

Services

[Privacy & Data Security](#)

A Quick Look into Colorado, Virginia, Connecticut, Utah and California's Comprehensive Privacy Laws and Amendments

On July 1, 2023 the Colorado Privacy Act ("CPA") will become effective. The CPA will elevate Colorado to the small group of states leading the way in implementing comprehensive data privacy legislation following the 2018 adoption of the California Consumer Privacy Act ("CCPA"). Colorado, Virginia, Connecticut and Utah have all passed comprehensive state privacy laws that will become effective on various dates throughout 2023. While each privacy law has similarities to the CCPA and the California Privacy Rights Act ("CPRA"), they each have unique differences that every business should be prepared to implement if they meet the relevant thresholds and engage with personal data in those states.

Colorado:

Application and Exemptions: Effective July 1, 2023, the CPA will apply to entities that meet the following criteria: "Conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and

- controls or processes the personal data of at least 100,000 consumers or more during a calendar year; *or*
- 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."

Unlike some of the other newly passed state privacy laws, the CPA does not have a revenue threshold which results in the CPA applying to many entities regardless of the entity's size. Additionally, the CPA does not apply to certain specified entities including state and local governments and state institutions of higher education, personal data governed by listed state and federal laws, listed activities, and employment records.

Definitions: As with all laws, there are a couple of important definitions to be aware of as you consult with your legal counsel regarding the CPA's applicability to your entity. The act defines a "controller" as a person that, alone or jointly with others, determines the purposes and means of processing personal data. While it defines a "processor" to mean a person that processes personal data on behalf of a controller, the CPA defines "Personal Data" as information that is linked or reasonably linkable to an identified or identifiable individual. It is important to take note that Personal Data does not include information that is de-identified or that is publicly available.

Individual Right to Opt Out: The CPA grants Colorado residents the right to opt out of a controller's processing of their personal data, such processing including targeted advertising, sale, or profiling. Residents also have the right to access, correct, or delete the data, or obtain from a controller a portable copy of the data.

Please note that the Colorado Privacy Act broadly defines "**sale**" as "the *exchange* of personal data for monetary or *other valuable consideration* by a controller to a third party." This wording does not limit sale in the traditional sense and will require entities to reassess their data-sharing practices to ensure it does not qualify as a sale.

Once an entity has received proper authentication documentation to verify the individual's identity, it must fulfill a request of an individual exercising one of their rights within a 45-day window from the receipt of the request. If it is reasonably necessary to request an additional 45 days to complete the request, the entity can have that extension; however, the entity must communicate the reason for such extension. Unlike other state privacy laws, the CPA provides a process to appeal a denial of such request and communicate with the attorney general if individuals have concerns about the denial.

In addition to granting the rights enumerated above, the CPA also sets out additional requirements for entities to follow:

1. The CPA specifies how Controllers must fulfill duties regarding consumers' assertion of their rights, transparency, purpose specification, data minimization, avoiding secondary use, care, avoiding unlawful discrimination, and sensitive data;
2. The CPA requires that Controllers conduct a data protection assessment for each of their processing activities involving personal data that presents a heightened risk of harm to consumers; and
3. The CPA will require companies to honor a universal opt-out signal starting July 1, 2024. The attorney general may promulgate the technical specifications for a universal opt-out mechanism that controllers must use that will allow consumers to opt out of targeted advertisements and/or the sale of personal data through a universal opt-out mechanism.

The CPA specifies that a violation of its requirements can be considered a deceptive trade practice for purposes of enforcement, but the CPA may be enforced only by the attorney general or district attorneys. Please click [here](#) if you would like to read the text of the CPA directly.

Other States:

As mentioned above, California, Virginia, Connecticut, and Utah have all enacted comprehensive privacy legislation that will become effective next year. Like Colorado, those privacy laws grant consumers rights including the right to access, right to correction (except in Utah), right to deletion, right to portability, right to opt-out sale of personal data, and right to opt out of targeted advertising. Additionally, guidelines and guidance from state regulatory agencies will follow once these privacy laws become fully operative. Entities need to note the different thresholds in each state and determine whether they will be subject to the newly enacted privacy laws.

Key Contacts

Victoria "Tori" Donovan
 Denver
 (303) 292-7781
victoria.donovan@kutakrock.com

Xin Ai
 Omaha
 (402) 346-6000
xin.ai@kutakrock.com

Turquoise Early
 Omaha
 (402) 346-6000
turquoise.early@kutakrock.com

As of the date of this article, six additional states (Massachusetts, Michigan, New Jersey, North Carolina, Ohio, and Pennsylvania) have active consumer privacy bills in committee. The American Data Privacy and Protection Act was also scheduled for the House Committee markup on June 23, 2022, demonstrating a national recognition of the data privacy area. Entities are recommended to regularly check their compliance with the dynamic privacy laws.

Next Steps:

Looking forward into 2023, entities are encouraged to ensure they have a current, accessible privacy policy that is accurate and transparent as it relates to collection, use practices and consents. In preparation for these upcoming laws, entities should start mapping their personal data and assess their sharing practices to ensure they are able to accurately trace data and fulfill any information request. Depending on the size of the entity, an automated process to field such requests may be required. If you have questions about a particular privacy law, updated guidance or how your company can comply, please contact your Kutak Rock attorney or one of the authors listed on the left. You can also visit us at www.KutakRock.com.

(View the PDF here: <https://www.kutakrock.com/newspublications/publications/2022/08/colorado-virginia-connecticut-utah-and-california>)

