BLANKROME
CELEBRATING 75 YEARS

Privacy, Security & Data Protection

JUNE 15, 2021 • NO. 4

2021 Colorado Privacy Act Passes and Heads to Governor for Signature

Colorado appears set to become the third state to adopt comprehensive privacy legislation following passage of the Colorado Privacy Act by the Colorado Legislature on June 8, 2021. The Colorado Privacy Act mimics its predecessors, the California Consumer Privacy Act and the Virginia Consumer Data Protection Act, in a number of ways, including by providing consumers the rights to access, obtain a portable copy of, correct, and delete their personal data. The Colorado Privacy Act also aims to give consumers more control over their personal data by providing consumers with the right to opt out of the sale of personal data and the processing of their personal data for purposes of targeted advertising or profiling, as well as requiring consent to process "sensitive" personal data. Despite similarities to California and Virginia laws, the Colorado Privacy Act includes unique compliance requirements. Businesses subject to the law will need to pay close attention to these differences as they ramp up compliance programs in response to various state privacy laws that will become effective in 2023.

Following California and Virginia, Colorado will likely become the third state to enact a comprehensive privacy legislation. After a series of revisions, on June 8, 2021, the Colorado Legislature passed SB 190 (the "Act"), which provides data privacy rights for Colorado residents ("consumers") similar to those provided under the California Consumer Privacy Act ("CCPA") and Virginia's Consumer Data Protection Act ("CDPA"). Unless the governor vetoes the bill within 10 days of transmission to the governor's office, the Act will come into effect July 1, 2023.

APPLICABILITY

The Act seeks to protect "personal data," which is broadly defined as information that is linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information.

The Act applies to entities that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and satisfies one or both of the following thresholds: (1) controls or processes the personal data of 100,000 consumers or more during a calendar year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more. A consumer is an individual who is a Colorado resident acting only in an individual or household context. Like the CDPA, individuals acting in a commercial or employment context, job applicants and beneficiaries of individuals acting in an employment context do not qualify as consumers under the Act.

EXEMPTIONS

Additionally, similar to the CCPA and CDPA, the Act exempts several entities and types of personal information governed under federal law, including protected health information and de-identified information under HIPAA, financial institutions and nonpublic personal information under the GLBA, information regulated by the FCRA, COPPA, and FERPA, and information regulated by the Driver's Privacy Protection Act of 1994. The Act also exempts information maintained for employment records purposes.

CONTROLLERS AND PROCESSORS

Like the EU General Data Protection Regulation ("GDPR") and CDPA, the Act distinguishes between controllers and processors. The obligation of a business under the law depends upon the role of the business with respect to the personal data at issue. A "controller" alone or jointly with others determines the purposes for and means of processing personal data. "Processors" process personal data on behalf of a controller. Controllers bear most responsibilities under the Act. However, processors have direct obligations to assist controllers with their compliance efforts. Among other responsibilities, processors must take appropriate technical and organizational measures to help controllers respond to consumers' requests to exercise their rights, provide assistance relating to the security of processing personal data and breach notifications, provide information to allow controllers to conduct and document data protection assessments ("DPA"), and allow for audits by the controller.

Controllers and processors are required to enter into a written contract for the processor's processing of the controller's personal data. The Act requires certain provisions to be included in the contract, which emulate the requirements under Article 28 of the GDPR. For instance, the agreement must set forth the type of personal data subject to the processing and the nature, purpose and duration of the processing, only allow the processor to engage a subcontractor after the processor provides the controller an opportunity to object, and requires the processor to flow down compliance obligations under the Act to subcontractors by written agreement.

CONSUMER RIGHTS

The Act provides consumers the right to opt out of the processing of their personal data for targeted advertising, sale (broadly defined as the exchange of personal data for monetary or other valuable consideration by a controller to a third party), or profiling that produces legal or similarly significant effects concerning a consumer. The Act also provides consumers rights to access, obtain a portable copy of, correct, or delete their personal data.

With respect to the right to opt out, effective July 1, 2024, consumers must be able to exercise their opt-out right through a user-selected universal opt-out mechanism that meets technical specifications to be established by the Colorado Attorney General. The Colorado Attorney General will establish the technical specifications by July 1, 2023. Unlike the CCPA, which makes a global privacy control optional, controllers must comply with the universal opt-out under the Act, which will create complexities in compliance processes for entities subject to the various comprehensive state privacy laws.

Like the CCPA and CDPA, consumers' requests must be verifiable, and a controller may deny a request if the request cannot be authenticated. The Act sets forth other reasons for denying a request, including if the data is pseudonymized (*i.e.,* it can no longer be attributed to a specific individual without the use of additional information) and the controller can demonstrate that the information necessary to identify the consumer is kept separately and subject to effective technical and organizational controls that prevent the controller from accessing such information. However, a consumer must be provided the opportunity to appeal any denials of a request.

Consistent with the CCPA and CDPA, controllers are required to respond to consumers' requests to exercise their rights within 45 days of receiving the request. This time period may be extended an additional 45 days with notice of the delay and the reasons for the delay. Controllers are required not to charge a fee for a consumer's first request but may do so for a second or subsequent request within a 12-month period.

SENSITIVE DATA

The Act affords extra protections for the processing of sensitive data. "Sensitive data" is defined as personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, or genetic or biometric data that may be processed to uniquely identify an individual or personal data from a known child. The Act requires controllers to receive a consumer's consent before processing the consumer's sensitive data. Consent must be a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous consent. Consent cannot be obtained by way of acceptance of general or broad terms of use or through "dark patterns."

DATA PROTECTION ASSESSMENTS AND OTHER CONTROLLER DUTIES

Controllers are required to conduct and document a DPA of each of its processing activities that involve personal data acquired on or after the effective date of the Act when conducting processing that presents a heighted risk of harm to a consumer. Processing that presents a heighted risk of harm to a consumer includes processing sensitive data, processing for purposes of targeted advertising, selling personal data, or profiling if there is a reasonably foreseeable risk of financial or physical injury to consumers, among other activities. The Act's examples of processing that presents a heightened risk of harm is not exclusive and so controllers will need to initially evaluate all processing activities to determine whether they potentially fall into this category and require a DPA.

DPAs must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to consumers' rights, as mitigated through safeguards the controller may employ to reduce the risks. Controllers must make the DPA available to the Colorado Attorney General upon request.

In addition to responding to consumer requests and conducting and documenting DPAs, controllers must provide a privacy notice to consumers that includes: (1) the categories of personal data collected, processed, and/or shared with third parties; (2) the purposes for processing such data; (3) the categories of third parties with whom the controller shares personal data; (4) how and where consumers may exercise their rights; and (5) whether the controller sells personal data or processes personal data for targeted advertising.

Moreover, controllers have a duty to adhere to certain principles when processing personal data, such as purpose specification, data minimization, avoiding processing for secondary purposes that are not compatible with the specified purpose, using reasonable measures to secure personal data, and avoiding unlawful discrimination. What security measures meet controller duties are not specified. The Act provides that data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business. Creating and maintaining internal processes for documenting DPAs and demonstrating that processing activities are being conducted in accordance with the requisite principals will be an important aspect of compliance with the Act.

ENFORCEMENT

The Act is enforced by the Colorado Attorney General and district attorneys and does not provide a private right of action. A 60-day cure period to rectify non-compliance is provided before the Colorado Attorney General or district attorney may take enforcement action. However, this cure period will only be provided until January 1, 2025. Non-compliance with the Act is considered a deceptive trade practice, which can result in civil penalties of up to $20,000 for each violation up to a total of $500,000 for any related series of violations.

For additional information, please contact:

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Alex C. Nisenbaum
949.812.6011 | alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com