Davis Polk

Colorado passes comprehensive privacy law

June 24, 2021 | Client Update | 6-minute read

On June 8, Colorado's legislature passed the Colorado Privacy Act (ColoPA), which will impose new, substantial privacy requirements on many businesses operating in Colorado. Colorado Governor Jared Polis is expected to sign ColoPA into law by July 7. Although ColoPA will not take effect until July 1, 2023, businesses should not delay in considering its potential impact on their operations.

Colorado is the third U.S. state to pass a comprehensive privacy law, following California and Virginia. ColoPA shares many attributes with the California Privacy Rights Act (CPRA), which will amend the California Consumer Privacy Act (CCPA) effective, in most material respects, on January 1, 2023, and the Virginia Consumer Data Protection Act (VCDPA), which takes effect the same day. Despite a number of similarities, ColoPA also includes certain unique provisions discussed below, which businesses will need to consider and which may influence legislation in development in other states.

ColoPA applies to controllers—businesses that determine the purposes and means of processing personal data—who conduct business in Colorado and either (i) process personal data of more than 100,000 consumers per year or (ii) earn revenue from the personal data of over 25,000 consumers per year. "Consumers" include Colorado residents acting only in an individual, rather than commercial or employment, capacity. ColoPA also imposes a limited number of obligations on "processors," who store and process data on behalf of a controller.

ColoPA's distinction between controllers and processors mirrors the VCDPA, but other defined terms differ between the two laws. For example, ColoPA includes an expansive definition of "process," which encompasses sale, storage, and other uses of personal data. ColoPA also defines "affiliates" to include companies that share 25% common ownership, which is lower than the 50% threshold imposed by the CPRA and VCDPA.

ColoPA does not apply to financial institutions that are subject to the Gramm-Leach-Bliley Act or to personal data collected in compliance with it. It similarly does not apply to air carriers or to certain data regulated by federal statutes, including the Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), Driver's Privacy Protection Act, Children's Online Privacy Protection Act (COPPA), and Family Educational Rights and Privacy Act (FERPA).

Highlights of ColoPA

- **Broad enforcement authority:** Although ColoPA does not create a private right of action, it grants enforcement authority to both the Colorado attorney general and district attorneys, who may bring actions with civil penalties up to $20,000 per violation. By contrast, the VCDPA solely vests enforcement in the attorney general. ColoPA affords businesses a 60-day cure period following notice of an enforcement action, however, this provision will sunset on January 1, 2025. Penalties may be assessed on a per-transaction and per-consumer basis and there is no cap on damages.
- **Required disclosures and consumer rights**: Like the CPRA and VCDPA, ColoPA provides consumers with various data subject rights, including: to access or delete personal data; correct inaccuracies in personal data; obtain personal

data in a portable format; and opt out of the processing of their personal data for targeted advertising, sale, or profiling for certain activities.

ColoPA does not prescribe the method by which controllers must allow consumers to exercise their rights, but specifies that they must "take into account the ways in which consumers normally interact with [them]." ColoPA requires controllers to provide consumers with a privacy notice that details the categories and purposes of personal data collected and shared with third parties. In addition, any controller that processes personal data for targeted advertising or sale must provide an opt-out mechanism both in its privacy policy and in another clear, conspicuous, readily accessible location.

Controllers must generally respond to consumer requests within 45 days and must create an appeal process for consumers whose requests they are not able to fulfill. Businesses should consider reviewing their privacy policies and procedures to ensure that they meet the disclosure and consumer rights requirements prescribed by ColoPA.

- **Mandatory universal opt-out mechanism:** ColoPA requires the attorney general to promulgate rules for a "universal opt-out" mechanism from targeted advertising and sale of personal data by July 1, 2023. After July 1, 2024, controllers must accommodate this mechanism. The scope of the universal opt-out provision is unique to ColoPA—although the CPRA introduces a similar procedure, it is not binding on businesses. Controllers may create procedures through which consumers may opt back in to the collection of personal data and supersede any previous decision to universally opt out. Given the uncertainty about how the attorney general will implement this provision, business should consider monitoring this topic for further updates.
- **Two tiers of personal data**: ColoPA defines personal data to cover any information "linked or reasonably linkable to an" individual, and exempts de-identified data and publicly available information from this category. Similar to the VCDPA, controllers may not process "sensitive data"—such as data relating to racial or ethnic origin, religious beliefs, health conditions, sexual orientation, citizenship status, or genetics—without obtaining a consumer's affirmative consent. Acceptance of a controller's broad terms of use, hovering over or closing a piece of content, or acceptance which is obtained through a manipulatively designed website does not suffice to establish consent. Businesses should consider inventorying the types and sources of data that they obtain from consumers to ensure they are applying ColoPA to applicable personal data. They should also consider reviewing their processes to ensure adequate notice and consent from customers—particularly for sensitive data.
- **Contracts with processors:** ColoPA requires processors and controllers to enter into a contract that describes instructions for processing personal data, the type of personal data being processed, and other provisions for carrying out the obligations of ColoPA. In addition, processors must ensure that any of their subcontractors are contractually obligated to fulfill their duties under ColoPA. Controllers should consider identifying the processors that they engage with and drafting and negotiating data contracts with them. Businesses should also note that the distinction between processor and controller is a context-dependent inquiry: if a processor begins to act as a controller, it may assume additional obligations under ColoPA.
- **Data protection assessments**: Similar to the VCDPA, ColoPA requires controllers to conduct "data protection assessments" before using data for "processing that presents a heightened risk of harm to a consumer." Activities requiring a data protection assessment include processing of personal data for targeted advertising or profiling, sale of personal data, and processing of sensitive data. While these assessments are not publicly accessible, they are reviewable by the attorney general. Although the data protection assessment requirement does not apply retroactively, companies that expect to engage in new processing of consumer's personal data after July 2023 should ensure they maintain a process to conduct assessments.

The passage of ColoPA marks a third major privacy law that will come into effect in 2023, along with the VCDPA and CPRA. Businesses should consider assessing the applicability of these laws to their operations and the measures needed to ensure compliance. Businesses also should keep a close watch on the continued evolution of U.S. data privacy legislation, as each new law that is passed can have a significant impact on their compliance programs. Previous client updates regarding related U.S. privacy laws are available here.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Mikaela Dealissia
+1 212 450 3534
mikaela.dealissia@davispolk.com

Pritesh P. Shah
+1 212 450 4147
pritesh.shah@davispolk.com