THOMPSON HINE

Privacy & Cybersecurity Update

June 2021

Colorado Enacts New Data Privacy Law

As more states consider new privacy laws, Colorado has added itself to the list of states that have enacted comprehensive privacy legislation. On June 8, Colorado's legislature passed the Colorado Privacy Act (CPA), which grants residents new data privacy rights and creates new obligations for how businesses collect and use their personal data. Although the CPA does not create a private right of action, violations of the law constitute a deceptive trade practice, and Colorado's attorney general and local district attorneys are vested with the authority to investigate and impose civil penalties against noncompliant businesses. Unless certain state constitutional processes are invoked or the governor exercises veto authority (which is unlikely), the CPA will take effect on July 1, 2023. Although the CPA is similar to recently enacted data privacy laws in other states (e.g., California, Virginia), it does contain some unique requirements that businesses will need to address.

Scope of applicability. The CPA primarily applies to a limited set of organizations that control the processing of Colorado residents' personal data (classified as "Controllers") and to the third-party service providers who assist in the data processing activities (classified as "Processors"). These classifications mirror the structure set forth in other data protection laws (e.g., Virginia, EU GDPR). In particular, the CPA applies to Controllers conducting business in Colorado or producing or delivering commercial products or services that intentionally target Colorado residents and (i) control the collection of or process the personal data of at least 100,000 consumers annually, or (ii) derive revenue from or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of at least 25,000 consumers. The CPA defines "personal data" broadly as any "information that is linked or reasonably linkable to" an identifiable person. On the other hand, it creates many exceptions to its scope of applicability and does not, for example, apply to personal data concerning an individual acting in the commercial or employment context or to protected health information, nonpublic personal information, and other data subject to certain federal privacy laws (e.g., HIPAA, GLBA, FCRA, FERPA, COPPA).

Data privacy rights. The CPA creates several new data privacy rights and privileges for Colorado consumers:

- the right to confirm whether a Controller is processing their personal data;
- the right to access personal data in a portable, and to the extent technically feasible, readily usable format to enable transfer to another entity;
- the right to correct inaccurate personal data, and
- the right to delete personal data.

The CPA creates a framework for how Controllers must intake, authenticate and respond to consumer privacy requests and mandates that organizations create "an internal process" to allow a consumer to "appeal" a Controller's decision not to honor a data rights request, but it lacks any material specificity on how the appellate review must be formulated. It is not uncommon for Controllers to dispute that a consumer's personal data is "inaccurate" and refuse to "correct" it. In turn, the CPA provides some flexibility in this area and allows Controllers to make these decisions based on the "nature of the Personal Data and the purposes of the processing."

Opt-out rights. In addition, the CPA provides consumers with the right to opt out of the processing of their personal data to the extent it relates to targeted advertising, the sale of personal data or certain types of profiling. Consumers may exercise these rights directly or through third-party agents. The CPA further provides that Controllers must (as of July 2024) allow for consumers to exercise their opt-out rights in certain situations (e.g., targeted advertising, data sales) through a "user selected universal opt-out mechanism" that meets certain requirements set forth by the Colorado attorney general in future regulations. The CPA adopts a definition of "sale" similar to the one set forth in California's data protection law. Under the CPA, "sale" means the "exchange of Personal Data for monetary or other valuable consideration by a Controller to a third party." However, the CPA creates important exemptions to the definition of "sale," such as the disclosure of personal data to a Processor or a Controller's affiliate.

Privacy policies and other notices. A Controller is required to provide consumers with a "reasonably accessible, clear, and meaningful" privacy notice that describes its data processing activities (e.g., categories of personal data collected and processed, the express purposes of processing, types of personal data shared with third parties, categories of recipients). It must also describe how consumers can exercise their data privacy rights and the Controller's appeals process. A controller that sells personal data or uses it for targeted advertising purposes has the additional obligation to "clearly and conspicuously disclose" such processing and the manner in which consumers can exercise their opt-out rights.

Consent. The CPA limits how a Controller can use personal data without a consumer's consent. For example, a Controller must not process personal data "for purposes that are not reasonably necessary to or compatible with" the original purposes for which the personal data was collected and processed, unless it obtains the consumer's consent. Also, a Controller is prohibited from processing "Sensitive Data" without obtaining appropriate consent. The CPA defines "Sensitive Data" as personal data that reveals a consumer's racial or ethnic origin, religious beliefs, health diagnosis, sex life or sexual orientation, or immigration status; relates to certain genetic or biometric data; or involves personal data collected from a "known child." The requirement of express prior consent (as opposed to honoring after-the-fact opt-out requests) may add new burdens on Controllers.

Data protection assessments. Pursuant to the CPA, a Controller is prohibited from engaging in data processing that "presents a heightened risk of harm to a Consumer" without first undertaking a data protection assessment. In turn, the CPA defines this category of processing broadly to address a variety of common business activities, such as targeted advertising, selling of data, the processing of Sensitive Data, and certain types of profiling. The assessment must be made available to the Colorado attorney general, upon request.

Data processing agreements. Like many other data protection laws, the CPA requires Controllers and Processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and duration of data processing, the limited manner in which the Processor can use the personal data, confidentiality and employee/personnel vetting requirements, proof of compliance, and auditing. The CPA provides that Processors may only retain subcontractors after furnishing a Controller the opportunity to object to the arrangement and (if so approved by the Controller) only if the subcontractor agrees to the same data protection terms applicable to the Processor. The CPA also requires these Controller-to-Processor contracts to include clauses requiring the Processor to, at the end of the data processing services, delete or return the personal data in its custody, unless retention is required by law; however, it does not expressly create any exceptions for personal data retained in backup or archived formats.

Data security. The CPA places affirmative data security obligations on Controllers. It requires them to "take reasonable measures to secure personal data during both storage and use from unauthorized acquisition," and such measures must be appropriate to the volume, scope and nature of the personal data. The CPA does not address or otherwise attempt to limit other data security requirements set forth in other areas of Colorado law. For instance, pursuant to CO ST § 6-1-713.5, certain businesses must "implement and maintain reasonable security procedures and practices" to safeguard "personal identifying information," and these measures must be based on the "nature and size of the business and its operations."

Conclusion

Although the CPA contains some unique obligations compared to other data protection laws recently enacted (e.g., California, Virginia), it contains many common data privacy principles, and businesses that have implemented data protection programs to account for other data privacy legislation should be well positioned to comply with the CPA.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Mona Adabi
202.263.4147
Mona.Adabi@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

or any member of our Privacy & Cybersecurity group.