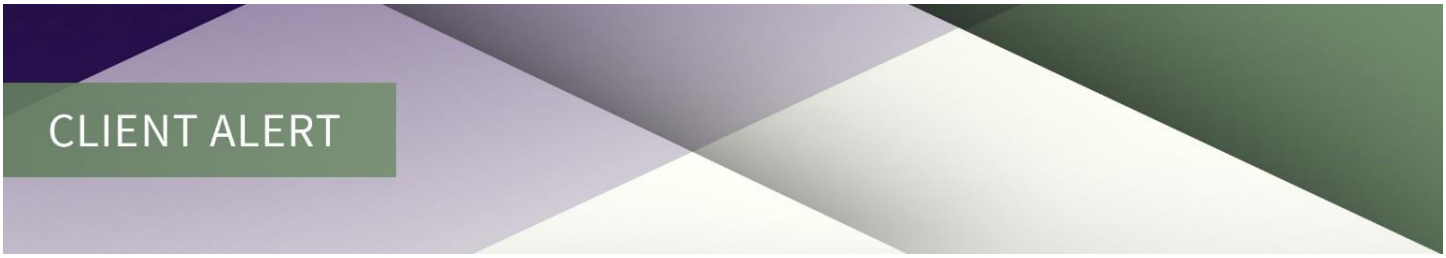

Connecticut Makes Five: A Review of the Newest Comprehensive State Privacy Law

May 11, 2022

AUTHORS

Daniel Alvarez | Laura Jehl | Rick Borden | Stefan Ducich
Samuel Lewis

Connecticut has joined the growing number of U.S. states to enact a comprehensive privacy law, following California, Colorado, Virginia, and Utah. On May 4, 2022, Connecticut enacted An Act Concerning Personal Data Privacy and Online Monitoring (the "Connecticut Privacy Law"), which will come into effect on **July 1, 2023**.[1] While the Connecticut Privacy Law draws heavily on familiar concepts from its predecessor laws, it is more prescriptive on issues relating to the processing of children's data, conducting data protection assessments ("DPAs"), and the implementation of a global opt-out mechanism. Coupled with recently enacted amendments to the Virginia Consumer Data Protection Act ("VCDPA"), the new Connecticut law highlights the dynamic nature of the legal and regulatory landscape on privacy and data security issues in the U.S.

Connecticut Privacy Law – Overview

The Connecticut Privacy Law employs a framework familiar to organizations who may have already had to work on compliance with laws in California, Colorado, Utah, and Virginia. The Connecticut Privacy Law also uses the language of the EU's General Data Protection Regulation ("GDPR")—in particular, "controllers" and "processors"—that has been incorporated into other states' laws to outline the obligations of such entities with respect to processing personal data and guaranteeing Connecticut consumers (i.e., residents of the state) the right to control the use of their data. Like the GDPR,

[1] Substitute Senate Bill No. 6, "An Act Concerning Personal Data Privacy and Online Monitoring" available [here] (last accessed May 11, 2022).

the Connecticut Privacy Law requires controllers to maintain records, in particular with respect to data protection assessments.

Scope

The Connecticut Privacy Law applies to entities doing business in Connecticut—or whose products or services are targeted to Connecticut consumers—and which, in the last year, controlled or processed the personal data of at least:

(1) 100,000 Connecticut consumers; or
(2) 25,000 Connecticut consumers, and derived at least 25% of gross revenue from the sale of personal data.

These thresholds are similar, but not identical, to the other state laws. These differences will unfortunately require organizations to continue to track multiple triggering requirements.

In addition, the Connecticut Privacy Law excludes certain data and entities from its scope. For example, the law expressly does not apply to the processing of employees' data within the employment relationship, and includes broad, entity-wide exclusions for (i) financial institutions subject to the privacy and data security requirements of the Gramm-Leach-Bliley Act, (ii) covered entities and business associates subject to the Health Insurance Portability and Accountability Act; and (iii) nonprofit organizations, among others.

Obligations on Controllers and Processors

Like the other comprehensive U.S. state laws and the GDPR, the Connecticut Privacy Law imposes a number of obligations on covered entities with respect to the collection, processing, and sharing of personal data. For example:

Consent. Controllers must obtain clear, affirmative and unambiguous consent to process personal data and provide a mechanism to withdraw such consent, in cases where the organization is either processing sensitive data or is processing data in ways that are different from the original purpose for collection.

Security. Controllers must implement and maintain reasonable security practices appropriate to the volume and nature of data involved, and provide public notices about the processing of personal data. In addition:

DPAs. Controllers must conduct and document a DPA for all processing that "presents a heightened risk of harm to a consumer."[2] This includes any processing of sensitive data, or processing non-sensitive, personal data for the purpose of (i) targeted advertising; (ii) selling such data; or (iii) profiling (where profiling presents a reasonably foreseeable risk of certain harms). As under other states laws, DPAs are documented, risk-based assessments that weigh the benefits that may flow from processing—to the consumer, controller, and other stakeholders—against risks to the rights of the consumer. The Connecticut Attorney General may compel production of a DPA if such assessment is relevant to an

[2] Connecticut Privacy Law sec. 8.

investigation. However, the DPA would remain confidential and may not be disclosed under the Freedom of Information Act.

Minors' Data. The Connecticut Privacy Law prohibits the processing of personal data of consumers known to be between 13 and 16 years old for the purpose of targeted advertising or the sale of their personal data without the consent of the minor consumer.[3]

Global Opt-Out. Not later than **January 1, 2025**, controllers subject to the Connecticut Privacy Law must make a mechanism available that allows Connecticut consumers to opt out of all processing of their personal data for targeted advertising and data sales by that controller. There are several conditions that attach to this (e.g., no unfair disadvantage to other controllers), but this will likely entail significant technical and operational developments to meet the prescribed requirements. Controllers should feature a clear and conspicuous link to the mechanism on their website.

Processor Contracts. Controllers and processors must enter into contracts that memorialize the nature of the relationship and some of the details related to complying with the law.

Consumers' Rights

Connecticut consumers enjoy certain rights with respect to their data that are similar to those of consumers in California, Colorado, Utah, and Virginia. These include the right to confirm whether their data is processed by a controller, to access, correct, delete and obtain a copy of such personal data, and to opt out of personal data processing for the purposes of: (i) targeted advertising, (ii) the sale of personal data, and (iii) "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."[4] As with the California Consumer Protection Act ("CCPA")/California Privacy Rights Act ("CPRA"), the Connecticut Privacy Law prohibits discrimination against a consumer for exercising these rights.

Enforcement

The Connecticut Privacy Law joins the majority of preexisting state privacy laws by granting the state Attorney General exclusive authority to enforce violations. Unlike CCPA/CPRA, the Connecticut Privacy Law does not provide for a private right of action.

Initially, controllers facing enforcement action under the Connecticut Privacy Law have 60 days following notice from the Attorney General's office to cure the violation. However, the mandatory cure period will expire on **January 1, 2025**, after which the Attorney General may choose whether to allow a controller to cure or to initiate an enforcement action immediately.

[3] The CCPA requires consumers between the ages of 13 and 16 to affirmatively authorize the sale of their data.

[4] The CPA and VCDPA allow consumers to opt out of these types of processing, while the CPRA, CCPA, and the UPA target a narrower range of processing.

Important Dates

July 1, 2023	The Connecticut Privacy Law comes into effect
January 1, 2025	The 60-day cure period for identified deficiencies expires
	Controllers must make the global opt-out mechanism available

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel Alvarez
202 303 1125
dalvarez@willkie.com

Laura Jehl
202 303 1056
ljehl@willkie.com

Rick Borden
212 728 3872
rborden@willkie.com

Stefan Ducich
202 303 1168
sducich@willkie.com

Samuel Lewis
202 303 1175
slewis@willkie.com