# Connecticut Governor Signs Nation's Fifth Comprehensive Consumer Data Privacy Law

June 21st, 2022 | and K. Dailey Wilson

On May 10, 2022, Connecticut Governor Ned Lamont signed Substitute Bill No. 6 (the "Connecticut Data Privacy Act" or "CTDPA") into law. The CTDPA will become effective on July 1, 2023.

By enacting the CTDPA, Connecticut becomes the fifth state in the nation to implement a generally applicable consumer data privacy law, following the California Consumer Privacy Act and California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Utah Consumer Privacy Act. While the CTDPA is similar to these other state laws, small differences between these laws can have a large and variable impact on a business's data processing, considering data processing regulation is so fact-specific. The increase in the number of states passing data processing laws raises the stakes for businesses. Business attorneys should continue to monitor developments in other states, including regulatory developments in California related to changes to its data privacy laws set for January 2023.

The CTDPA applies to persons that either (A) conduct business in Connecticut, or (B) produce products or services that are targeted to residents of Connecticut; and that during the preceding calendar year: (1) controlled or processed the personal data of not less than 75,000 consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction), or (2) controlled or processed the personal data of at least 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data. The CTDPA applies to information that is linked or reasonably linkable to an identified or readily identifiable individual. The law also provides special protections for sensitive data, which includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status. Sensitive data also includes the processing of genetic personal data or certain biometric data, if the processing is for the purpose of uniquely identifying an individual, as well as precise geolocation data. The CTDPA employs a broader definition for "biometric data" than other state laws.

However, the CTDPA does not apply to, among other things:

- financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act;
- certain activities regulated by the Fair Credit Reporting Act;
- de-identified data; or
- certain publicly available information.

The CTDPA also does not restrict a controller's or processor's ability to comply with other law,

engage in certain fraud prevention and detection and security activities, or engage in certain internal processing uses, among other limited activities.

**CONSUMER RIGHTS**

The CTDPA provides consumers with a number of rights related to their personal data. Under the CTDPA, consumers have the right to:

1. confirm whether or not a controller (the person that determines the purpose and means of processing personal data) is processing personal data;
2. access their personal data;
3. correct inaccuracies in their personal data;
4. delete personal data that the consumer provided or the controller obtained about the consumer;
5. obtain a portable copy of personal data that the consumer previously provided to the controller in a format that is readily usable and allows the consumer to transmit the data to another controller without impediment; and
6. opt out of the processing of personal data for (1) targeted advertising, (2) the sale of personal data, or (3) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

The first five rights listed above do not apply to pseudonymous data, provided the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and subject to effective technical and organizational controls that prevent the controller from accessing such information. “Pseudonymous data” is defined by the CTDPA as personal data that cannot be attributed to a specific individual without the use of additional information provided such additional information is subject to the safeguards addressed above.

The CTDPA also requires controllers to adopt and offer, by July 1, 2025, a platform, technology, or mechanism that allows consumers to opt-out through an opt-out preference signal sent to the controller indicating such consumer’s intent to opt out of the sale or processing of personal data for the purposes of targeted advertising.

**CONTROLLER OBLIGATIONS**

The CTDPA imposes different obligations depending on whether the business is a controller or a processor (the entity processing personal data on behalf of the controller). Therefore, a business will need to analyze whether it is (according to the CTDPA definitions) acting as a controller or a processor when engaging in any personal data processing.

Under the CTDPA, **controllers** must, among other things:

- provide a privacy notice containing specific disclosures, including the categories of personal data processed, the purposes for which personal data are processed, how a consumer may exercise a right, the categories of personal data that the controller shares with third parties, the categories of third parties with whom the controller shares personal data, an active electronic email address that the consumer may use to contact the controller, and—if selling personal data or processing personal data for targeted advertising—a clear and conspicuous disclosure of how a consumer can opt out;
- establish, implement, and maintain reasonable administrative, technical, and physical data

security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

- not process sensitive data without first obtaining the consumer's consent or, in the case of a child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 *et seq*., setting out specific standards for adequate consent;
- provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request;
- not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge that, or willfully disregards whether, the consumer is at least thirteen years of age but younger than eighteen years of age;
- not discriminate against a consumer for exercising a right by denying a good or service to the consumer, charging the consumer a different price or rate for a good or service, or providing the consumer a different level of quality of a good or service; and
- establish a process for a consumer to appeal the controller's refusal to take action on a request to exercise the consumer's rights.

The CTDPA also requires controllers to conduct and document *data protection assessments* when conducting data processing that presents a heightened risk of harm to a consumer. Processing that presents a heightened risk of consumer harm includes:

- processing of personal data for the purposes of targeted advertising;
- sale of personal data;
- processing of personal data for profiling, where such profiling presents a reasonably foreseeable risk of certain types of harm to consumers; and
- the processing of sensitive data.

**PROCESSOR OBLIGATIONS**

A **processor** must follow a controller's instructions and must assist the controller in meeting the controller's obligations, including obligations related to data security and breach notification, as well as provide necessary information to enable the controller to conduct and document data protection assessments. Persons processing personal data must also be subject to a duty of confidentiality.

The CTDPA imposes requirements for contracts between controllers and processors as well as requirements for engaging subcontractors, including requiring the subcontractor in writing to meet the obligations of the processor regarding personal data.

**ENFORCEMENT**

The Connecticut Attorney General has the exclusive authority to enforce the CTDPA. From July 1,

2023, until December 31, 2024, the attorney general must issue a notice of violation to the controller if the attorney general determines that a cure is possible. The controller will have sixty days to cure the violation. Beginning on January 1, 2025, the attorney general will have the authority to decide whether to grant a controller or processor the opportunity to cure an alleged violation, taking into consideration the number of violations, the size and complexity of the controller or processor, the nature and extent of the controller's or processor's processing activities, the substantial likelihood of harm to the public, and the safety of persons or property. A violation of the CTDPA will constitute an unfair trade practice. Penalties for engaging in an unfair trade practice include imposition of a restraining order, civil penalties of up to $5,000 for willful violations, and, in the case of private litigation, actual and punitive damages as well as court costs and attorneys' fees.

The CTDPA does not provide for a private right of action by consumers.