



CONNECTICUT DATA PRIVACY ACT (CTDPA)

CHECKLIST



USERCENTRICS

Connecticut Data Privacy Act (CTDPA) gives Connecticut residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Original effective date	July 1, 2023
Major amendment (Public Act 25-113 / SB 1295)	Effective July 1, 2026
Retroactive	No

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Controls or processes the personal data of at least 35,000 Connecticut consumers annually (lowered from 100,000 by the 2026 amendment), or
- Controls or processes any volume of Connecticut consumers' sensitive data, with no consumer-count minimum (excluding data processed solely to complete a payment transaction), or
- Offers Connecticut consumers' personal data for sale in any volume, with no consumer-count minimum

The prior 25,000-consumer-plus-revenue trigger no longer applies as written, as sensitive-data processing and data sale now bring a business into scope regardless of volume.

Exemptions include:

- Nonprofit organizations (general CTDPA obligations only, not exempt from Consumer Health Data duties)
- State and local government agencies, and entities contracting with them
- Higher education institutions
- National securities associations
- [GLBA](#)-regulated financial institutions (shifting toward narrower entity-specific exemptions under the 2025 amendments)
- [HIPAA](#)-covered entities and business associates (entity-level, not just data-level)
- [FCRA](#)-regulated data
- FERPA-regulated data

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection:

- Categories of personal data processed by the controller, including sensitive data
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any
- Whether the business collects, uses, or sells personal data to train large language models (LLMs), new as of the 2026 amendment

Rights: Inform website visitors of their privacy rights and how to exercise them.

Language: Keep the privacy policy clear and easy to understand.

These requirements can be managed by using a [Privacy Policy Generator](#) and a [CMP](#) to manage consent choices and create consent records.

3 Disclose Whether Personal Data Is Used to Train Large Language Models

New for 2026: your privacy notice must state whether your business collects, uses, or sells personal data to train large language models, naming the categories of data and any third-party model providers involved.

4 Inform Consumers About Their Rights

Consumers' rights under the amended CTDPA:

- **Right to access:** Inquire and receive confirmation of whether personal data is processed, receive access to it, and know the inferences drawn from it (broadened by the 2026 amendment)

- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data collected about them (with exceptions)
- **Right to data portability:** A copy of personal data in a portable, readily usable format
- **Right to opt out:** Of processing for the purposes of sale, targeted advertising, or profiling, no longer limited to solely automated decisions
- **Right to non-discrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent/guardian if the data subject is a child under 13, per [COPPA](#)
- **Right to restrict use of sensitive personal information:** Limit or refuse collection or use of personal data the law classifies as sensitive

Note: When responding to access requests, do not disclose certain higher-risk identifiers directly (e.g., Social Security numbers, biometric data). Instead, notify the consumer that the data is held, without revealing it.

5 As a Best Practice, Review and Update Your Privacy Policy or Notice Every 12 Months

Review operations and potential legal changes every 12 months. Update the [privacy policy](#) and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible.

Data sold: List all categories of personal information your business has sold in the past 12 months.

6 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Obtain the consumer's affirmative, opt-in consent before processing [sensitive personal data](#), which now includes neural data alongside the existing categories (health, biometric, precise geolocation, and others). Like Alabama, and unlike California's opt-out model, the CTDPA requires consent upfront, not an opt-out mechanism after the fact.

Minors aged 13–17: Targeted advertising and sale of personal data for this age group is prohibited outright, regardless of consent, when a controller has actual knowledge or willfully disregards that the consumer falls in this age range. This is a blanket prohibition, not a consent-based gate — a stricter standard than Alabama’s opt-in approach for the same purposes.

Known children (12 and younger): Obtain verifiable consent from a parent or legal guardian, consistent with COPPA, before processing personal data concerning a known child.

7 Enable and Respond to Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form). Set up a system to enable submission, verification, and tracking of [DSARs](#). If identity cannot reasonably be verified, inform the consumer and explain why, and enable them to rectify. Keep records of all requests and responses for 2 years after the last consumer interaction.

Respond within 45 days from the date the request is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window.

**Falling thresholds, rising enforcement and litigation,
eroding ad revenue. Do you know your risk?**

GET IN TOUCH