The Connecticut Data Privacy Act (CTDPA)

The CTDPA grants Connecticut consumers individual rights and imposes corresponding obligations on covered businesses.

GDPR-like Controller / Processor Distinction

Like the EU GDPR, the CTDPA distinguishes between:

Controllers: Entities that, alone or jointly with others, determine the purpose and means of processing personal data; and

Processors: Entities that process personal data on behalf of a controller. The CTDPA imposes specific obligations and limitations on processors, and it sets forth required contents of controller-processor contracts.

Individual rights

1. **Right to Know / Access.** Confirm whether a controller is processing the consumer's personal data and access that personal data, *unless such confirmation or access would require the Controller to reveal a trade secret* (this exception is not provided under VA or CO law).

2. **Correction:** Correct inaccuracies in the consumer's personal data.

3. **Delete:** Request deletion of the consumer's personal data *provided by*, *or obtained about*, *the consumer*.

4. **Data Portability:** Obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

5. **Opt Out:** Opt out of the processing of the consumer's personal data for purposes of targeted advertising, sale of personal data, or profiling. Unlike CO law, a *Controller is not required to authenticate opt-out requests*.

Controllers' obligations

Notice. Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Notice must include, for example, the purpose of processing, the personal data that controllers share with third parties, if any, and how consumers may exercise their consumer rights.

Data Security. Controllers must establish, implement, and maintain reasonable administrative, technical, and physical practices to protect the confidentiality, integrity, and accessibility of personal data, appropriate to the volume and nature of the data.

Sensitive/Children's Data. Controllers are prohibited from processing sensitive data without obtaining consent. Controllers may only process the personal data of children *under age 13* in accordance with COPPA. Unlike the other state privacy laws, CTDPA requires Controllers to *provide an effective mechanism for a consumer to revoke consent, and to cease processing the data no later than 15 days after receiving such request*.

Nondiscrimination. Controllers may not discriminate against consumers for exercising their rights under the CTDPA, *e.g.*, by denying or charging a different price for a good or service. An exception applies if an offer is related to the consumer's voluntary participation in a loyalty or similar program.

Consumer Appeals. The CTDPA requires controllers to establish a process for a consumer to appeal the controller's refusal to take action on a consumer request.

Data Protection Impact Assessments. The CTDPA requires controllers to perform and document data protection assessments for each of its processing activities that presents a heightened risk of harm, such as targeted advertising, sale, profiling, or the processing of sensitive data.

The Connecticut Data Privacy Act (CTDPA)

Who Must Comply?

The CTDPA applies to entities that conduct business in Connecticut that produce products or services that are targeted to Connecticut consumers, <u>and</u> during the preceding calendar year:

Controlled or processed personal data of at least **100,000 consumers**, *excluding personal data controlled or processed for the purpose of completing a payment transaction* (CT is the first state to include this explicit carve out); <u>or</u>

Controlled or processed the personal data of at least **25,000 consumers** <u>and</u> derived over **25% of gross revenue** from the sale of personal data.

Key Definitions

Consumer: A resident of the state not acting in an employment or commercial context.
- Recognizes employee and "business-to-business" exceptions.

Personal Data: Any information linked or reasonably linkable to an identified or identifiable individual.
- Excludes de-identified data and publicly available information.

Sensitive Data: (i) Personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sex orientation, citizenship, or immigration status; (ii) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (iii) personal data collected from a known child (*i.e.*, under age 13); or (iv) precise geolocation data.

Targeted Advertising: Displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests.
- Excludes, *e.g.*, advertisements based on activities within a controller's own websites or online applications, or the context of a consumer's current search query, visit to a website, or online application.

Key Exceptions

Entities: The CTDPA exempts nonprofits, tribes, institutions of higher education, air carriers, financial institutions subject to Title V of the GLBA, and HIPAA-covered entities and business associates.

Types of Personal Data: The CTDPA exempts personal data created or maintained in the employment context or for purposes of select federal laws, including HIPAA, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and the Driver's Privacy Protection Act.

Permitted Processing: The CTDPA does not restrict a controller or processor's ability to comply with laws or regulations or provide a product or service specifically requested by a consumer, among other purposes.

Enforcement

- **Connecticut AG** has exclusive enforcement authority.
- **No private right of action.**
- From July 1, 2023 through December 31, 2024, businesses have **60-day period** to cure alleged violations, upon receipt of AG notice. (Different cure period than provided under VA and UT privacy law.)
- Beginning January 1, 2025, AG has discretion to grant opportunity to cure.

For more, please visit:
MoFo's CCPA/CPRA Resource Center for additional state privacy law resources. The CTDPA will become **operative on July 1, 2023**.
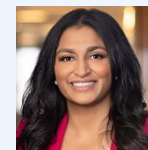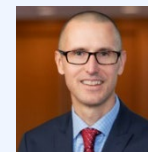
MoFo Contacts

Kristen J. Mathews
Partner, New York
(212) 336-4038
KMathews@mofo.com

Julie O'Neill
Partner, Boston
(617) 648-4731
JONeill@mofo.com

Purvi G. Patel
Partner, Los Angeles
(213) 892-5296
PPatel@mofo.com

Nathan D. Taylor
Partner, Washington, D.C.
(202) 778-1644
NDTaylor@mofo.com

Marian Waldmann Agarwal
Partner, New York
(212) 336-4230
MWaldmann@mofo.com
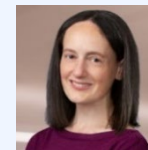
Mary Race
Of Counsel, Palo Alto
(650) 813-5609
MRace@mofo.com
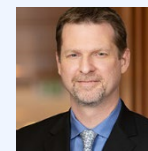
Vincent Schroder
Of Counsel, Palo Alto
(650) 813-4083
VSchroder@mofo.com