

# Ten Percent and Rising: Connecticut Becomes Fifth U.S. State to Enact Privacy Law

Alysa Z. Hutnik, Alexander I. Schneider

May 11, 2022

On Tuesday, Connecticut became the fifth state to pass comprehensive privacy legislation when Governor Ned Lamont signed “[An Act Concerning Personal Data Privacy and Online Monitoring](#)” into law. Connecticut joins California, Virginia, Colorado, and Utah in enacting new privacy laws that take effect in 2023. Out of fifty states in the U.S., ten percent have now passed a comprehensive privacy law.

Effective July 1, 2023, the Connecticut law adopts a general framework of definitions, consumer rights, and compliance obligations based on concepts of data controller and data processor from the EU’s General Data Protection Regulation (GDPR), and the right to opt out of the “sale” of personal data as first articulated in the California Consumer Privacy Act (CCPA). Overall, the Connecticut law mirrors Colorado’s privacy law but then borrows select concepts from the California, Virginia, and Utah laws. The result is a hybrid of the pre-existing state laws, but not a law that introduces significant contradictions or unique compliance challenges.

The following are highlights of the Connecticut law:

- **Applicability.** Consistent with other state laws, Connecticut’s privacy law applies to companies that do business in Connecticut and meet certain thresholds. In order to apply, the company must process personal data of more than 100,000 Connecticut consumers, or process personal data of 25,000 Connecticut consumers but also derive a significant percentage of income from the “sale” of personal data – 25 percent. The law does not apply to non-profits.
- **Federal Law Exemptions.** Similar to other state laws, Connecticut exempts Covered Entities or Business Associates subject to HIPAA and Financial Institutions or data subject to the Gramm-Leach-Bliley Act. The law also exempts certain activities of consumer reporting agencies and furnishers and users of consumer reports where regulated by the Fair Credit Reporting Act.
- **Employee and B2B Exceptions.** Similar to the Colorado, Virginia, and Utah laws, the Connecticut law does not apply to personal data of employees or individuals acting in a commercial context. California’s employee and B2B contact data exemptions are set to sunset at the end of 2022, although legislation is pending to [extend these exemptions](#).
- **Opt-Out of Sale and Targeted Advertising.** The Connecticut law provides a right to opt-out of the sale of personal data. The definition of a “sale” is “the exchange of personal data for monetary or other valuable consideration by the controller to a third party,” which is similar to

the definition in the Colorado privacy law. The Connecticut law also provides for a right to opt-out of processing of personal data for purposes of targeted advertising. Similar to Colorado, “targeted advertising” is defined as “displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer’s activities over time and across nonaffiliated internet web sites or online applications to predict such consumer’s preferences or interests.” The definition excludes targeting advertisements based on activities within a business’s own websites or apps.

- **Consent for Sales and Targeted Advertising Involving Minors:** For minors at least 13 years of age and younger than 16 years of age, a business may not process data for targeted advertising or sell the minor’s data without consent. The minor has a right to revoke consent in a manner that is “at least as easy as the mechanism by which the consumer provided the consumer’s consent.” This provision is similar to the California right to opt-in to the sale or sharing of a minor’s personal information.
- **Consent to Process Sensitive Data.** The Connecticut law requires consent to process sensitive data, similar to the Virginia and Colorado laws. The law defines sensitive data to include data revealing racial or ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sex life, sexual orientation, and citizenship and immigration status; genetic and biometric data that identifies an individual; and precise geolocation data. This definition is similar to the Virginia law; in contrast, the Colorado law does not include precise geolocation data within its definition of “sensitive data.”
- **Children’s Data.** Personal data collected from a known child is considered to be sensitive data. The Connecticut law requires processing this data in accordance with the federal Children’s Online Privacy Protection Act (COPPA).
- **Consumer Rights.** The Connecticut law provides consumers the right to access their personal data in a portable format, delete their personal data, and correct inaccuracies in their personal data.
- **Contract Terms.** The Connecticut law includes a laundry list of terms that must be added to contracts between controllers and processors. These terms, which overlap with contract requirements in the other state privacy laws, include instructions on processing data, duty of confidentiality, deletion at the end of provision of services, requiring a processor to provide evidence of compliance to a controller, the opportunity to object to sub-processors, and controller audit rights.
- **Enforcement and Regulation.** The Connecticut law does not include a private right of action or rulemaking process. There is a 60 day right to cure violations until Jan. 1, 2025. The law is the first to omit an express penalty per violation. Instead, a violation constitutes an unfair trade practice for purposes of Connecticut’s Consumer Protection Law, Section 42-110b. The Consumer Protection Law, in turn, grants the Connecticut Attorney General the right to seek injunctive relief and \$5,000 statutory penalties only for willful misconduct.

The following chart summarizes and compares requirements of the five U.S. state privacy laws (mobile users click [here](#)):

California Privacy Rights Act (CPRA)	Colorado Privacy Act (CPA)	Virginia Consumer Data Protection Act (VCDPA)	Utah Consumer Privacy Act (UCPA)	Connecticut Act Concerning Personal Data Privacy (CPDP)
---	----------------------------------	--	---	--

Effective Date	January 1, 2023	July 1, 2023	January 1, 2023	December 31, 2023	July 1, 2023
Thresholds to Applicability	Conducts business in CA,			Conduct business in Utah or target products or services to Utah residents,	Produce products or services that are targeted to CT residents, and
	Determines the purposes and means of processing personal info. of CA residents, and Meets one of the following thresholds:	Conducts business in CO or targets products or services to CO residents, and Meets either of these thresholds: Processes personal data of > 100K consumers in a year; <u>or</u>	Conducts business in VA or targets products or services to VA residents; and Meets either of these thresholds: Processes personal data of > 100K consumers; <u>or</u>	Have more than \$25 million in annual revenue, and Either: During a calendar year processes personal data of >100K consumers, <u>or</u>	In the preceding year: Process personal data of >100K consumers (excluding payment transaction data), <u>or</u>
Sales	Processes personal data of > 100K consumers or households, <u>or</u> Earns > 50% of annual revenue from selling or sharing personal info. Right to opt-out of the sale of personal information.	Earns revenue or receives a discount from selling personal data and processes personal data of >25K consumers.	Processes personal data of >25K consumers and derives >50% of gross revenue from the sale of personal data.	Process personal data of > 25K consumers and derive > 50% of revenue from the sale of personal data.	Process personal data of > 25K consumers and derive > 25% of revenue from the sale of personal data.
	Opt-in consent required to “sell” personal information of minors under age 16. Right to opt-out of the “sharing” of	Right to opt-out of the sale of personal data.	Right to opt-out of the sale of personal data. The definition of a “sale” requires monetary consideration.	Right to opt-out of the sale of personal data. The definition of a “sale” requires monetary consideration.	Right to opt-out of the sale of personal data. Opt-in consent required to “sell” personal data of minors 13 to 16.

	personal information for purposes of cross-context behavioral advertising.	Right to opt-out of targeted advertising	Right to opt-out of targeted advertising	Right to opt-out of targeted advertising	Right to opt-out of targeted advertising
<b>Targeted Advertising</b>	Opt-in consent required to “share” personal information of minors under age 16.				Opt-in consent required for processing personal data of minors 13 to 16 for targeted advertising.
<b>Global Privacy Control</b>	Yes (optional subject to regulatory process)	Yes, required by July 1, 2024.	No	No	Yes, required by Jan. 1, 2025.
<b>Sensitive Data</b>	Right to limit the use and disclosure of sensitive personal information.	Consent to process sensitive data.	Consent to process sensitive data.	Provide notice and an opportunity to opt out of processing of sensitive data.	Consent to process sensitive data.
<b>Profiling</b>	Pending regulations	Right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.	Right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.	N/A	Right to opt-out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.
<b>Minor &amp; Children’s Data</b>	Opt-in consent required to “sell” or “share” personal information of minors under age 16.	COPPA exception; obtain parental consent to process personal data concerning a known child.	Process sensitive data of a known child in accordance with COPPA.	Process personal data of a known child in accordance with COPPA.	Process sensitive data of a known child in accordance with COPPA. Consent to sell personal data of minors 13 to 16 or process their personal data for targeted advertising.
<b>Consumer</b>	Access, Deletion,	Access, Portability,	Access, Portability,	Access,	Access, Deletion,

<b>Rights</b>	Correction, Portability	Deletion, Correction	Deletion, Correction	Portability, and Deletion	Correction, Portability
<b>Authorized Agents</b>	Permitted for all consumer rights requests	Permitted for opt-out requests	N/A	N/A	Permitted for opt-out requests
<b>Appeals</b>	N/A	Must create process for consumers to appeal refusal to act on consumer rights	Must create process for consumers to appeal refusal to act on consumer rights	N/A	Must create process for consumers to appeal refusal to act on consumer rights
<b>Private Right of Action</b>	Yes, for security breaches involving certain types of sensitive personal information	No	No	No	No
<b>Cure Period</b>	30-day cure period is repealed as of Jan. 1, 2023.	60 days until provision expires on Jan. 1, 2025.	30 days	30 days	60 days until provision expires on Dec. 31, 2024.  Starting Jan. 1, 2025, AG may grant the opportunity to cure.
<b>Data Protection Assessments</b>	Annual cybersecurity audit and risk assessment requirements to be determined through regulations.	Required for targeted advertising, sale, sensitive data, certain profiling.	Required for targeted advertising, sale, sensitive data, certain profiling.	N/A	Requires for targeting advertising, sale, sensitive data, certain profiling.