Updates
July 08, 2021
Colorado Becomes the Third US State to Enact Comprehensive Privacy Legislation

Colorado Governor Jared Polis signed the Colorado Privacy Act (CPA) into law on July 7, 2021, making it the third comprehensive state privacy law enacted in the United States. California led with the California Consumer Privacy Act (CCPA), which was recently amended by the California Privacy Rights Act of 2020, and the Virginia Consumer Data Protection Act (VCDPA) followed this March. Colorado adds to these laws by bringing privacy legislation to the middle of the country.

The CPA will go into effect on July 1, 2023, and apply to conduct occurring thereafter.[1] The CPA contains many provisions made familiar by other privacy laws such as providing consumers with rights to their data, requiring opt-outs for certain processing, and distinguishing between controllers and processors of data. We provide an overview and summary of the main aspects of the CPA below, with comparisons to some of the other existing privacy laws.

Scope and Applicability

Although a Colorado law, the CPA will have broad applicability in the United States.

The CPA Applies to Colorado Businesses and Businesses Outside of Colorado

The CPA applies to those who do business in Colorado as well as to those who operate outside of Colorado, if their products or services intentionally target Colorado residents. The criteria for extraterritorial application are similar to the targeting criteria in Article 3(2)(a) of the EU General Data Protection Regulation (GDPR).[2] Specifically, the CPA applies to a "controller" that:

- Conducts business in Colorado *or* produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and
- Satisfies one or both of the following thresholds:
    - 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.[3]

Similar to the GDPR and the VCDPA, a "controller" under the law is defined as a person who, alone or jointly with others, determines the purposes for and means of processing personal data.[4]

The CPA Protects Colorado "Consumers"

The CPA protects the personal data of "consumers," who are defined as Colorado residents acting only in an individual or household context. The law does not apply to personal data collected for employment purposes nor does it apply to B2B data. The CPA does not consider individuals acting in a commercial or employment context, as job applicants, or as beneficiaries of someone acting in an employment context, "consumers" under the law.[5]

Numerous Listed Exceptions

Numerous exceptions and carve-outs in the CPA allow certain listed entities, types of information, and activities to escape coverage, including protected health information governed by the Health Insurance Portability and

Accountability Act of 1996 (HIPAA), and other personal data that is subject to certain federal laws (among them the Children's Online Privacy Protection Act of 1998 (COPPA) and the Family Educational Rights and Privacy Act of 1974 (FERPA)).[6]

The CPA Creates Obligations for Processors

Like the VCDPA and GDPR, the CPA recognizes the role of processors and imposes separate requirements for handling personal information for those engaging with or acting as processors. A "processor" under the CPA is a natural or legal entity that processes personal data on behalf of a controller.[7] Similar to the CCPA's treatment of personal information shared with "service providers," as well as the treatment of personal data shared with processors under the VCDPA, disclosures to a processor under the CPA are not considered sales under the law.[8]

The CPA requires a controller and processor to enter into a contract that governs the processor's activities on behalf of the controller. The requirements for such contracts in the CPA are similar to those for processor agreements in Article 28 of the GDPR as well in the VCDPA.

Contracts must include the following:

- The processing instructions to which the processor is bound, including the nature and purpose of processing.
- The type of data subject to, and duration of, the processing.
- Persons engaged to process the data must be subject to confidentiality obligations.
- The controller must be given an opportunity to object to subcontractors and such subcontractors must be bound by the same obligations as the processor under a written contract.
- Security requirements for both parties.
- The processor must delete or return all personal data to the controller upon completion of services.
- The processor must submit to audits by the controller and provide information necessary to demonstrate compliance with the contract.[9]

Consumers Have Personal Data Rights

Following the framework for existing privacy legislation, the CPA gives consumers rights to access, correct, and delete personal data held by a controller, as well as the right to data portability and to opt out of certain processing. In relation to these rights, the CPA exempts pseudonymous data, and imposes additional requirements for a universal opt-out mechanism and valid consent.

Controllers Must Respond to Consumer Requests

The CPA gives consumers rights to:

- Opt out of the processing of their personal data for purposes of:
  - Targeted advertising;
  - The sale of personal data; or
  - Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.
- Access their personal data.
- Correct inaccuracies in their personal data.

- Delete their personal data.
- Obtain their personal data in a portable format.[10]

Controllers have 45 days to respond to an authenticated consumer request, which can be extended by 45 additional days where reasonably necessary.[11]

Not Applicable to Pseudonymous Data

Like the VCDPA, the CPA does not extend the rights of consumers to pseudonymous data, which is defined as data that can no longer be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to the specific individual.[12] A controller must be able to demonstrate that such measures are in place that prevent the controller from accessing the additional information.[13]

Universal Opt-Out Mechanism

When the CPA goes into effect, controllers will have the option of presenting consumers with a universal opt-out mechanism to exercise their right to opt out of targeted advertising or sales of their personal data. Beginning July 1, 2024, however, a universal opt-out mechanism will be required, and will need to conform to technical specifications to be issued by the attorney general.[14]

Consent Requirements

Consent plays an important role in the CPA. A controller must obtain a consumer's affirmative consent before using personal data for a purpose secondary to the purpose for which it was first collected, and before processing sensitive data.[15] Additionally, a controller may obtain consent from consumers for targeted advertising or sales of their data, and the consumer's consent would take precedence over any choice the consumer makes using a universal opt-out mechanism, provided that the consumer must be able to easily revoke their consent.[16]

For consent to be effective under the CPA, it must be a "clear, affirmative act" and signify the consumer's "freely given, specific, informed, and unambiguous agreement." The CPA specifically states that the following does not constitute consent:

- Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;
- Hovering over, muting, pausing, or closing a given piece of content; and
- Agreement obtained through "dark patterns", defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."[17]

Data Protection Assessments Required for High-Risk Processing

Similar to the assessments required by the VCDPA and GDPR, the CPA requires a controller to undertake data protection assessments before conducting processing that presents a heightened risk of harm to a consumer.[18] Processing that presents a heightened risk of harm to a consumer includes:

- Processing 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;

    - 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.
- Selling personal data.
- Processing sensitive data.[19]

Data protection assessments must be documented and made available to the attorney general upon request.[20]

Enforcement and Liability

There is no private right of action under the CPA.[21] The Colorado attorney general and district attorneys have exclusive authority to enforce the law.[22] Businesses have a 60-day period from the date it receives a notice of violation from the attorney general or a district attorney to cure the violation, however, this provision will be automatically repealed on January 1, 2025, after which the cure mechanism disappears.[23] A violation of the CPA is subject to civil penalties of up to $20,000 per violation imposed under Section 6-1-112 of the Colorado Revised Statutes.[24]

Prepare for the CPA

The Colorado Privacy Act adds to the litany of laws and regulations with which businesses must comply. While we wait for momentum to build to a federal data privacy law, companies are left to navigate the patchwork of state and industry sector laws to which they are subject. We encourage businesses to start preparing and analyzing the overlaps and differences in the CPRA, VCDPA, and CPA in advance of their effective dates. While we have provided some high-level comparisons here, there are nuances in the laws that require careful evaluation to determine if a compliance program covers all obligations. Businesses and individuals are advised to seek experienced counsel to help with their assessments.

Endnotes

[1] If a special referendum petition is filed within 90 days after the adjournment of the General Assembly, the CPA or any challenged provisions will be subject to approval at Colorado's general election in November 2022.

[2] Pursuant to Article 3(2)(a) of the GDPR, its provisions apply to a controller or processor not established in the EU conducting processing activities related to " the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union...."

[3] 6-1-1304(1).

[4] 6-1-1303(7).

[5] 6-1-1303(6).

[6] See the listed exemptions in 6-1-1304(2).

[7] 6-1-1303(19).

[8] 6-1-1303(23)(b)(I).

[9] 6-1-1305(5).

[10] 6-1-1306(1).

[11] 6-1-1306(2)(a)..

[12] 6-1-1303(22).

[13] 6-1-1307(3).

[14] 6-1-1306(1)(a)(IV)(A), (B).

[15] 6-1-1308(4), (7).

[16] 6-1-1306(1)(a)(IV)(C).

[17] 6-1-1303(5).

[18] 6-1-1309(1).

[19] 6-1-1309(2).

[20] 6-1-1309(4).

[21] 6-1-1310(1).

[22] 6-1-1311(1)(a).

[23] 6-1-1311(1)(d).

[24] The Colorado Privacy Act will be enacted as part 13 to Article 1 of title 6 in the Colorado Revised Statutes, which is the Colorado Consumer Protection Act. Violations of the CPA will be subject to the civil penalties for violations of Article 1, contained in C.R.S. 6-1-112.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Communications Retail & Consumer Products

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors