



Connecticut Data Privacy Act (“CTDPA”) Compliance Snapshot

Understand the Law. Identify Your Obligations. Prepare for Compliance.

This CLIClaw Compliance Snapshot provides a concise overview of the Connecticut Data Privacy Act (“CTDPA”), including its applicability, consumer privacy rights, key business obligations, third-party requirements, enforcement provisions, and compliance considerations.

Designed as a practical reference for businesses, the snapshot helps organizations understand the law's principal requirements, evaluate potential applicability, and identify areas that may require additional compliance planning or operational review.

Use this snapshot as a starting point for understanding Connecticut's privacy requirements and determining whether further assessment, implementation, or legal guidance is needed.

DISCLAIMER

These materials are provided for informational and compliance support purposes only and are not intended as legal advice. Use of these materials does not establish an attorney-client relationship.

Organizations are responsible for evaluating applicable legal requirements and should consult qualified legal counsel regarding specific obligations.

CLIClaw makes no warranties regarding the completeness or applicability of these materials and disclaims liability for reliance on their use.

CONNECTICUT DATA PRIVACY ACT (CTDPA) 2026 COMPLIANCE SNAPSHOT

Public Act 23-3 | Effective July 1, 2023 | Updated October 16, 2026



The Connecticut Data Privacy Act (CTDPA) establishes consumer privacy rights and compliance obligations for organizations that collect, use, or disclose personal data of Connecticut residents. The law has been amended to address, among other things, sensitive data, facial recognition, precise geolocation, profiling, and data brokers.

01

APPLICABILITY

Which Organizations May Be Covered?



- Applies to organizations that conduct business in Connecticut or produce products or services targeted to Connecticut residents and that:
 - Process the personal data of at least 35,000 Connecticut residents in a calendar year; or
 - Process the personal data of at least 10,000 Connecticut residents and derive more than 25% of gross revenue from the sale of personal data.
- Certain organizations and data types are exempt, including nonprofits and certain government entities.
- Additional provisions apply to specific activities, such as data brokers.

02

CONNECTICUT RESIDENT RIGHTS

What Rights Do Consumers Have?



- Confirm whether personal data is being processed and access a copy of their data.
- Correct inaccuracies in their personal data.
- Delete personal data, subject to certain exceptions.
- Obtain a copy of their personal data in a portable and, to the extent technically feasible, readily usable format.
- Opt out of the sale of personal data and processing for targeted advertising.
- Obtain information about categories of third parties to which personal data has been disclosed.
- Obtain information about profiling and the logic involved in such processing.

03

KEY BUSINESS OBLIGATIONS

What Must Covered Organizations Do?



- Provide clear and accessible privacy notices that meet CTDPA requirements.
- Establish and honor consumer-rights request procedures.
- Obtain consent for processing sensitive data, where required.
- Conduct data protection assessments for processing activities that present a heightened risk of harm.
- Use written contracts with processors that include required terms.
- Implement and maintain reasonable administrative, technical, and physical security safeguards.

04

SENSITIVE DATA AND NEW PROTECTIONS

What Additional Requirements Apply?



- Consumer health data requires consent and is subject to additional protections.
- Facial recognition technology is subject to specific notice, consent, and data minimization requirements.
- Precise geolocation data is subject to additional restrictions.
- Controllers must limit the collection, use, and retention of sensitive data to what is adequate, relevant, and reasonably necessary.
- Additional obligations apply to profiling and certain automated decision-making practices.

05

ADDITIONAL COMPLIANCE CONSIDERATIONS

What Else Should Organizations Address?



- Implement and recognize qualifying universal opt-out mechanisms for sales and targeted advertising.
- Evaluate and document high-risk processing activities through data protection assessments.
- Review profiling practices and provide required information to consumers.
- Assess data broker obligations, including registration and deletion request system requirements and associated timelines.
- Maintain data inventories and update policies, procedures, and training.

06

ENFORCEMENT

How is the Law Enforced?



- Enforced by the Connecticut Attorney General.
- No private right of action.
- Violations may result in civil penalties of up to \$5,000 per violation, with higher penalties for intentional violations.
- The Attorney General may seek injunctive relief and other equitable remedies.



Need to Put Connecticut's Privacy Requirements Into Practice?

Explore CLIClaw's Privacy Compliance Solutions for assessments, procedures, checklists, and documentation tools.

[Explore Privacy Compliance Solutions →](#)



General information only; not legal advice.
Practical Solutions. Greater Compliance.

CLIClaw.com | © 2026 CLIClaw LLC
Last reviewed: October 16, 2026

