BRACEWELL

INSIGHTS

Colorado Privacy Act: New protections for consumers in the Centennial State

December 1, 2021

*By: **Lucy Porter** and **Matthew G. Nielsen***

On July 1, 2023, the Colorado Privacy Act (CPA) will go into effect as the third state law generally governing consumer data privacy and was the second enacted in 2021. If you do business with consumers in Colorado, regardless of your location, you should begin familiarizing yourself with the requirements of the CPA now. While the CPA is similar to the California Privacy Rights Act (CRPA) and Virginia's Consumer Data Privacy Act (VCDPA), certain elements distinguish the Colorado law from its counterparts. Unlike the California law, the CPA does not apply to personal data in the employee or business-to-business relationship. This client alert provides a breakdown of the general requirements and obligations on businesses and key distinctions with other state data privacy laws.

Covered Businesses and Applicability

Covered Controllers. The CPA applies to any business, called a "controller" under the statute, who "alone, or jointly with others, determines the purposes for and means of processing personal data," and "conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado" and:

- Controls or processes the personal data of 100,000 consumers or more during a calendar year; or
- 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 consumers or more.

There are a number of exemptions to the applicability provision that should be considered as part of the analysis of applicability. First, the definition of consumers does not include "individual[s] acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context." Second, the Act does not apply to certain types of personal data, as defined by the type of data, such as patient data, or as defined by the statute by which the collection and use of the data is regulated such as Gramm-Leach-Bliley. Third, the Act does not apply to certain types of businesses, such as air carriers, public utilities (as defined by Colorado Law), or those subject to Gramm-Leach-Bliley. Notably,

there is no revenue threshold requirement, meaning an applicability analysis begins by looking at the number of records processed.

Covered Individual. To reiterate, the CPA does not apply to employee data, which, like the VCDPA means a consumer is a Colorado resident acting only in an individual or household context.

Personal Data. The CPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual," but does not include "de-identified data or publicly available information," including data "that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public." This definition is similar to the VCDPA.

Controller and Processor Obligations

If the CPA is applicable to a controller then they, and their processors (a person that processes personal data on behalf of a controller) must adhere to a set of obligations. The CPA sets out an analysis for determining whether a person is acting as a controller or a processor.

Obligations and Duties of Controllers

Under the Act, controllers must:

- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;
- Comply with the duty of transparency by providing notice of the sale of personal data and the ability to opt out and by providing "a reasonably accessible, clear, and meaningful privacy notice" that includes:
    - Categories of personal data collected/processed;
    - Purpose(s) of processing;
    - How consumers may exercise rights and appeal controller's response to consumer's request;
    - Categories of personal data shared; and
    - Categories of third parties personal data is shared with;
- Respond to the consumer's exercise of their rights;
- Comply with the duty of purpose specification;
- Comply with the duty of data minimization;

- Comply with the duty to avoid secondary use;
- Comply with the duty of care that is appropriate to the volume, scope, and nature of the personal data processed.
- Comply with the duty to avoid unlawful discrimination;
- Process sensitive data only with the consent of the consumer. Sensitive data is "(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; (b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or (c) personal data from a known child;"
- Perform data protection assessments before beginning processing activities that present a heightened risk of harm to a consumer - certain situations of targeted advertising or profiling, selling personal data, and processing sensitive data are activities that present a heightened risk of harm; and
- Engage processors only under a written contract, which shall include the type of personal data processed and other requirements under the CPA.

Obligations of Processors

Under the Act, processors must:

- Assist controllers in meeting their obligations under the CPA;
- Adhere to instructions of controller and assist controller in meeting those obligations, including security of processing and data breach notification;
- Ensure a duty of confidentiality for each person processing personal data; and
- Engage subcontractors pursuant to a written contract and only after providing the controller an opportunity to object.

Rights of Consumers

Like the VCDPA and CPRA, the CPA includes a suite of rights which consumers may request with respect to their personal data:

- Right of access;
- Right to correction;
- Right to delete;

- Right to data portability;
- Right to opt out, including specifically of targeted advertising or the sale of personal data; and
- Right to appeal, including the right to contact the attorney general if the appeal is denied.

Within forty-five days of receipt of a request, a controller must respond by (a) taking action on the request, (b) extending the time for taking action up to an additional forty-five days, or (c) by not taking action and providing the instructions for an appeal. Information provided under a first request within a 12 month period must be at no charge to the consumer. Controller's may implement processes to authenticate the identity of consumers requesting rights.

Enforcement of the CPA

There is no private right of action under the CPA with enforcement authority delegated to both the Colorado attorney general and district attorneys. The CPA doubles the cure period granted to controllers provided under the VCDPA and CPRA to 60 days; however, the entitlement to a cure period will sunset on January 1, 2025. Under the CPA a violation is a deceptive trade practice under the Colorado Consumer Protection Act, such that while the CPA does not specify a penalty amount, the Colorado Consumer Protection Act specifies a penalty of up to $20,000 per violation.

What's Next

If the CPA is the first data protection legislation applicable to your organization, the time to transition your team– IT, marketing, legal – is now. Delays in implementation are likely and could be costly.

Bracewell is available to assist you with analyzing your obligations under the CPA, crafting or harmonizing privacy policies, reviewing contracts between you and your processors, and providing guidance on any other data protection legislation.

This alert is the second in a series reviewing the 2021 data privacy legislation landscape. You can find our first alert in this series ***here***. Stay tuned for our next piece breaking down the Virginia Consumer Data Privacy Act.