wiley

NEWSLETTER

Colorado Legislature Passes Comprehensive Privacy Law: Five Things You Should Know About the Colorado Privacy Act

June 2021

Privacy In Focus®

On June 8, 2021, the Colorado Legislature passed the Colorado Privacy Act (CPA or "Act"), moving Colorado close to becoming the third state in the nation with its own omnibus privacy law, joining California and Virginia. If Gov. Jared Polis signs it into law, the Colorado Privacy Act will establish a comprehensive data privacy regime in the Centennial State that shares several similarities with the privacy laws in California and Virginia. Yet, despite these similarities, the CPA is still nuanced to such a degree that it will create a third, distinct data privacy framework with which companies that operate nationwide must contend.

Upon Gov. Polis's signature, the CPA will be set to go into effect on July 1, 2023 – six months later than the Virginia Consumer Data Protection Act (CDPA) and California Privacy Rights Act (CPRA) with effective dates on January 1, 2023. We will be looking more closely at the law in future articles, and how it compares to California and Virginia. Here, we outline five key points that companies should know now about the CPA:

1. The CPA Applies to Controllers That Conduct Business in Colorado and That Meet Certain Thresholds for Processing and/or Selling Personal Data

The CPA generally applies to data controllers – persons that determine the purposes for and means of processing personal data – that do business in Colorado, or produce or deliver commercial

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
State Privacy Laws

products or services that are targeted to Colorado residents, and that either:

1. Control or process the personal data of 100,000 or more Colorado resident consumers over a calendar year; or
2. 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 25,000 or more Colorado resident consumers.

However, the CPA's scope is subject to several exceptions. For instance, the CPA does not extend to protected health information that is collected, stored, and processed by a covered entity or its business associates under the Health Insurance Portability and Accountability Act's (HIPAA) implementing regulations. Similarly, the CPA does not cover personal data that has been collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), or that is regulated by the Children's Online Privacy Protection Act of 1998 (COPPA). Additionally, the CPA carves out of its scope "individual[s] acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."

2. The CPA Establishes Consumer Rights Similar to Virginia's

The CPA establishes five rights for Colorado consumers:

1. Right to opt out: Consumers have the right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or automated profiling in furtherance of decisions that produce legal or similarly significant effects.
2. Right of access: Consumers have the right to confirm whether a data controller is processing personal data concerning the consumer and to access that personal data.
3. Right to correction: Consumers have the right to correct inaccuracies in their personal data, taking into account the nature of the personal data and the purposes for which it is processed.
4. Right to deletion: Consumers have the right to delete personal data concerning the consumer.
5. Right to data portability: When exercising their right to access, consumers have the right to obtain their personal data in a portable and readily usable format that allows the consumer to easily transmit the data to another entity.

3. The CPA Imposes Obligations on Data Controllers Similar to Virginia's

Under the CPA, controllers of personal data are subject to the following duties:

1. Duty of transparency: The CPA's duty of transparency consists of three obligations. First, controllers must provide consumers with a privacy notice that contains certain elements. Second, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose that it is doing so and how a consumer may opt out. Third, controllers may neither require a consumer to create a new account in order to exercise a right, nor increase the cost, or decrease the availability, of their product or service based on a consumer's

exercise of one of their rights alone.

2. Duty of purpose specification: Controllers must specify the express purposes for which they are collecting and processing data.
3. Duty of data minimization: Controllers must limit their collection of personal data to what is reasonably necessary in relation to the specified purposes for processing that data.
4. Duty to avoid secondary use: Controllers may not process personal data for purposes that are not reasonably necessary to or compatible with their specified purposes without the consumer's prior consent.
5. Duty of care: Controllers must take reasonable measures to secure personal data.
6. Duty to avoid unlawful discrimination: Controllers may not commit any violations of state or federal anti-discrimination laws against consumers in processing their personal data.
7. Duty regarding sensitive data: Controllers must obtain a consumer's opt-in consent before processing that consumer's sensitive data. The CPA defines sensitive data to include personal data revealing information such as racial or ethnic origin, religious beliefs, mental or physical health condition, sex life or sexual orientation, or citizenship status; genetic or biometric data processed for identification purposes; or personal data from a child.

Additionally, a controller must also enter into a contract with a processor that sets out certain criteria for the personal data that will be processed, and how that data will be processed and retained, among other things.

Also similar to the Virginia framework, controllers under the CPA will need to conduct and document data protection assessments prior to engaging in processing activities that present a heightened risk of harm to a consumer. These activities include processing personal data for purposes of targeted advertising or for profiling that poses a reasonably foreseeable risk of harm to the consumer; selling personal data; and processing sensitive data, as defined above.

4. The CPA Imposes a Future Universal Opt-Out Requirement

On July 1, 2024 – one year after the CPA goes into effect – controllers must allow consumers to opt out of the processing of their personal data for targeted advertising or sale through a user-selected, universal opt-out mechanism. This opt-out mechanism must meet technical specifications to be established by the Attorney General.

5. The CPA Directs the Attorney General to Conduct a Rulemaking

Unlike the CDPA, the CPA grants the Attorney General the authority to promulgate rules for the purpose of carrying out the Act. As one component, the CPA directs the Attorney General to, by the CPA's effective date, adopt rules detailing the technical specifications for at least one universal opt-out mechanism, as explained above.

The CPA further provides that by January 1, 2025, the Attorney General *may* adopt rules governing the issuance of opinion letters and interpretive guidance. The purpose of these rules, which would have to go into effect by July 1, 2025, would be to develop an operational framework for business that includes a good faith reliance defense for an action that may otherwise constitute a violation of the CPA.

Looking Forward

Because the CPA does not go into effect until July 1, 2023, covered businesses will have some time to come into compliance with the Act's obligations. However, with two other distinct comprehensive data privacy frameworks to potentially wrestle with, businesses will benefit by beginning to map out their compliance strategies in the near term.

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Please reach out to any of the authors with questions.