STINSON

News & Insights

Colorado and Other States Join the Data Privacy Law Landscape - What You Need to Know

Alert
06.22.2023

By Judith Araujo, Steve Cosentino and Simone Stover

The new Colorado Privacy Act (CPA) will take effect on July 1, 2023, requiring companies that operate within the state to comply with heightened privacy requirements. Colorado joins several other states with comprehensive privacy laws. However, the CPA contains some unique provisions that companies, including nonprofits, should take note of to avoid penalties.

KEY COMPONENTS

The CPA applies to entities that conduct business or deliver commercial products or services targeted to residents in Colorado and either: (1) process or control the data of 100,000 or more consumers annually or (2) receive any revenue or discount from selling the personal data or control of personal data of 25,000 or more consumers annually.

The CPA defines "processing" as "the collection, use, sale, storage, disclosure, analysis, deletion, or modification of Personal Data and includes the actions of a Controller directing a Processor to Process Personal Data." "Controlling" uses the common definition of determining the purposes for and means of Processing Personal Data.

These thresholds and definitions are similar to those in several other states. However, what makes the CPA unique is that it does *not* exempt nonprofit entities. For-profit *and* nonprofit entities must comply with several provisions, which include:

- Ensuring consumers' rights to the following:

  - The right to access their own data. However, entities are not required to release data in a manner that would reveal a trade secret.
  - The right to data portability. This only applies to personal data the entity possesses concerning the consumer.
  - The right to deletion. This includes any personal data the entity has about the consumer.
  - The right to correct inaccuracies in their personal data.
  - The right to opt out. In Colorado, consumers can opt out of the sale of their personal data or targeted advertising, but this process requires authentication. Additionally, companies must implement a user selected universal opt-out mechanism by July 1, 2024.
- Obtaining consent before processing sensitive data. This includes data about race or ethnic origin, religious beliefs, mental or physical health, citizenship status, sexual orientation, and identifying biometrics. Additionally, *any* personal data of children under the age of 13 falls under this umbrella.
- Providing privacy notices about how data will be used and processed. Data must be processed in a way that "ensures reasonable and appropriate administrative, technical, organizational, and physical safeguards..." Among other factors, businesses should consider industry standards, the size and complexity of the organization, and the sensitivity of the data when determining reasonable safeguards.
- Refraining from discriminating against consumers who exercise their rights.
- Entering into Data Protection Agreements with vendors to ensure compliance with the CPA and to put them in the role of "processor," as opposed to "third party" to whom opt-out rights would apply.

EXEMPTIONS

Like many other states, Colorado has carved out entity-level exemptions for companies such as financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), air carriers regulated by the Federal Aviation Administration, and national securities associations registered under the Securities Exchange Act.

While a number of other states provided entity-level exemptions for companies governed by the Health Insurance Portability and Accountability Act (HIPAA), Colorado's exemption is unique in that it only exempts data that is covered by HIPAA. That means that health care related companies in Colorado, particularly health-tech companies, will need to confirm that they are not processing personal information that falls outside of HIPAA. That often happens in the context of websites and mobile apps that provide ancillary services.

Colorado and Other States Join the Data Privacy Law Landscape - What You Need to Know

OTHER STATES

In addition to Colorado, several other states have new data privacy laws and regulations that have either taken effect or will be enacted within the year, including California, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Utah and Virginia.

Like Colorado, Connecticut's laws will go into effect on July 1 under the Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA). The CTDPA is similar to the CPA in several ways, including its trade secret exception, its registered national securities associations exemption, and its protection of personal data of individuals under 13 (though the Connecticut law also requires opt-in consent before selling or processing personal data for the purposes of targeted advertising for consumers under 16).

However, Connecticut's law is different from Colorado's in several ways. Like many other states, Connecticut's law exempts nonprofit entities. Additionally, unlike Colorado, Connecticut's law exempts higher education institutions and data covered by the Family Educational Rights and Privacy Act. Connecticut has an entity-level exemption for HIPAA covered companies. It also does not require authentication to opt out. And while Connecticut does have a similar universal opt-out mechanism requirement, it will not go into effect until January 1, 2025.

ACTION ITEMS

The CPA does not provide for a private right of action enabling private citizens to file lawsuits under the CPA. Rather, the Attorney General's Office and district attorneys will have sole enforcement power. They are required to give companies in violation of the CPA 60 days to achieve compliance. However, violations can result in civil penalties of up to $20,000 per violation. Additionally, the 60-day cure period will only be available until January 1, 2025.

With this in mind, companies should take the following steps to ensure compliance with the CPA:

- Conduct a review of your data collection, use and transfer practices.
- Conduct a review of your use of cookies and other marketing and targeted advertising tools.
- Consider adopting a website cookie consent banner to assist with enabling consumers to opt-out of targeted advertising.
- Update your data privacy policies to align with and recognize the requirements of the CPA.
- Develop a Data Protection Agreement to be used with vendors processing personal information.
- Develop a secure process for responding to Data Subject Access Requests and authenticating opt-out requests.

- Establish an annual policy for reviewing and updating your privacy policy.

For more information on the Colorado Privacy Act law landscape, please contact Judith Araujo, Deb Bayles, Steve Cosentino or the Stinson LLP contact with whom you regularly work.

Simone Stover co-wrote this article while working as a summer associate with Stinson LLP.

CONTACTS

Judith Araujo

Stephen J. Cosentino, CIPP

Simone T. Stover

RELATED CAPABILITIES

Banking & Financial Services

Business Litigation

Corporate Finance

Cybersecurity & Data Privacy

Intellectual Property & Technology

Private Business