CLIENT ALERTS & INSIGHTS

Connecticut Broadens Data Privacy Act Requirements Effective July 1, 2026

JUNE 3, 2026

Authors: Ryan T. Sulkin, Jacob “Jake” Bennett

Featured Practices: Data Privacy & Cybersecurity, Intellectual Property, State Attorneys General Investigations & Enforcement

Key Takeaways

- Amendments to the Connecticut Data Privacy Act (the “CTDPA”) take effect July 1, 2026, bringing more businesses under the law and updating requirements for sensitive data, consumer rights, privacy notices, and more.
- The lowered applicability thresholds and elimination of a guaranteed cure period significantly increase enforcement risk, exposing more businesses to penalties and scrutiny.
- Organizations should update data governance, consent practices, and privacy disclosures now to ensure compliance ahead of the July 2026 deadline and prepare for further obligations under SB 4 later in the year.

Revised Applicability Scope and Exemptions

Effective July 1, 2026, the CTDPA’s existing applicability thresholds are reduced, resulting in the CTDPA covering businesses processing personal data of at least 35,000 Connecticut residents or selling personal data of at least one resident. Notably, a business “sells” personal data under the CTDPA when it exchanges such data for monetary or other valuable consideration with a third party. Previously, businesses had to process the personal data of (i) 100,000+ residents, or (ii) 25,000+ residents with over 25% of their revenue from selling such data. The amendments also establish a new threshold: businesses controlling or processing a single Connecticut resident’s sensitive data, as defined thereunder, are now subject to the CTDPA. Additionally, the blanket entity-level exemption for GLBA-regulated entities is now a data-level exemption for GLBA information and entity-level exemptions for certain traditional financial institutions.

Sensitive Data Revised Definition and Requirements

The definition of “sensitive data” now includes personal data revealing mental or physical disability or treatment, nonbinary status, transgender status, information derived from biometric and genetic data, neural data, financial account information, and government-issued identification numbers (i.e., driver’s licenses, SSNs, passports). In addition to obtaining consent prior to processing sensitive data, such processing must be reasonably necessary in relation to the purpose for which such

sensitive data is processed, and the CTDPA now expressly prohibits the sale of sensitive data without consumer consent.

New and Expanded Data Subject Rights

With the amendments, Connecticut residents gain new data subject rights. Data subjects may request (i) a list of third parties to whom the controller has sold their personal data, (ii) access to inferences derived from their data, (iii) information on whether their data is processed for certain profiling purposes (i.e., processing to evaluate or predict personal aspects such as a consumer's economic situation, health, preferences, behavior, or location), and (iv) information on automated decision profiling results, the rationale of such profiling, the ability to review the data processed during such profiling, and, in certain instances involving housing, the right to require a rerun of the analysis after correcting inaccurate personal data.

Additional Privacy Notice Disclosures

The CTDPA now prescribes how and where privacy notices must be displayed, required languages, and when to inform residents of changes to notices or a business's practices more broadly. The amended CTDPA requires residents to be notified of material changes to the privacy notice and given an opportunity to withdraw consent to any further, materially different collection or use of previously collected personal data. This aligns with the Federal Trade Commission's stance that retroactive privacy notice changes may be unfair or deceptive to consumers.

Other Amendment Changes

In addition to the above, the CTDPA amendments also (i) update the data minimization requirement to what is reasonably necessary and proportionate (as opposed to adequate, relevant, and reasonably necessary) to the disclosed purpose, (ii) add a new impact assessment requirement for certain profiling activities (i.e., profiling for the purposes of making a decision that produces any legal or similarly significant effect), (iii) add a duty for processors to help controllers with data subject requests "insofar as is possible" rather than as is "reasonably practicable," and (iv) add a prohibition on sharing personal data for targeted advertising and selling personal data when the controller has actual knowledge, or willfully disregards, that the data subject is a minor.

Looking Forward

With the expanded scope, many businesses previously outside the CTDPA are now subject to it. The Connecticut Attorney General, the regulator enforcing the CTDPA, is a Consortium of Privacy Regulators member and has publicly committed to investigative sweeps. Further, the statutory cure period under the CTDPA expired at the end of 2024, meaning businesses will not have a guaranteed opportunity to remedy an issue before enforcement action is taken. Given this heightened enforcement environment, compliance with the complex patchwork of U.S. privacy laws is more critical than ever. While achieving compliance may be costly and cumbersome, risks and penalties from noncompliance continue to increase as more states broaden their laws while simultaneously coordinating on enforcement. We recommend that clients within the scope of the amended CTDPA proactively bring their privacy practices into compliance with the law before the July 1, 2026, effective date to reduce the risk of enforcement and increased penalties.

Additionally, on May 27, 2026, Governor Ned Lamont signed SB 4

which, among other things, amends the CTDPA to (i) prohibit the sale of precise geolocation data, (ii) establish new requirements concerning facial recognition technology, (iii) redefine "publicly available information" and deletion rights related thereto, and (iv) remove the materiality threshold from its purpose limitation. While the SB 4 amendments are not effective until October 1, 2026, they echo the ongoing trend of state privacy law changes that businesses must continue to monitor and remain in compliance with.

Ryan Sulkin is Team Lead of Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.624.6398 or rsulkin@beneschlaw.com.

Jake Bennett is an Associate in Benesch's Data Privacy & Cybersecurity Practice Group. He can be reached at 312.517.9561 or jbennett@beneschlaw.com.