



May 18, 2022

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[Jean Paul Yugo](#)

[Nagashima](#)

[Michael E. Nitardy](#)

[Samantha M. Berten](#)

Connecticut is the Fifth State to Have a Comprehensive Privacy Law

When Connecticut passed S.B. No. 6 – Connecticut Data Privacy Act (CTDPA), it became the fifth state in the U.S. to have a data privacy protection law. CTDPA will become effective on July 1, 2023. Below is a quick summary of the CTDPA.

Who is Covered?

The law applies to persons who conduct business in Connecticut or produce services that are targeted to residents of Connecticut. Additionally, during the preceding calendar year, such persons must have:

- controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

This is very similar to other data privacy laws, such as the Utah Consumer Privacy Act (UCPA), though the Connecticut law lowers the gross revenue threshold to 25% instead of 50%.

The law does not apply to government data or data from any political subdivision of the state, nonprofit organizations, higher education institutions, SEC national securities associations, financial institutions, or data subject to the Gramm–Leach–Bliley Act (GLBA), data subject to the Family Educational Rights and Privacy Act (FERPA), or Health Insurance Portability and Accountability Act (HIPAA) covered entities or business associates.

What is the Definition of a Sale?

A sale is broadly defined as “the exchange of personal data for monetary or other valuable consideration by the controller to a

third party.” This does not include:

- the disclosure of personal data to a processor that processes the data on behalf of the controller;
- the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- the disclosure or transfer to an affiliate of the controller;
- the disclosure of personal data where the consumer directs the controller to disclose the data or to interact with a third party;
- the disclosure of data the consumer intentionally makes available to the public and did not restrict to a specific audience; or
- disclosure or transfer of personal data to a third party as part of a merger, acquisition or bankruptcy action.

What Rights are Provided to Whom under CTDPA?

Like the data privacy laws in California, Colorado, Virginia and Utah, a Connecticut consumer has the right to:

- confirm whether or not a controller is processing their data and the consumer may access their data;
- correct inaccuracies in the consumer’s personal data;
- delete personal data provided by, or obtained about, the consumer;
- obtain a copy of the consumer’s personal data;
- opt-out of the processing of their personal data for the purposes of (A) targeted advertising, (B) the sale of their personal data, or (C) profiling in furtherance of solely automated decisions.

The opt-out right will become effective on January 1, 2025.

How are Sensitive Data Treated under the CTDPA?

Like the California Consumer Privacy Act, the CTDPA defines sensitive data as personal data that includes the following:

- data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status;
- the processing of genetic or biometric data for the purpose of uniquely identifying an individual;
- personal data collected from a known child; or
- precise geolocation data.

Websites and companies must obtain consent to process sensitive data and need to offer Connecticut residents ways to revoke such consent. Further, once consent is revoked, websites and companies will only have 15 days to stop processing such data.

Additionally, businesses are banned from collecting personal data and using targeted advertising on children between the ages of 13 and 16. The law also forces companies to honor browser privacy signals so that consumers can opt-out of data sales from all companies in one step.

Who will Enforce the CTDPA?

The Connecticut Office of the Attorney General will enforce the law, with a penalty of up to \$5,000 under the Connecticut Unfair Trade Practice Act, plus actual and punitive damages, costs, and reasonable attorney's fees. Through 2024, there is a 60-day cure period for any violations, but after 2025 the only opportunity to cure will be at the discretion of the attorney general.

What Other Obligations do Controllers Have Under the CTDPA?

The CTDPA requires the controller to conduct a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. Processing of heightened risk of harm to a consumer includes:

- the processing of personal data for purposes of targeted advertising;
- the sale of personal data;

- the processing of personal data for the purpose of profiling, where such profiling presents a reasonably foreseeable risk of the following:
 - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
 - financial, physical or reputational injury to consumers;
 - a physical or other intrusions upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
 - other substantial injury to consumers; and
- the processing of sensitive data.

The Attorney General may require that the data protection assessment be made available to the Attorney General if it becomes relevant in an investigation.

What is the Impact of CTDPA?

This law further labels California's consumer privacy law as an outlier. California is now the only state out of five that has a private right of action for a data breach and extends rights to workforce members and business-to-business contacts. Now, it seems clear that the trend is to have laws that require notice and provide consumers rights but is not as overly broad as California's privacy law. However, the Connecticut law is much more consumer-focused than Utah's privacy law because it focuses on allowing consumers the right to opt-out.

For further information, please contact [Michael E. Nitardy](#), [Jean Paul Yugo Nagashima](#), [Samantha Berten](#), or any other member of Frost Brown Todd's [Privacy & Data Security](#) practice group.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.