ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

JULY 29, 2021

Colorado Privacy Act Becomes Third Comprehensive State Privacy Act in the United States

by *Michael Young* and *Dorian Simmons*

The Colorado Privacy Act (CPA) became law when Governor Jared Polis signed the bill on July 7, 2021. The CPA is the third general state privacy law in the United States, following the Virginia Consumer Data Protection Act (CDPA) and the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). Although the CPA does not provide an express private right of action, businesses that violate the Act may face liability for deceptive acts (and a civil penalty of $20,000 per violation), enforced by the Colorado attorney general and/or Colorado state district attorneys.

Applicability

The CPA applies to certain controllers and their processors that control or process personal data. The Act defines "controllers," "processors," and "personal data" similarly to Virginia's CDPA: *controllers* are persons that determine the purposes and means of processing personal data either alone or jointly; *processors* are persons that process personal data on behalf of controllers; and *personal data* is information that is linked or reasonably linkable to an identified or identifiable individual excluding de-identified and publicly available data. "Person" is undefined within the CPA; however, the term likely includes legal entities. Unlike other comprehensive state privacy laws, the CPA appears to apply to nonprofit organizations.

Entities

The CPA applies to controllers that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and meet one of the following thresholds:

- Control or process the personal data of at least 100,000 consumers during a calendar year; or
- Derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of at least 25,000 consumers.

Exemptions

The CPA contains exemptions similar to other privacy laws. For instance, the Act does not apply to certain medical information, including personal data governed by the Health Insurance Portability and Accountability Act, and personal data subject to the Fair Credit Reporting Act, Children's Online Privacy Protection Act, and Gramm–Leach–Bliley Act (GLBA). In addition to a GLBA data-level exemption, the law includes an entity-level exemption for financial institutions and their affiliates that are subject to the GLBA and its implementing regulations. The CPA also exempts employee information and business-to-business data from substantial regulation. Data maintained for employment-record purposes is exempt. The law applies to protect "consumers," but the term "consumer" excludes individuals acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.

Enforcement and Liability

By its express terms, the CPA does not permit consumers to bring a private claim under the Act or any other law for a violation of the CPA.[1] The Act exclusively empowers the attorney general and district attorneys to bring claims against controllers and processors. Until January 1, 2025, the Act allows controllers 60 days to cure alleged violations. If the violations remain uncured or a violation occurs after the statutory cure period has expired, the attorney general or the district attorney may bring a claim of a deceptive trade practice under the Colorado Consumer Protection Act and seek a maximum civil penalty of $20,000 per violation.

The CPA prohibits controllers and processors from contracting to relieve liability based on the role played in the violation. Liability will be allocated based on the principle of comparative fault. A controller or a processor that discloses personal data in compliance with the CPA will not be found liable if the recipient processes personal data in violation of the Act if the disclosing party had no actual knowledge at the time of the disclosure that the recipient intended to violate the Act. Similarly, a controller or processor that receives personal data in compliance with the CPA will not be found liable if the disclosing party violates the Act.

Rulemaking Power

The CPA provides the attorney general the power to promulgate rules to carry out the Act. In addition to this general rulemaking power, by July 1, 2023, the attorney general is required to adopt rules that provide the technical specifications for one or more universal opt-out mechanisms that controllers are required to implement starting July 1, 2024. The attorney general also has until January 1, 2025 to "adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework" for complying with the CPA. The compliance framework could include a defense for businesses that adopt such a framework. The rules setting out this process "must become effective" by July 1, 2025.

De-identified Data

De-identified data is generally exempt from obligations under the CPA because de-identified data is not personal data if certain conditions are met. However, controllers maintaining de-identified data *are* required

---

[1] We do not predict how effective this provision will be and note that similar provisions in other laws (such as California's CCPA) have not prevented plaintiff's attorneys from bringing actions.

to exercise reasonable oversight over contractual commitments related to de-identified data and to take appropriate steps to address breaches of those commitments. Similar to Virginia's CDPA, controllers are also required to consider their use of de-identified data when conducting data protection assessments.

De-identified information means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data:

- Takes reasonable measures to ensure the data cannot be associated with an individual.
- Publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data.
- Contractually obligates any recipients of the information to comply with these requirements.

This approach to de-identified information is similar to the approach reflected in California's CPRA and Virginia's CDPA. All three privacy laws broadly align with the de-identification framework set forth in the FTC's 2012 Staff Report.

Pseudonymous Data

The CPA exempts "pseudonymous data" from certain data subject rights (the right of access and the rights to correction, deletion, and data portability). Pseudonymous data is personal data that cannot be attributed to a specific individual without additional information if such information is "kept separately" and is subject to technical and organizational measures to ensure that the data is not attributed to a specific individual. Similar to Virginia's CDPA, controllers that maintain pseudonymous data are not required to honor consumer rights requests (except requests to opt out) if the controllers can demonstrate that the information needed to identify the consumer exercising the right is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

Consumer Rights

The CPA provides consumers rights of access and the rights to data portability, correction, deletion, and opt-out. Controllers must support these rights.

- **Right of Access.** As with Virginia's CDPA, consumers have the right to confirm whether a controller is processing their personal data and to access such data.
- **Right to Data Portability.** Similar to the data portability right under Virginia's CDPA, Colorado consumers have the right to access their personal data in a portable and, to the extent technically feasible, readily usable format that allows them to transmit their data to another entity without hindrance, notwithstanding whether the personal data is processed by automatic means. Unlike the CDPA, the portability right under the CPA does not appear to be limited to personal data that consumers have previously provided to the controller. Further, consumers are limited to exercising this right two times per year under Colorado's law.

- **Right to Correction.** As with Virginia's CDPA and California's CPRA, consumers have the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes for processing the consumer's personal data.
- **Right to Deletion.** Consumers have the right to require deletion of their personal data. This right is not limited to data collected from the consumer.
- **Right to Opt Out.** Similar to Virginia's CDPA, the right to opt out applies to the processing of personal data for the purposes of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. However, there are several differences between Virginia's CDPA and opt-out rights under Colorado's law.
  - Colorado's CPA expressly allows consumers to opt out of the processing of personal data used to provide advertisements based on personal data "inferred" over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests.
  - The "sale" of personal data under the CPA includes the exchange of personal data for "other valuable consideration." However, under the CPA, sale does not include disclosures directed by the consumer.
  - "Profiling in furtherance of decisions that produce legal or similarly significant effects" is not expressly limited to profiling in furtherance of decisions *made by controllers*. This raises the question of whether consumers can opt out of processing that allows third parties to make certain profiling decisions. If so, then controllers may have an implicit responsibility to understand how their processing enables third-party profiling (and to take steps to limit such activity in response to an appropriate opt-out).

The CPA prohibits controllers from increasing the cost of, or decreasing the availability of, products or services based solely on the exercise of consumer rights. However, the CPA allows controllers to offer different price, rate, level, quality, or selection of goods or services if the offer is related to the consumer's voluntary participation in a loyalty rewards program.

Process for Exercising Consumer Rights

In their privacy notices, controllers must describe methods that consumers may use to exercise their personal data rights. Such methods must take into account the way consumers normally interact with the controller, the need for secure and reliable communications relating to the request, and the ability of the controller to authenticate the identity of the consumer making the request. As with California and Virginia privacy law, controllers are prohibited from requiring consumers to create a new account to exercise their rights, but controllers can require consumers to use an already-existing account.

If a consumer exercises a consumer right, controllers must respond within 45 days of receiving the request. A controller may extend the response period by 45 days when reasonably necessary, taking into account the complexity and number of requests. Controllers must honor authenticated consumer-rights requests by providing consumers the information requested free of charge except for the second or subsequent request within a 12-month period; in such cases, the controller may charge an amount according to Colorado's public record statute. If the controller decides not to honor the request, the controller must provide the consumer an explanation and instructions on how to appeal the decision. A controller is not required to

comply if the controller cannot authenticate the request using "commercially reasonable efforts," in which case the controller may request additional information reasonably necessary to authenticate the request.

Additional requirements relating to exercising the right to opt out

Before July 1, 2024, controllers *may* choose to implement a universal mechanism to facilitate opt-outs. Starting July 1, 2024, controllers *must* implement such an opt-out mechanism pursuant to rules promulgated by the attorney general, which are pending promulgation.

Appeal Process

If a controller denies a consumer-rights request, then the consumer must be offered an opportunity to appeal the controller's decision. The CPA allows controllers to set a reasonable period when consumers may exercise their right to appeal after receiving notice of the controller's decision not to act. The appeal process must be "conspicuously available and as easy to use as the process for submitting a request." After the controller has received an appeal request, the controller must inform the consumer of its decision to act or not act within 45 days of the receipt of the appeal request along with a written explanation of the reasons in support of the response. The period to respond can be extended by 60 additional days when "reasonably necessary, taking into account the complexity and number of requests serving as the basis for the appeal." The controller is also required to inform the consumer of their ability to contact the attorney general if the consumer has concerns about the results of the appeal.

Duties of Controllers and Processors

The CPA imposes certain obligations on controllers and processors. The CPA requires controllers and processors to enter into detailed contracts that provide processing instructions and specify the type of personal data to be processed and the duration of processing. The contract must also reflect the obligations of processors to:

- Impose a duty of confidentiality on persons processing the personal data.
- Engage subprocessors pursuant to a written agreement and allow controllers to object to subprocessors.
- Delete or return all personal data to the controller at the end of processing at the choice of the controller.
- Make available to the controller all information necessary to demonstrate compliance with the CPA.
- Allow for, and contribute to, the controller's reasonable audits and inspections.

The contract must also require both controllers and processors to implement appropriate technical and organizational security measures appropriate to the risk of processing personal data.

Other duties of controllers

The CPA requires controllers to limit the processing of personal data to processing that is necessary, reasonable, and proportionate to the specific purposes authorized by the CPA. Additionally, the CPA enumerates a number of independent statutory duties applicable to controllers:

- **"Duty of Transparency."** Controllers are required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice.

- **"Duty of Purpose Specification."** Controllers are required to specify the "express purposes" for which personal data is collected and processed.
- **"Duty of Data Minimization."** The controller's collection of personal data must be "adequate, relevant, and limited" to what is reasonably necessary for the specified purposes for which the personal data is processed.
- **"Duty to Avoid Secondary Use."** Controllers must obtain consent before processing personal data for purposes other than those that are reasonably necessary or compatible with the purposes specified by the controller.
- **"Duty of Care."** Controllers must take reasonable measures to secure personal data from unauthorized acquisition during storage and use. The security measures must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.
- **"Duty to Avoid Unlawful Discrimination."** Controllers are prohibited from processing personal data in violation of state and federal consumer antidiscrimination laws.
- **"Duty Regarding Sensitive Data."** Controllers are prohibited from processing sensitive data without obtaining consent. Sensitive data consists of (1) 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; (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. ("Child" means an individual under 13 years of age.) Before processing personal data concerning a known child, controllers are required to obtain consent from the child's parent or lawful guardian. Notably, the CPA does not define biometric data.

Other duties of processors

Processors are required to assist the controller by helping the controller fulfill its obligation to respond to consumer-rights requests and meet security requirements arising under the CPA and Colorado's data breach notification act. Processors must also provide to the controller information necessary to enable the controller to conduct and document any data protection assessments requirement under the CPA.

Data Protection Assessments

The CPA requires controllers to conduct a data protection assessment if the processing of personal data creates a heightened risk of harm to a consumer. This requirement only applies to personal data acquired on or after July 1, 2023. Processing that presents a heightened risk of harm to a consumer includes processing sensitive data, selling personal data, and processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- Financial or physical injury to consumers;
- A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers.

Controllers are required to make data protection assessments available to the Colorado attorney general upon request.

Effective Date

The effective date of the CPA is currently July 1, 2023. This date can change if a referendum petition is filed pursuant to the Colorado Constitution against the CPA within 90 days of the Colorado General Assembly adjourning; if this occurs, the challenged sections of the CPA will not take effect unless approved by voters in Colorado's November 2022 general election. The challenged section(s) would then take effect the later of July 1, 2023 or the date the vote is officially declared by the governor. The CPA does not contain terms expressly applying its provisions retroactively.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Maki DePalo
404.881.4280
maki.depalo@alston.com

James A. Harvey
404.881.7328
jim.harvey@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Wim Nauwelaerts
+32.2.550.3709
202.239.3709
wim.nauwelaerts@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

ALSTON & BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

WWW.ALSTON.COM