wiley

ALERT

Major Changes to Connecticut's Consumer Privacy Law Will Take Effect July 1, 2026

April 27, 2026

The Connecticut Data Privacy Act (CTDPA) is set to undergo major changes as of July 1, 2026, when key amendments to the law take effect. The amendments will expand the scope of the CTDPA's applicability and update requirements relating to sensitive data, consumer rights (including profiling), minors' data, privacy notices, and privacy assessment obligations, among other areas.

Below, we highlight several consequential updates for organizations subject to the Connecticut law and outline steps organizations can take now to prepare for these changes.

Key Changes to the CTDPA Under July 2026 Amendments

Expanded Applicability Triggers. The amendments expand the universe of organizations that may be subject to the CTDPA by (i) lowering the minimum processing threshold, and (ii) creating new "no-threshold" triggers tied to certain activities. Specifically, under the amendments, the CTDPA will apply to entities that conduct business in Connecticut or target products or services to Connecticut residents and, during the preceding calendar year:

- Controlled or processed personal data of at least 35,000 consumers, excluding personal data controlled or processed solely to complete a payment transaction;
- Controlled or processed consumers' sensitive data, excluding personal data controlled or processed solely to complete a payment transaction; or
- Offered consumers' personal data for sale.

Authors

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Ania Trichet
Associate
202.719.4737
atrichet@wiley.law

Practice Areas

Advertising Technology (AdTech) Data Privacy and Consumer Protection
FTC and Consumer Protection
Privacy, Cyber & Data Governance
State Privacy Laws

Of note, the 35,000-consumer threshold in the first applicability trigger was lowered from 100,000, and the second and third applicability triggers have no volume thresholds.

The CTDPA still contains various exceptions, including new and clarified exceptions that organizations should review carefully in determining applicability.

Broadened Definition and New Restrictions for Sensitive Data. The amendments expand the CTDPA's definition of "sensitive data" to encompass additional types of data, including certain government identifiers (e.g., driver's license/passport), financial account-related elements, and Social Security numbers (SSNs). In addition to the preexisting requirements related to sensitive data, such as a requirement to obtain consent prior to processing sensitive data, the amendments now expressly prohibit the sale of sensitive data without consumer consent.

Additions and Updates to Consumer Rights. The amendments also change the consumer rights granted by the law in significant ways. For example, the amendments:

- Establish new rights tied to certain covered automated profiling decisions, including the rights for consumers to question outcomes, be informed of reasoning, review data used, and (in certain contexts) correct and request reevaluation of decisions;
- Establish a new right to obtain a list of third parties to whom the controller has sold the consumer's personal data; and
- Make changes to existing consumer rights as well, including by expressly including inferences derived from the consumer's personal data and certain covered automated profiling information under the right to know and the right to access certain personal data, and by expanding the right to opt out to include any covered automated profiling decision, not just those that are solely automated.

Additionally, the amendments clarify that controllers may not provide certain categories of sensitive data (e.g., SSNs, certain financial data, biometric elements) in response to consumer requests; instead, the controller must only confirm this data was collected.

New Prohibition on Certain Processing of Youth Data. Under the existing CTDPA, prior to engaging in targeted advertising or selling the personal data of individuals between ages 13-16, controllers were required to obtain opt-in consent. The amendments expand the protected age range to 13-17, and impose a blanket prohibition on targeted advertising and the sale of personal data for this age group, regardless of consent, where the controller has "actual knowledge, or wilfully disregards, that the consumer is at least [13] but younger than [18]."

Additions to Privacy Notice Requirements. The amendments update privacy notice requirements by adding new content and more prescriptive presentation obligations. Specifically, notices will need to disclose whether the entity uses or sells personal data to train large language models (LLMs). The amendments also prescribe how the link to the notice should be displayed and include procedures for retroactive material changes.

New Impact Assessment Requirement for Certain Covered Automated Profiling. The amendments add a new impact assessment requirement specifically where controllers engage in "any profiling for the purposes of making a decision that produces any legal or similarly significant effect." The impact assessment requirement will apply to processing activities created or generated on or after August 1, 2026.

Updated Controller Duties. In addition to the new duties listed above to require consent for selling sensitive data and prohibit certain processing activities with respect to youth data, the amendments also update other controller duties, including (1) making changes to the standards for data minimization and secondary data uses; (2) adding a "reasonably necessary" requirement for controllers to process sensitive data (in addition to the existing consent requirement); and (3) reinforcing and strengthening antidiscrimination expectations.

Compliance Considerations Ahead of July 1, 2026

Organizations evaluating readiness for the July 2026 amendments may consider the following actions:

1. Assess applicability under the new 35,000-consumer threshold and the "no-threshold" triggers for processing sensitive data and selling personal data. Under these new applicability triggers, some businesses that were not subject to the CTDPA prior to July may now be within the scope of the law.
2. Map data against the expanded definition of sensitive data to ensure compliance for this broader set of data, including the requirements to obtain consent for the processing and sale of sensitive data.
3. Update consumer rights notices and operations to accommodate new and expanded rights and implement new limitations on data that may be provided in response to a consumer request.
4. Assess whether the organization has actual knowledge of processing data of individuals under the age of 18, and if so, ensure compliance with specific processing restrictions.
5. Refresh privacy notices to meet the new content and presentation requirements, including but not limited to adding the new LLM training disclosure.
6. Review profiling governance and assessment templates to incorporate new impact assessment expectations.