Connecticut Becomes Fifth State to Enact Comprehensive Data Privacy Law

05.12.2022

ATTORNEYS

Maureen E. Fulton

Mikaela M. Witherspoon

PRACTICE AREAS

Data Privacy and Security

On May 10, 2022, Governor Ned Lamont signed into law Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, making Connecticut the fifth state to enact comprehensive state privacy legislation. The law, also known as the Connecticut Data Privacy Act ("CTDPA"), will go into effect on July 1, 2023.

This law includes many of the same rights and obligations as the consumer privacy laws passed in California (the California Consumer Privacy Act of 2018 and subsequent California Privacy Rights Act), Colorado (the Colorado Privacy Act), Utah (the Utah Consumer Privacy Act) and Virginia (the Virginia Consumer Data Protection Act). The Connecticut law is most closely modeled on the Colorado Privacy Act and the Virginia Consumer Data Protection Act but includes some notable differences.

Scope of the CTDPA

The new Connecticut law will apply to legal entities conducting business in Connecticut or delivering products or services targeted to Connecticut residents that either (1) control or process the personal data of 100,000 or more consumers during a year, excluding personal data controlled or processed solely for the purpose of completing payment transactions; or (2) control or process the personal data of 25,000 or more consumers and derive more than 25 percent of their gross revenue from the sale of personal data. There is no annual revenue threshold for the Act to apply.

Connecticut Becomes Fifth State to Enact Comprehensive Data Privacy Law

"Consumers" are defined as Connecticut residents and explicitly exclude individuals acting in a commercial or employment context. "Personal data" is defined to mean information that is linked or reasonably linkable to an identified or identifiable individual. Like Virginia and Colorado, the Connecticut law's requirements will not extend to de-identified data or publicly available information. The definition of the "sale" of personal data is similar to the broad definition used in California and Colorado's laws and includes the exchange of data for monetary or other valuable consideration.

Consumers' Rights Under the CTDPA

The five primary consumer rights denoted in the CTDPA are the right to access, right to delete, right to correct, right to data portability, and right to opt out. These rights are summarized as follows:

- Right to Access: The right to confirm whether a controller is processing the consumer's personal data and to access that data. In contrast to the Virginia law, controllers are not required to provide confirmation or access if doing so would require the controller to reveal a trade secret;
- Right to Delete: Allows consumers to delete the data that was provided to or otherwise obtained by a controller;
- Right to Correct: Allows consumers to correct any inaccuracies in their personal data;
- Right to Data Portability: Allows consumers to obtain a copy of personal data processed by the controller in a portable format that allows the consumer to transmit their data to another controller, subject to the same trade secret exemption provided in the right to access; and
- Right to Opt Out: As in Virginia and Colorado, consumers have the ability to opt out of data processing used for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce "legal or similarly significant effects" concerning the individual.

Similar to California, Virginia, and Colorado's laws, the CTDPA includes a provision limiting the collection of data to data that is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed." A controller may not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer.

Consent Requirements Under the CTDPA

Connecticut Becomes Fifth State to Enact Comprehensive Data Privacy Law

Controllers must obtain opt-in consent from the consumer to collect or process sensitive personal data. This includes data relating to race, religion, mental or physical health diagnosis, sex life, sexual orientation, citizenship or immigration status; genetic or biometric data processed for the purpose of uniquely identifying an individual; personal data collected from a known child; and precise geolocation.

Opt-in consent is also required to process a consumer's personal data for targeted advertising purposes or to sell the consumer's data if the controller knows and willfully disregards that the consumer is between 13 and 16 years old.

Additional CTDPA Requirements

- Providing clear and conspicuous links that allow consumers to opt out of processing. In addition, beginning January 1, 2025, controllers must recognize universal opt-out preference signals that indicate the consumer's intent to opt out of targeted advertising and sales. This requirement also appears in the Colorado law and requires a user-friendly mechanism that allows consumers to freely and unambiguously choose to opt out of the personal data processing. A mere default setting will be insufficient. Unlike Colorado, controllers are not required to verify opt-out requests, theoretically making it easier for consumers to opt out;
- Responding to consumer requests within 45 days;
- Establishing a privacy policy. The privacy notice must disclose the categories of personal data processed, the purpose of the processing, how a consumer can exercise their rights and appeal, the categories of personal data shared with third parties, the categories of third parties with whom the controller shares personal data, a method for contacting the controller, whether personal data is sold to third parties and how to opt out, and whether personal data is used for targeted advertising and how to opt out;
- Conducting data protection assessments for activities such as using data for targeted advertising, selling personal data, processing personal data for the purpose of profiling where the profiling presents a reasonably foreseeable risk of substantial injury to consumers, and processing sensitive data;
- Implementing "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data"; and
- Implementing a data processing agreement for any processing activities undertaken by a processor on a company's behalf. The agreement must include instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.

Connecticut Becomes Fifth State to Enact Comprehensive Data Privacy Law

Enforcement

As for enforcement, like Virginia, Colorado, and Utah, Connecticut's law will not provide a private right of action to consumers, with the Connecticut Attorney General, having exclusive enforcement authority. Before initiating an action, the attorney general must notify the controller of the violation and allow the controller 60 days to cure the violation, which is double the 30-day cure period provided under the Virginia, California, and Utah laws. However, this right to cure will terminate on January 1, 2023, after which the attorney general will have discretion as to whether to allow a controller an opportunity to cure. A violation of the law will be considered an unfair trade practice under the Connecticut Unfair Trade Practices Act and entities could potentially face civil penalties of up to $5,000 per willful violation.

Exemptions Under the CTDPA

Similar to the Virginia law, the CTDPA includes both entity-level and data-level exemptions. The following types of entities are exempted: (1) state and local governments, (2) any financial institution or data subject to the Gramm-Leach-Bliley Act, (3) a covered entity or business subject to HIPAA, (4) national securities associations registered under the Securities Exchange Act of 1934, (5) a nonprofit organization, and (6) an institution of higher education. There are sixteen categories of data level exemptions, including specific information regulated by HIPAA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Airline Deregulation Act, as well as specific employee and job applicant data.

Koley Jessen will continue to monitor developments related to Connecticut's data privacy law and advise as updates become available. If you have questions on whether your business needs to comply with the this law or what steps you must take to comply with its provisions, please contact one of the specialists in Koley Jessen's Data Privacy and Security Practice Area.