THOMPSON HINE

Privacy & Cybersecurity Update

May 2022

Connecticut Enacts New Consumer Data Privacy Law

Connecticut joined the ranks of U.S. states that have enacted comprehensive privacy legislation when on May 10, Connecticut Governor Ned Lamont signed into law the Connecticut Data Privacy Act (CTDPA), which grants consumers new data privacy rights and creates new obligations for how businesses collect and use their personal data. Although the CTDPA does not create a private right of action, a violation of the law constitutes an "unfair trade practice" and Connecticut's attorney general is vested with the authority to enforce such violations. The CTDPA will take effect on July 1, 2023. Similar to recently enacted data privacy laws in other states (e.g., California, Virginia, Colorado, Utah), the CTDPA contains requirements that businesses will need to address in their data privacy compliance programs.

Scope of applicability. The CTDPA primarily applies to organizations that process Connecticut residents' personal data ("Controllers") and to the third-party service providers that assist Controllers in data processing activities ("Processors"). In particular, the CTDPA applies to Controllers that conduct business in Connecticut or produce products or services that target Connecticut residents and during the preceding calendar year either (i) controlled or processed personal data of at least 75,000 consumers, excluding personal data used solely for completing payment transactions, or (ii) controlled or processed personal data of at least 25,000 consumers and derived over 25% of their gross revenue from the sale of personal data.

Definition of personal data. In line with other data privacy laws, the CTDPA defines personal data broadly as any "information that is linked or reasonably linkable" to an identified or an identifiable individual. It, however, provides many exceptions to its scope of applicability and does not, for example, apply to personal data processed in the commercial or employment context or to protected health information, publicly available information, or other data subject to certain federal laws (e.g., HIPAA, GLBA, FCRA, FERPA).

Data privacy rights. The CTDPA creates several new data privacy rights and privileges for Connecticut consumers:

- The right to confirm whether a Controller is processing their personal data and to access such personal data.
- The right to correct inaccuracies in their personal data.
- The right to obtain a copy of such personal data in a portable, and to the extent technically feasible, readily usable format to enable transfer to another entity.
- The right to delete personal data provided by or concerning the consumer.

The CTDPA creates a framework for how Controllers must intake, authenticate, and respond to consumer privacy requests and mandates that organizations "establish a process" to allow a consumer to "appeal" a Controller's refusal to act on a data rights request. The CTDPA specifies that appeal process must be conspicuously available and similar to the process for intaking privacy rights requests. The Controller must inform the consumer in writing about the actions taken in response to the appeal, including the reasons for the decisions, and how the consumer may contact the attorney general to submit a complaint.

Opt-out rights. The CTDPA provides consumers with the right to opt out of the processing of their personal data to the extent it relates to targeted advertising, the sale of personal data, or certain types of profiling that have significant impact on the consumer. Further, consumers

may exercise these rights directly or through third-party agents. The CTDPA further provides that Controllers must (as of January 1, 2025) allow consumers to exercise their opt-out rights in certain situations (e.g., targeted advertising, data sales) through "an opt-out preference signal sent, with such consumer's consent," by a platform, technology, or mechanism. The CTDPA adopts a definition of sale similar to the ones set forth in California's and Colorado's data protection laws. Under the CTDPA, "sale" means "the exchange of personal data for monetary or other valuable consideration by a Controller to a third party." The CTDPA creates common exemptions to the definition of sale, such as the disclosure of personal data to a Processor or a Controller's affiliate. The term "targeted advertising" essentially refers to a Controller's ability to display an advertisement to consumers based on their personal data collected over time from their online activities and to predict preferences or interests.

Rewards programs and anti-discrimination. The CTDPA, like other state data protection laws, permits Controllers to offer consumers different services or similar services at different prices that are related to loyalty or rewards programs. However, a Controller may not discriminate against a consumer for exercising a data privacy right (e.g., by denying the consumer a good or service or charging a different price, or by providing a different level of quality of a good or service). In addition, a Controller is not required to provide any product, service, or functionality to a consumer if the consumer must furnish their personal data but fails to do so.

Consent. The CTDPA limits how a Controller can use personal data without a consumer's consent. For example, a Controller must obtain consent to process a consumer's personal data for purposes other than those for which the data was collected. A Controller is also prohibited from processing sensitive data without obtaining appropriate consent. The CTDPA defines "sensitive data" as personal data that reveals a consumer's racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship or immigration status, personal data from a known child, precise geolocation data, or certain genetic or biometric data.

Data protection assessments. When engaging in data processing that "presents a heightened risk of harm to a Consumer," the CTDPA requires a Controller to conduct and document a data processing assessment. In turn, the CTDPA defines this category of processing broadly to address a variety of common business activities, such as targeted advertising, selling of data, processing of sensitive data, and certain types of profiling. The assessment must be made available to the Connecticut attorney general upon request.

Processor obligations and contracts. The CTDPA places affirmative obligations on Processors, such as those related to compliance with a Controller's instructions and the implementation of security controls to safeguard personal data from unauthorized use. Like many other data protection laws, it also requires Controllers and Processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, the limited manner in which the Processor can use the personal data, confidentiality, and compliance assessments. The CTDPA also requires these Controller-to-Processor contracts to include clauses requiring the Processor to, at the end of the data processing services, delete or return the personal data in its custody, unless retention is required by law. In addition, the CTDPA mandates written contracts between Processors and subcontractors that require the subcontractor to meet the Processor's obligations with respect to personal data.

Privacy policies and other notices. Controllers are required to provide consumers with a "reasonably accessible and clear" privacy notice that describes their data processing activities (e.g., categories of personal data collected and processed, purposes of processing, categories of personal data shared with third parties, categories of recipients). The notice must also describe how consumers can exercise their data privacy rights, including how they can appeal a Controller's decision. A Controller that sells personal data or uses it for targeted purposes has the additional obligation to "clearly and conspicuously disclose" such processing and how consumers can exercise their opt-out rights.

Data security. The CTDPA places affirmative data security obligations on Controllers. It requires them to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices," which must be appropriate to the volume and nature of the personal data.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com