HINSHAW

Privacy Bill Essentials: Colorado Privacy Act

Privacy, Cyber & AI Decoded Alert | 4 min read
Mar 29, 2021

On March 19, 2021, a comprehensive new bill was introduced in the Colorado Senate to protect personal data privacy. Titled the Colorado Privacy Act (CPA), the bill aims to provide Colorado consumers with additional personal data privacy rights and to implement various data-use duties upon certain entities targeting Coloradans. The bill is similar in many respects to the Virginia Consumer Data Protection Act, signed into law earlier this month.

To whom would it apply?

The CPA would apply to "controllers" that:

1. Conduct business in Colorado or otherwise produce products or services aimed at Colorado residents; and
2. Either (a) control or process the personal data of 100,000 consumers or more during a year or (b) control the personal data of at least 25,000 consumers and derive revenue or receive a discount from selling personal data.

"Controller" under the CPA means a person or group determining the purposes for and means of processing personal data. The bill defines a "consumer" as "an individual who is a Colorado resident acting only in an individual or household context" and excludes those acting in a commercial or employment context.

The CPA excludes various entities from its purview, including financial institutions or affiliates of financial institutions subject to the Gramm-Leach-Bliley Act and healthcare organizations handling protected health information.

What types of information would it cover?

Protected "personal data" is broadly defined as "information that is linked or reasonably linkable to an identified or identifiable individual." However, the CPA would not apply to employment records or personal data governed

© 2025 Hinshaw & Culbertson LLP

by applicable federal and state laws. Personal data does not include de-identified data or publicly available information, which has a similarly broad definition in the bill.

Publicly available information includes:

- Information within government records;
- Information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public or to widely distributed media; and
- Information made available to the general public by a person to whom the consumer has disclosed the information without restricting it to a specific audience.

The CPA would not cover information falling under the far-reaching definition of publicly available information.

What rights would it create?

Under the CPA, consumers would retain several rights regarding their personal data which they could exercise upon submitting a request to a controller at any time. Those rights include:

1. Opting out of personal data processing;
2. Accessing the consumer's personal data and confirm whether a controller is processing such data;
3. Correcting inaccurate data;
4. Deleting personal data; and
5. Transferring a consumer's data upon accessing the data to the extent feasible, no more than twice per year.

What obligations would it impose?

Controllers would have corresponding duties under the CPA. Mainly, controllers would have to provide consumers with a clear privacy notice that includes:

- Which categories of the consumers' personal data the controller collected or processed;
- The purpose behind processing certain categories of personal data;
- An estimate of time the controller may or will maintain the consumer's personal data;
- How consumers may exercise their rights granted by the bill;
- The categories of personal data shared with third parties; and
- The categories of third parties with whom the controller shares data with, specifically noting if the controller sells personal data for targeted advertising to which the consumer may object.

Further, the CPA would mandate controllers to (1) specify the purposes for which data is collected, (2) limit collection of personal data to what is necessary in relation to express purposes of processing the data, (3) avoid

processing personal data for unnecessary purposes, (4) take reasonable measures to secure personal data in storage and use, (5) avoid processing personal data in a way that would violate state and federal laws prohibiting unlawful discrimination, and (6) avoid processing consumers' sensitive data without first obtaining consent.

As well, controllers would be required to conduct a data protection assessment to collect and use personal data if such collection would present a heightened risk of harm to consumers. Collection that presents a heightened risk of harm includes the processing of personal data for targeted advertising or sale, or sensitive data processing. The attorney general may access and evaluate these assessments upon request to the controller.

How would it be enforced?

The CPA would be enforced exclusively by the attorney general or district attorneys. Controllers or processors in violation of the Act would be subject to a penalty under C.R.S. 6-1-112, which provides for civil penalties of not more than $2,000 per violation. The attorney general or a district attorney may seek an injunction to enjoin actions in violation of the CPA. Colorado citizens would not have a private right of action for violations of this Act.

When would it go into effect?

This Act would go into effect January 1, 2023, barring the filing of a referendum petition under the Colorado Constitution. It would apply to conduct occurring on or after the proposed date.

Where does it stand?

The CPA was introduced in the Senate on March 19, 2021, and is under consideration with the Colorado Senate Business, Labor, and Technology Committee.

Related Capabilities

Data Privacy, AI & Cybersecurity

© 2025 Hinshaw & Culbertson LLP