Colorado Privacy Act

Becky Burr, Adrienne Fowler, and Deepika Ravi

Colorado Governor Jared Polis has signed the Colorado Privacy Act into law, which is now officially slated to go into effect July 1, 2023. Colorado is the latest state—joining California, Nevada, and Virginia—to enact a comprehensive data privacy law akin to the European Union's GDPR and Brazil's LGPD. Like its counterparts, the Colorado Privacy Act creates privacy rights for consumers and imposes duties on "controllers" and "processors" of personal data. But no data privacy law is identical, even if the terms used may seem similar or even familiar. What follows is our high-level primer on the Colorado Privacy Act explaining its basic terms, consumer rights, duties of controllers and processors, and methods of enforcement.

Basic Terms of the Colorado Privacy Act

The Colorado Privacy Act introduces several terms that are worth reviewing before jumping into the substantive details of the Act itself.

First, the Act defines a consumer as a Colorado resident who acts in an "individual or household context" rather than "a commercial or employment context." A consumer's personal data includes any "information that is linked or reasonably linkable to an identified or identifiable individual." Certain kinds of data (e.g., race, ethnicity, religious beliefs, sex life, sexual orientation, genetic and biometric data, personal data of a known minor) are considered "sensitive" personal data, while other kinds of data (e.g., de-identified or publicly available data) are not considered personal data at all.

A controller is a business that determines the purpose and method of "processing" consumers' personal data. The act of processing includes "the collection, use, sale, storage, disclosure, analysis, deletion, or modification" of personal data, and a processor is an entity that performs these acts on behalf of a controller. A "sale" is a broad term encompassing many different types of data transfers "for monetary or other valuable consideration by a controller to a third party."

A consumer may consent to the processing of data, but that consent must be a "clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement." Importantly, the Colorado Privacy Act states that the following acts of acceptance do *not* amount to consumer consent: (1) agreeing to a general terms of use that mentions personal data processing; (2) "hovering over, muting, pausing, or closing a given piece of content"; and (3) accepting personal data processing through a "dark pattern" user interface that is designed to subvert user autonomy and choice.

The Consumer Rights Under the Act

First, consumers have the right to opt out of personal data processing for the purposes of targeted advertising, sale of personal data, or profiling of a consumer's interests and behavior. Controllers must provide consumers with a clear and conspicuous method to exercise this right.
Starting July 1, 2024, controllers must also allow consumers to exercise opt-out rights through a "user-selected universal opt-out mechanism." Allowing consumers to use a universal opt-out mechanism is optional prior to this date.

Second, consumers have the right to access their processed personal data. Third, consumers have the right to correct inaccuracies in processed personal data. Fourth, consumers have the right to delete their personal data. And fifth, consumers have the right to data portability.

Consumers can exercise any of the above rights by submitting a request to the relevant controller. The mechanism for submitting requests must be designed with the following factors in mind: (1) how consumers normally interact with the controller; (2) the need for secure and reliable communication; and (3) the ability to authenticate the identity of the consumer. This mechanism may require consumers to use an existing account, but cannot require consumers to create a new account in order to submit a request. Additionally, controllers must respond to consumer requests within 45 days, but have the option to exercise a 45-day extension as long as they inform the consumer the reasons for the delay.

The Duties Imposed Upon Controllers

First, controllers have a duty of transparency. They must disclose the categories of personal data collected and processed through a reasonably accessible and clear privacy notice. If controllers share or sell personal data to third parties, controllers must also disclose the categories of personal data shared or sold and the categories of third parties involved in this transaction. Consistent with consumer rights detailed above, controllers must clearly and conspicuously disclose how a consumer can exercise the right to opt out of the sharing or selling of her data.

Second, controllers have the duty to specify the express purpose of personal data processing. Third, controllers have the duty to minimize the processing of personal data to that which is reasonably necessary to the specified purposes. Fourth, controllers have the duty to avoid "secondary use," which encompasses any use that is not reasonably necessary or outside the scope of specified purposes. Fifth, controllers have the duty of care with respect to securing processed personal data. Sixth, controllers have the duty to avoid any processing of personal data that violates state or federal laws prohibiting discrimination. Seventh, controllers have the duty to obtain affirmative consent before processing sensitive data.

Finally, controllers also have the duty to conduct a data protection assessment prior to personal data processing that presents a heightened risk to consumers. Heightened risk is present when controllers process data for the purposes of targeted advertising, profiling consumer behavior, selling personal data, and managing sensitive data. A data protection assessment must analyze

(1) the potential benefits of data processing to "the controller, consumer, other stakeholders, and the public" and (2) the potential harms to consumer privacy rights. This assessment must be available to the Attorney General upon request.

The Colorado Privacy Act imposes the above duties upon controllers that conduct business in Colorado or furnish products or services intentionally targeted to Colorado residents. Importantly, the duties apply only to businesses that (1) control or process the personal data of 100,000 or more consumers per year and/or (2) derive revenue from the sale of personal data while processing or controlling the personal data of 25,000 or more consumers.

The Duties Imposed Upon Processors

Processors must adhere to the instructions of controllers and assist controllers to meet their duties described above by (1) taking appropriate technical and organizational measures necessary for controllers to respond to consumers' requests, (2) helping controllers implement appropriate data security measures, and (3) furnishing information relevant to data protection assessments. Processors must also ensure that their employees are subject to a duty of confidentiality regarding processed personal data.

The Methods of Enforcement

The Colorado Privacy Act confers exclusive authority to the Attorney General and District Attorneys to enforce its provisions. Prior to any enforcement action, the Attorney General or a District Attorney must issue a notice of violation to the controller and, if the violation can be remedied, allow 60 days to cure that violation. This grace provision is effective until January 1, 2025.

The Act also confers rulemaking powers to the Attorney General. Specifically, the Attorney General must adopt rules detailing technical specifications for one or more universal opt-out mechanisms by July 1, 2023.

The Act does not afford a private right of action against a controller or processor.

* * * *

For more information the Colorado Privacy Act or HWG's data privacy, security, and governance practice, please contact Becky Burr, Adrienne Fowler, Deepika Ravi, or the HWG lawyer with whom you regularly work.