July 9, 2021

Colorado Privacy Law Signed Into Law

On July 8, 2021, Colorado Governor Jared Polis signed the Colorado Privacy Act (the "Colorado Law"), a comprehensive privacy law that will take effect on July 1, 2023, into law. Colorado is the third U.S. state to pass a comprehensive privacy law, following California (the CCPA, as modified by the CPRA) and Virginia (the CDPA).

The Colorado Law generally resembles both the California and Virginia privacy laws, but more closely tracks the Virginia CDPA in terms of structure, approach, and language. The Colorado Law also contains some notable deviations from either law, including novel provisions regarding a mandatory universal opt-out mechanism for targeted advertising or sales of personal data.

Scope and Applicability

Following the lead of Virginia's CDPA, the Colorado Law applies more narrowly than the CCPA/CPRA by omitting any threshold for applicability based solely on revenue. In order to be subject to the Colorado Law, companies must

- Conduct business in Colorado or produce products or services intentionally targeted to Colorado residents, and
- Either
    1. annually control or process personal data of at least 100,000 Colorado residents or
    2. derive revenue or receive a discount on the price of goods or services from the sale of personal data and processes, or control the personal data of 25,000 or more residents.

Similarly, the Colorado Law tracks the Virginia law in defining "consumer" more narrowly than California. Colorado excludes individuals acting in a "commercial or employment context."

Of particular relevance for online advertising, Colorado's law defines "personal data" as information that is "linked or reasonably linkable to an identified or identifiable individual" – which avoids California's controversial formulation that covers data that is linked or linkable to a "household." Unlike Virginia's CDPA, however, the Colorado Law specifically defines "identified or identifiable individual" to include an individual who can be readily identified "directly or indirectly… by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier."

Exemptions

The Colorado Law contains several exemptions, including for specified governmental agencies and institutions of higher education, activities regulated by the Fair Credit Reporting Act, and data subject to the Children's Online Privacy Protection Act.

Most notably for financial institutions, the Colorado Law, like Virginia's, contains an exemption relating to the Gramm-Leach-Bliley Act that covers not only data governed by the Act but also financial institutions subject to and in compliance with the Act.

Of concern for health care institutions, the Colorado law, unlike Virginia's law, does not contain a similar "entity-level" exemption for covered entities and business associates subject to HIPAA. It does, however, contain exemptions relating to protected health information and medical information as well as other information processed in certain research contexts.

Controller and Processor Obligations

The Colorado Law follows the EU's GDPR and Virginia's law in using the technical terms "controller" and "processor" (rather than "business" and "service provider") to describe entities that determine the purposes and means of processing and those that process data on behalf of controllers. As is the standard international practice, Colorado's law requires controllers and processors to enter into contracts reflecting specified requirements, such as the nature, scope and purpose of the processing; deletion or return of personal data upon termination or expiration; and cooperation with audits.

Requirements for controllers include the provision of notice to data subjects, the implementation of appropriate safeguards for personal data, responding to individual rights requests, and conducting data protection assessments with respect to certain processing activities. The Colorado Law also contains various duties for controllers reflecting data processing principles, such as the duty to be transparent, to specify the purposes for processing, and to minimize the processing of personal data.

Processors are required to comply with the controller's instructions and to assist the controller in meeting various obligations under the Colorado Law. Processors must also enter into appropriate written contracts with any sub-processors, and unlike either the California or Virginia approach, they must not only notify but also offer the controller an opportunity to object to the use of any sub-processor.

Consumer Rights

The Colorado Law outlines several consumer rights, including for access, deletion, correction, and portability, as well as an opt-out right for the sale of personal data and relating to targeted advertising. Similar to both California and Virginia, the law outlines a process and timeline for handling consumer requests. Following Virginia's lead, the Colorado Law also requires the establishment of an appeals process that is triggered when a controller refuses to take action on a consumer request.

Sensitive Data

The Colorado Law introduces a requirement to obtain consumer consent for any processing of sensitive data, defined to include:

- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;
- Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; and
- Personal data from a known child.

This definition is narrower than both Virginia's CDPA (which in addition to the above includes precise geolocation information) and California's CCPA as amended by the CPRA (which includes several other data elements, but does not require an opt-in).

Consent and Dark Pattern Restrictions

Following the EU's GDPR and Virginia's CDPA, the Colorado Law defines consent as (in summary) a "clear, affirmative act signifying consumer's freely given, specific, informed, and unambiguous agreement."

Notably, the Colorado Law enters new territory by specifically vitiating consent obtained through "dark patterns," meaning interfaces "designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."

Data Protection Assessment

Similar to the EU and Virginia, the Colorado Law will require controllers to conduct data protection assessments when the processing of personal data presents a heightened risk, including with respect to any targeted advertising, sale of personal data, certain types of profiling, or processing of sensitive data.

These assessments must be made available to the Colorado Attorney General upon request, but are exempt from public inspection under the Colorado open records law, and their disclosure expressly does not constitute a waiver of any attorney-client privilege or work-product protection – an innovation that Virginia pioneered in the hopes of shaping a more cooperative relationship with industry.

Universal Opt-Out Mechanism

In a novel requirement, the Colorado Law requires the Attorney General to adopt (by July 1, 2023) rules with technical specifications for "one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data."

Unlike a similar concept contemplated by the CPRA and subject to future rulemaking, the Colorado Law will ***require*** controllers to honor opt-out requests made through such a mechanism. The Colorado Law makes clear that the mechanism may not "unfairly disadvantage another controller" nor be a "default setting" but should rather "clearly represent[] the consumer's affirmative, freely given, and unambiguous choice to opt out."

No Private Right of Action; Enforcement

The Colorado Law expressly does not contain or create a private right of action. Both the Colorado Attorney General and district attorneys are authorized to enforce the law.

Until January 1, 2025, prior to any enforcement action, controllers must be given a sixty-day opportunity to cure a violation (if cure is deemed possible).

* * *

The Colorado Law is evidence of the growing momentum among states to pass comprehensive privacy laws, reflecting a European approach to privacy, as filtered into U.S. law via Virginia. It is the third such law to be enacted, and many other states are currently considering proposals for similar laws along both the Virginia and California adaptations of the approach pioneered in Europe, but which is rapidly becoming a global standard.

We are watching this area closely and will continue to provide updates as there are further developments, including on our RopesDataPhiles.com blog.