

Colorado Privacy Act Passes With Nationwide Implications for Businesses

After California and Virginia, Colorado recently became the third state to pass a comprehensive consumer data privacy bill. Although this new Colorado Privacy Act (CPA) overlaps with the California and Virginia privacy laws, it differs from those laws in some respects. For example, it does not generally exempt nonprofit organizations from its scope, but generally exempts information in the employment and business-to-business context. This new Colorado law will become effective on July 1, 2023. Further, it permits the Colorado attorney general to develop regulations implementing the CPA and provides a process for issuing opinion letters and interpretive guidance.

Applicability

The CPA applies to legal entities that conduct business or produce commercial products or services that are intentionally targeted to Colorado residents AND either:

1. Control or process personal data of more than 100,000 consumers per calendar year; OR
2. Derive revenue (or receive a discount on the price of goods or services) from the sale of personal data and control or process the personal data of at least 25,000 consumers.

Exemptions

The CPA exempts certain entities and/or types of personal information. Some limited examples include the following:

- Data collected and processed within the employment and business-to-business context;
- Protected health information and de-identified information under the Health Insurance Portability and Accountability Act (HIPAA);
- Financial institutions and nonpublic personal information under the Gramm–Leach–Bliley Act (GLBA);
- Certain information regulated by the Fair Credit Reporting Act (FCRA), Children’s Online Privacy Protection Act (COPPA), or Family Educational Rights and Privacy Act (FERPA); and
- Information regulated by the Driver’s Privacy Protection Act of 1994.

Consumer Rights

The CPA defines a “controller” as a person or entity that “alone or jointly with others, determines the purposes for and means of processing personal data.” Controllers must provide Colorado consumers the following data subject rights:

- The right to opt-out of the processing of personal data, including processing for targeted advertising, profiling, and sale;
- The right of access to confirm whether a controller is processing personal data and the right to access the consumer’s data;
- The right to correct inaccuracies of personal data;
- The right to delete personal data;
- The right to obtain a portable copy of personal data; and
- An appeals process for refusal of any rights.

Controller and Processor Responsibilities

A “processor” is a person or entity (i.e., service provider or vendor) that processes personal data on behalf of a controller. Some notable requirements for controllers and processors under the CPA (in addition to those already noted for controllers above) include:

- Controllers must provide privacy notices that outline (i) the categories of personal data collected or processed by the controller or a processor; (ii) the purposes for which the categories of personal data are processed; (iii) how and where consumers may exercise their rights with respect to their data, including the controller’s contact information and how a consumer may appeal a controller’s action with regard to the consumer’s request; (iv) the categories of personal data that the controller shares with third parties, if any; and (v) the categories of third parties, if any with whom the controller shares personal data.
- Controllers must conduct a data protection assessment for processing activities involving personal data that present a heightened risk of harm.
- Processors must assist controllers with obligations under the CPA, including assisting with data subject requests by taking appropriate technical and organizational measures.
- Processors must provide controllers with an opportunity to object before engaging a subcontractor.
- Data processing by a processor must be conducted under a contract between the controller and processor that is binding on both parties. Specific provisions must be included, such as the type of personal data subject to the processing, the duration of the processing, and processing instructions to which the processor is bound.
- Controllers have a duty to avoid secondary use so that personal data is not processed for purposes that are not reasonably necessary or compatible with the specified purposes for which the personal data are processed.
- Controllers have a duty of data minimization so that the collection of personal data is adequate, relevant, and limited to what is reasonably necessary.
- “Dark patterns” (user interfaces designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice) are banned when obtaining consumer consent for certain processing of data.

Enforcement

The CPA can be enforced by district attorneys and the Colorado attorney general through injunctions or civil penalties. Civil penalties may be up to \$2,000 per violation and are not to exceed \$500,000 for any related series of violations. There is no private right of action for violations of the CPA, but violations constitute a deceptive trade practice for purposes of public enforcement. Notably, the CPA provides a 60-day cure period for controllers to rectify non-compliance before the attorney general or district attorney may take enforcement action. This cure period will be phased out after January 1, 2025, at which time the Colorado attorney general may act without such notice.

What’s Next?

As the new California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (CDPA), and Colorado Privacy Act (CPA) go into effect January 1, 2023, organizations should start preparing for compliance with these laws during the remainder of 2021 and in 2022. Many of the efforts required to comply with the CPRA and CDPA will assist with CPA compliance. However, organizations should take care to implement measures that adequately address the unique aspects of each law.

CPA requirements will be further developed and clarified as the Colorado attorney general implements regulations and provides regulatory guidance. Additionally, as Colorado gathers public feedback regarding the CPA, the Colorado General Assembly may enact legislation to fine-tune the CPA in the relatively near future. Because multiple states have enacted consumer privacy laws, and more will likely soon follow, businesses obligated to comply with multiple state laws should consider adopting policies and procedures that apply to consumers in multiple states, following the most restrictive applicable state requirements.

Chambliss will continue monitoring these and other developments in the information privacy area. Should you have any questions regarding the CPA or preparations for compliance, please contact [Cal Marshall](#) or your relationship attorney for more information.