Articles + Publications | June 15, 2021

Colorado Passes Comprehensive Data Privacy Law

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Timothy A. Butler | Chelsea Lamb | Matthew J. Fay

On June 8, the Colorado legislature passed the Colorado Privacy Act (CPA). Assuming Governor Jared Polis signs the bill into law within 30 days, as is expected, Colorado will become the third state in the United States to enact a comprehensive data privacy law.

What's the key takeaway?

While there are differences, the CPA is much like the California Privacy Rights Act of 2020 (CPRA), which amended the California Consumer Privacy Act of 2018 (CCPA), and much like the recently enacted Virginia Consumer Data Protection Act (VCDPA). That's welcome news for privacy compliance professionals, as the CPA will require only relatively minor revisions to privacy programs that have already been tuned to the California and Virginia laws.

That said, the CPA signals again that the states are acting to fill the void left by an absence of a comprehensive federal privacy law. And while the comprehensive data privacy laws passed by California, Virginia, and Colorado are quite similar, the distinctions between the three laws will, to some degree, frustrate compliance efforts and leave consumers confused about their privacy rights — and industry frustration and consumer confusion will only grow as additional states pass comprehensive data privacy laws.

Below, we've provided a brief primer on the CPA.

What's the effective of the CPA?

If signed by the Governor, July 1, 2023.

Who must comply with the CPA?

The CPA applies primarily to "controllers" and "processors."

A controller is any "person that, alone or jointly with others, determines the purposes for and means of processing personal data." CPA § 6-1-1303(7). But a controller is subject to the CPA only if it: (1) conducts business in Colorado *or* intentionally markets its products or services to Colorado residents *and* (2a) controls or processes the personal data of 100,000 or more Colorado residents in a calendar year *or* (2b) controls or processes the personal data of 25,000 or more Colorado residents *and* derives revenue or cost savings from the sale of personal data. *See* CPA 6-1-1303(6), 6-1-1304(1).

A processor is any "person that processes personal data on behalf of a controller." *See* CPA § 6-1-1303(19).

What information is protected by the CPA?

The CPA protects both "personal data" and "sensitive data."

Personal data is "information that is linked or reasonably linkable to an identified or identifiable individual." CPA § 6-1-1303(17)(a). But personal data does not include a variety of different types of data, including (1) employment data; (2) de-identified or publicly available data; or (3) data that is directly governed by the Health Information Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act (DPPA), the Children's Online Privacy Protection Act (COPPA), or the Family Educational Rights and Privacy Act (FERPA). *See* CPA §§ 6-1-1303(17)(a), 6-1-1404(2).

Sensitive data is personal data that reveals "racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual relationship, or citizenship or citizenship status" *or* "genetic or biometric data that may be processor for the purpose of uniquely identifying an individual" *or* personal data from a "known child" – i.e., an individual under thirteen years of age. *See* CPA §§ 6-1-1303(4) & (24).

What rights are granted to consumers?

The CPA grants consumers a number of rights, including, among others: (1) the **right to opt out** of any processing for the purposes of targeted advertising, sales to third parties, or for profiling in relation to decisions that produce legal or similarly significant effects; (2) the **right to access** their personal data; (3) the **right to correct inaccuracies** in their personal data; (4) the **right to delete** their personal data; and (5) the **right to a portable copy** of their personal data. *See* CPA § 6-1-1306.

What obligations apply to controllers?

The CPA places a number of obligations on controllers, including, among others:

- ***Transparency.*** A controller must provide consumers with a "reasonably accessible, clear, and meaningful" privacy notice that, among other things, discloses the types of information the controller collects and why it collects them, the types of information the controller shares with third parties, the types of information the controller sells to third parties for targeted advertising, and how a consumer may exercise his or her right to opt out of the sale or processing of their data. *See* CPA § 6-1-1308(1) and (2).

- ***Data Minimization.*** A controller's collection of personal data must be "adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." *See* CPA § 6-1-1308(3).

- ***Duty to Avoid Secondary Use.*** A controller may not use personal data for purposes "that are not reasonably necessary or compatible with the specified purposes which the personal data are processed, unless the controller first obtains the consumer's consent." *See* CPA § 6-1-1308(4).

- ***Duty of Care.*** A controller must take “reasonable measures to secure personal data during both storage and use from unauthorized acquisition,” and those measures must “be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.” *See* CPA § 6-1-1308(5).

- ***Consent.*** A controller must not process sensitive data without first obtaining the consumer’s consent or, if the data concerns a child, the child’s parent’s consent. *See* CPA § 6-1-1308(7).

- ***Data Protection Assessments*****.** A controller must conduct a “data protection assessment” for processing that “presents a heightened risk of harm,” which includes any processing of sensitive data or processing for targeted advertising or profiling. *See* CPA § 6-1-1309(1).

What obligations apply to processors?

The CPA places a number of obligations on processors, including, among others:

- ***Data Processing Agreements*****.** A processor must be governed by a contract that sets out the controller’s processing instructions and certain specified obligations. *See* CPA § 6-1-1305(5).

- ***Data Subject Request.*** A processor must take “appropriate technical and organizational measures” to assist the controller in responding to consumer’s requests to exercise their rights. *See* CPA § 6-1-1305(2)(a).

- ***Duty of Care.*** A processor must help the controller meet its “obligations in relation to the security of processing” and “in relation to the notification of a breach of the security system.” *See* CPA § 6-1-1305(2)(b).

- ***Data Protection Assessments.*** A processor must provide the controller with information necessary to “enable the controller to conduct and document data protection assessments.” *See* CPA § 6-1-1305(2)(c).

- ***Confidentiality.*** A processor must “ensure that each person processing the personal data is subject to a duty of confidentiality.” *See* CPA § 6-1-1305(3)(a).

- ***Subcontractors.*** A processor must provide the controller with an opportunity to object to any subcontractor, and may only engage a subcontractor pursuant to a written agreement. *See* CPA § 6-1-1305(3)(b).

Who can enforce the CPA?

The CPA does not create private right of action. *See* CPA § 6-1-1310. It instead will be enforced by the Colorado Attorney General and Colorado’s district attorneys. *See* CPA § 6-1-1311.

Look for further articles on CPA compliance and building a privacy program that aligns with the CCPA, CPRA, and other privacy regimes.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Privacy + Cyber