

- there are also exemptions tied to certain provisions of state medical records laws, the state health benefit exchange, as well as certain exemptions for state institutes of higher education and state and local agencies when acting in compliance with the law and for noncommercial purposes.

The CPA grants consumers various rights, including:

- the right to opt-out of using their "personal data" for, "targeted advertising," "sale", and "profiling". Controllers are required to provide a clear and conspicuous method for consumers to opt-out. Beginning July 1, 2024, controllers will be required to accept opt-out requests through a universal optout mechanism that meets the technical specifications set out in the forthcoming regulations to be adopted by the Attorney General;

- the right of access, correction, deletion, and data portability regarding personal data that a controller maintains about them. A consumer has the right, no more than twice per calendar year, to obtain his or her personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity without hindrance, subject to certain exceptions; and

- right to appeal denial of a consumer request. Controllers are required to establish an internal process whereby consumers can appeal a controller's refusal to take action on a consumer request. The appeal process must be conspicuously available and as easy to use as the process for submitting a request.

The CPA imposes various obligations on controllers, including:

- a privacy notice. A controller must provide consumers with a privacy notice that includes certain information prescribed in the CPA, including: (i) the categories of personal data collected or processed; (ii) the purposes for which categories of personal data are processed; (iii) the categories of personal data the controller shares with third parties; (iv) the categories of third parties with whom the controller shares personal data; (v) whether the controller sells or processes personal data for targeted advertising; and (vi) how consumers may exercise their rights granted by the CPA;

- a duty of purpose specification and duty to avoid secondary use. A controller must specify the express purposes for which personal data is collected and processed, and may not process personal data for purposes that are not reasonably necessary to or compatible with the specified purpose(s) without first obtaining the consumer's consent;

- a duty of data minimization. A controller may only collect the personal data reasonably necessary in relation to the specified purposes for which the data is processed;

- a duty of care. A controller must take reasonable measures to secure personal data during storage and use. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business;

- a duty to avoid unlawful discrimination;

- a duty to not process "sensitive data" without first obtaining the consumer's consent;

- a duty to conduct and document data protection assessments prior to processing that "presents a heightened risk of harm" to a consumer; and

- a duty to enter into a data processing agreement with processors.

The CPA imposes various obligations on processors, including:

- adhere to the instructions of the controller;

- take appropriate technical and organizational measures to secure personal data, help the controller respond to consumer requests, and enable the controller to conduct data protection assessments;

- assist the controller in meeting its data security and data breach notification obligations under the CPA and Colorado's data breach notification law;

- only engage a subcontractor pursuant to a written contract and only after providing the controller with an opportunity to object; and

- enter into a processing agreement with the controller.

Regarding enforcement, the CPA does not provide a private right of action for consumers. The Colorado Attorney General and District Attorneys will have exclusive authority to

enforce the CPA. Prior to an enforcement action, a controller must be provided a notice of violation and a 60-day cure period if a cure is deemed possible. The maximum fine that can be imposed for a CPA violation is not specifically set forth in the CPA, but violations of the CPA are deemed a “deceptive trade practice” pursuant to the Colorado Consumer Protection Act, so the maximum penalty for a violation of the CPA will be $20,000 per violation (measured per consumer), and possibly as much as $50,000 in the event of a violation involving an elderly person.

Click the link above to view the details and full text of the CPA.