

And Then There Were Five: Connecticut Adopts Comprehensive State Privacy Law

May 2022

Privacy In Focus®

On May 10, 2022, Connecticut became the fifth state in the nation to pass its own omnibus privacy legislation, joining California, Virginia, Colorado, and Utah. While Senate Bill 6, the Personal Data Privacy and Online Monitoring Act (CTDPA), shares some similarity with other state privacy laws, there are nuances to the CTDPA that add to the growing patchwork of state laws that nationwide companies will need to contend with.

Indeed, companies need to act quickly to update their compliance programs. The CTDPA is set to go into effect on July 1, 2023 – at the same time that the Colorado Privacy Act takes effect – leap-frogging ahead of the Utah Consumer Privacy Act, which takes effect on December 31, 2023. The Connecticut and Colorado laws take effect six months after the Virginia Consumer Data Protection Act (VCTDPA) and California Privacy Rights Act (CPRA), both of which have January 1, 2023 effective dates.

Below, we provide a high-level summary of the new law, including which entities the CTDPA will apply to and five key aspects that companies should be aware of as they plan their compliance strategies.

Does the CTDPA Apply to Your Organization?

The CTDPA generally applies to entities that do business in Connecticut, or that produce products or services that are targeted to Connecticut residents, and that either: (1) control or process the personal data of not less than 100,000 or more Connecticut resident

Authors

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
State Privacy Laws

consumers during the preceding calendar year; or (2) control or process the personal data of not less than 25,000 Connecticut resident consumers *and* derived more than 25% of their gross revenue from the sale of personal data.

The Connecticut law exempts certain entities, including exemptions for certain nonprofit organizations. It also has exemptions related to federal privacy frameworks, including the Gramm-Leach-Bliley Act (GLBA) provisions; the Health Information Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA).

5 Key Aspects of the CTDPA

1. Consumer Rights. The CTDPA establishes five rights for Connecticut consumers, listed below. Like the laws in Virginia, Colorado, and Utah, these rights do not extend to individuals acting in a commercial or employment context.

- Right to opt out: Consumers have the right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects.
- Right to know/access: Consumers have the right to confirm whether or not a data controller is processing the consumer's personal data and to access that personal data.
- Right to correction: Consumers have the right to correct inaccuracies in their personal data, taking into account the nature of the personal data and the purposes for which it is processed.
- Right to deletion: Consumers have the right to delete personal data provided by, or obtained about, the consumer.
- Right to data portability: When exercising their right to access, consumers have the right to obtain their personal data in a portable and readily usable format that allows the consumer to easily transmit the data to another entity.

2. Obligations on Data Controllers. Under the CTPDA, controllers of personal data are subject to a number of duties, including obligations to:

- Provide consumers with privacy notices;
- Provide an opt-out link and mechanism;
- Maintain reasonable security practices regarding personal data;
- Provide consumers with notice and seek opt-in consent before processing sensitive data;
- Offer consumers an appeal process when a consumer request is denied;
- Not discriminate against consumers that exercise their rights; and
- Conduct privacy risk assessments for certain activities.

Additionally, a controller must also enter into a contract with a processor that sets out certain criteria for the personal data that will be processed, and how that data will be processed and retained, among other things.

3. Opt-Out Preference Signal. Like the Colorado law, the new CTDPA will require a controller to offer an opt-out preference signal that allows a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data. However, this provision of the law has a delayed implementation deadline of January 1, 2025.

4. Sunsetting Right to Cure. The Attorney General, prior to initiating any action for a violation, must issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within 60 days, the AG may initiate an action. The right to cure sunsets on December 31, 2024.

5. Study Task Force. The CTDPA also creates a task force to study, among other potential topics, algorithmic decision-making, children's data, and possible legislation that would expand the state's consumer privacy rights. The task force is set to convene no later than September 1, 2022 and is expected to submit a report on its findings and recommendations no later than January 1, 2023.

© 2022 Wiley Rein LLP