CONNECTICUT BECOMES THE FIFTH STATE TO ENACT A COMPREHENSIVE CONSUMER PRIVACY LAW

Eliza Davis

Aviva Surugeon

On May 10, 2022, Connecticut became the fifth state to enact comprehensive privacy legislation when Gov. Ned Lamont signed the Connecticut Data Privacy Act (CTDPA) into law. The CTDPA includes many of the same obligations and exceptions as the consumer privacy laws in California (CCPA), Colorado (CPA), Virginia (VCDPA), and Utah (UCPA). Many of the CTDPA's provisions either mirror or fall somewhere between the CPA and VCDPA; however, there are a few distinctions that companies should note before the CTDPA goes into effect on July 1, 2023.

To Whom Does It Apply?

The CTDPA applies to entities that conduct business in Connecticut or produce products or services targeted to Connecticut residents and that during the preceding calendar year, either:

- Controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing payment transactions.
- Controlled or processed the personal data of at least 25,000 consumers and derived over 25% of their gross revenue from the sale of personal data.

Notably, the CTDPA does not impose an annual revenue threshold obligation. In practice, this means that, unlike the CCPA, an entity is not subject to the law based solely on its annual revenues; and unlike the UCPA, entities do not need to exceed a certain annual revenue requirement to fall within the CTDPA's scope. Additionally, the explicit exclusion of personal data processed solely for payment transactions means businesses that process debit or credit cards only to the extent necessary to complete a sale will not be subject to the law's requirements.

Further, the CTDPA does not apply to, among others:

- Government entities;
- Higher education institutions;
- Non-profits;
- Businesses that are covered entities pursuant to HIPAA; and
- Information subject to HIPAA, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, or the Drivers Privacy Protection Act.

Scope

Under the CTDPA, "consumer" is defined as a Connecticut resident and explicitly excludes individuals "acting in a commercial or employment context." The CTDPA defines personal data as "information that is linked or reasonably linked to an identified individual or an identifiable individual." Like the CPA and VCDPA, the CTDPA specifies that deidentified data or publicly available information does not constitute personal data. Under the CTDPA, publicly available information means "information that (a) is lawfully made available through federal, state or municipal government records or widely distributed media, and (b) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public." Deriving a CPA-like definition, the CTDPA defines the "sale of personal data" as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party."

Consumer Rights

Similar to the VCDPA and CPA, the CTDPA provides consumers with several rights, including:

- To confirm whether a controller is processing the consumer's personal data;
- To correct inaccuracies in the consumer's personal data;
- To obtain a copy of consumer's personal data that the consumer previously provided to the controller;
- To opt-out of the processing of personal data for purposes of targeted advertising or the sale of personal data; and
- Data deletion.

Exercising Consumer Rights

A consumer may exercise a right by submitting a request to a controller, specifying which right the consumer intends to protect. Once a consumer submits a request, the controller has 45 days to:

- Take action on the consumer's request and inform the consumer of any action taken; or
- Inform the consumer of any reasons the controller is not taking action in response to the consumer's request; or
- Extend the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity or volume of the consumer's request and inform the consumer of the reason and length of the extension.

A controller may not charge the consumer a fee in response to the request unless it is the consumer's second request in a 12-month period. A controller may, however, charge a "reasonable fee to cover the administrative costs of complying with the request."

Data Controller Obligations

Similar to the European General Data Protection Regulation, the CTDPA establishes "controller" and "processor" roles, which differentiate how entities handle personal data. Controllers are those who determine the purposes and means of processing personal data, while processors are entities that process personal data on behalf of a controller and at the controller's direction. The law assigns different obligations based on an entity's status as a controller or processor. The CTDPA imposes several obligations on controllers, including:

- Limiting the collection of personal data to "what is adequate, relevant, and reasonably necessary" to the purposes for processing, as disclosed to the consumer;
- Providing consumers with privacy notices;
- Establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices to protect confidentiality, integrity, and accessibility of personal data; and
- Outlining contractual requirements in engaging data processors.

Similar to the CPA and VCDPA, the CTDPA requires controllers to obtain parental consent for the collection of personal data from a known child (i.e., under 13 years old). The CTDPA also joins the CPRA, VCDPA, and CPA in requiring controllers to conduct data protection assessments prior to engaging in data processing activities that present a higher risk to consumers.

Sensitive Data

Under Under the CTDPA, controllers are prohibited from processing "sensitive data" without first giving the consumer explicit notice and providing an opportunity to opt-out of processing. Sensitive data includes:

- Racial or ethnic origins;
- Religious beliefs;
- Sexual orientation;
- Citizenship/immigration status;
- Biometric information;
- Health information;
- Data collected from a known child; and
- Precise geolocation.

Enforcement

Similar to other privacy laws, the CTDPA does not provide for a private right of action. The CTDPA closely mirrors Virginia's approach in that enforcement falls solely to the attorney general. Prior to initiating an action, the attorney general must notify the controller of its violation. The CTDPA then gives a controller 60 days to cure the violation, which is double the 30-day cure periods granted under the CCPA, UCPA, and VDCPA. The CTDPA's right to cure, however, will cease to be required beginning Jan. 1, 2025, after which the attorney general will have discretion in whether to provide an opportunity to cure. A violation of the law is considered an unfair trade practice under the Connecticut Unfair Trade Practices Act, and, therefore, entities could face civil penalties up to $5,000 per willful violation.

Looking Ahead

We anticipate that 2022 will continue to be an active year for privacy regulations – with more and more states enacting their own comprehensive privacy laws. While preparing for CTDPA, which goes into effect on July 1, 2023, businesses can leverage their compliance efforts with other privacy laws, particularly the CPA; however, it is important to pay attention to the nuances between the patchwork of privacy regulations. For example, the CTDPA's heightened protections for children's data will require particular attention and analysis when developing a privacy program.

Redgrave will continue to monitor developments in this area. We advise companies on how to address privacy and security issues, including crafting comprehensive privacy programs that account for state specific regulations.

For additional information on this topic, please contact the authors **Eliza Davis** and **Aviva Surugeon.** For further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*