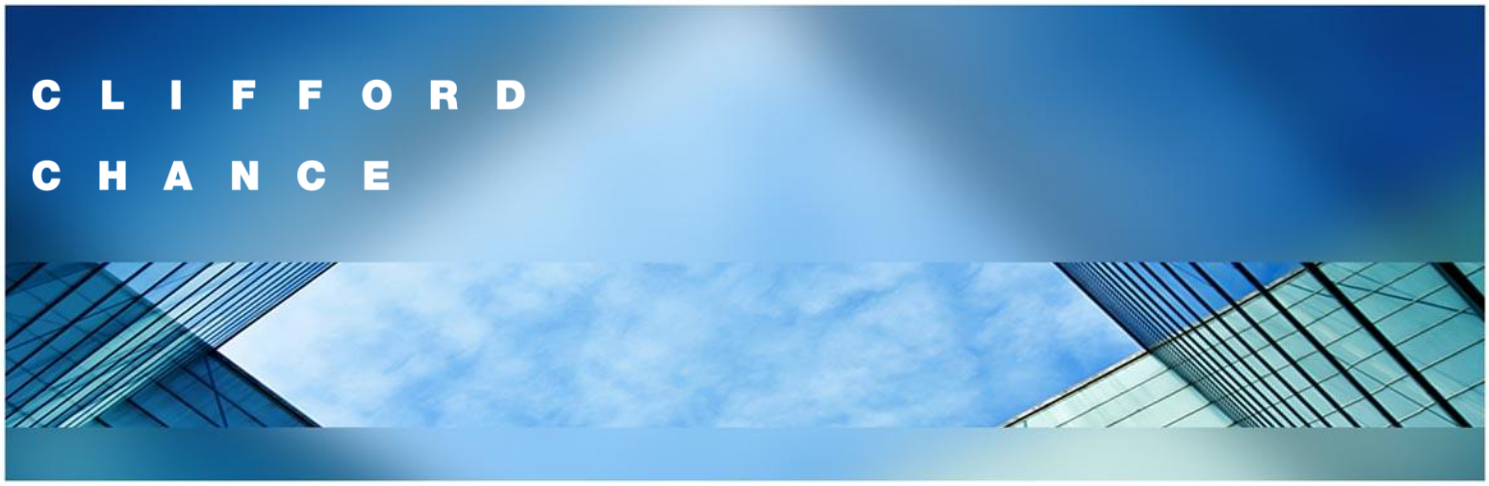

CONNECTICUT DATA PRIVACY ACT BECOMES NATION'S FIFTH STATE PRIVACY LAW, SETTING STRICTER STANDARDS

On May 10, 2022, Connecticut Governor Ned Lamont signed "An Act Concerning Personal Data Privacy and Online Monitoring" into law, making Connecticut the fifth state to pass a comprehensive consumer privacy law. The Act is the latest stitch in the patchwork of state and federal privacy laws that is growing ever more complex. And as has become a trend, while the law shares many similarities with its counterparts in other states, the Act also has certain unique provisions that companies that do business in Connecticut will need to carefully consider before the law goes into effect on July 1, 2023.

Key issues

- Connecticut's Act provides no private right of action but empowers the state Attorney General to bring enforcement actions and to impose fines along with actual and punitive damages.
- There is a right to cure alleged violations, but this is scheduled to sunset in 2025.
- Connecticut joins Colorado in requiring covered entities to recognize global opt-out "preference signals."
- The Act guarantees consumers the right to revoke consent for certain types of processing.
- The Act goes into effect July 1, 2023.

OVERVIEW OF THE ACT

Scope: Which Companies Must Comply

The Act applies to entities that conduct business in Connecticut or that produce products or services targeted to residents of Connecticut, and which:

- Controlled or processed the personal data of at least 100,000 Connecticut consumers within the preceding calendar year, excluding personal data used only to complete a payment transaction; or
- Controlled or processed the personal data of at least 25,000 Connecticut consumers within the preceding calendar year, if the entity derived more than 25% of its gross revenue from the sale of personal data.

The Act applies more broadly than the recent Utah Consumer Privacy Act (UCPA), which limits its application to companies that meet a minimum threshold of *both* their annual revenue and the number of Utah residents whose personal data they process. Connecticut's Act is more in line with California's legislation, the California Privacy Rights Act (CPRA), which applies to business that meet *either* a revenue or resident threshold (though Connecticut establishes higher thresholds).

Like other states, Connecticut does not define what it means to "conduct business" within the state, creating potential uncertainty regarding the law's scope. That said, the law applies not only to companies that do business in Connecticut, but also to businesses targeting Connecticut consumers, meaning that Connecticut's bill would likely capture some companies that do not have a physical presence in Connecticut.

Consumer Rights

Connecticut's Act establishes five main consumer privacy rights:

- The right to confirm whether a company is processing their personal data and to **access** that data;
- The right to **correct inaccuracies** in the consumer's personal data;
- The right to **request deletion** of personal data provided by the consumer or obtained about the consumer;
- The right to **opt-out** of the processing of their personal data for targeted advertising, sale, or for profiling in furtherance of automated decisions producing legal or other significant effects concerning the consumer; and
- The right to **obtain a copy of** their data in a form portable and readily usable, to the extent technically feasible and practicable.

Controllers will be required to establish one or more means for consumers to submit requests to exercise their rights as established by the Act: this could include a clear and conspicuous link on a web page allowing the consumer to actively opt-out of targeted advertising or sales of data, though the Act does not prescribe precise procedures. By January 1, 2025, controllers will also be required to recognize opt-out "preference signals," which could be platform or browser settings indicating a consumer's global preference to opt-out of the sale or use of their data. The requirement to recognize these more passive indicia of consumer intent is a relatively strict privacy requirement: though Colorado's law has a similar requirement, California has no such obligation.

In addition to establishing the right to opt out of certain types of processing, the law also provides consumers with the ability to **revoke their consent** to various types of processing, including the processing of sensitive and other personal data.

Controllers must respond to a consumer's request within 45 days after receipt of the request, though the period can be extended to 90 days when reasonably necessary and after the controller timely informs the consumer of the extension.

Responsibilities of Controllers

The law imposes different obligations for "controllers" and "processors" of personal data. Similar to the EU GDPR, the Act defines "controllers" as individuals or legal entities that, alone or with others, determine the purpose and means of processing personal data. "Processors," for their part, process the personal data on behalf of a controller.

Controllers and processors will need to comply with three broad requirements. The first, they must create reasonable administrative, technical, and physical security practices to protect collected data. Second, such data must be limited

only to that which is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed. Third, consumers must be informed about how their date is being processed in the form of a disclosure. Such disclosure will come in the form of a clear, accessible, and meaningful privacy notice which indicates:

- The categories of personal data processed by the controller;
- The purpose for processing the personal data;
- How consumers may exercise their rights and appeal controllers' decisions;
- The categories of personal data shared with third parties;
- The categories of third parties with which the controller shares personal data; and
- An email address or other online process through which the consumer may contact the controller.

Controllers which sell personal data to third parties or process personal data for targeted advertising must clearly disclose such sales to consumers, as well as the means through which consumers can opt-out of such processing. The law defines the **sale** of personal data as the exchange of personal data for monetary or other valuable consideration. This definition is among the broader formulations of "sale" that states have adopted in their privacy laws, including exchanges for "valuable consideration"—a somewhat ambiguous term that will likely be subject to interpretation.

Sensitive Data

Sensitive data within the Act is data that:

- Reveals racial or ethnic origin, religious belief, mental or physical health conditions or diagnoses, sex life or orientation status, or citizenship or immigration status;
- Is biometric or genetic data processed for the purpose of uniquely identifying an individual;
- Is collected from a known child (defined as individuals under 13 years of age but with other restrictions on those up to 16 years of age); or
- Contains precise geolocation information.

Sensitive data may not be processed without the consumer's consent or, in the case of known children, must be handled in accordance with the Children's Online Privacy Protection Rule (COPPA).

Like most other state privacy laws, Connecticut requires controllers and processors to engage in **assessments** for various processing activities. Specifically, such assessments must capture collection processes that "present a heightened risk of harm" to consumers, including personal data used for targeted advertising, the sale of personal data, the processing of sensitive data, or the processing of data for the purpose of profiling where the profiling could result in certain foreseeable risks to consumers.

Processors are required to allow and cooperate with controllers' reasonable assessments.

Exemptions: What Data is Not Covered

There are several significant exemptions to the types of data covered by the law. For example, the Act:

- does not apply to personal data already protected by other laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act;
- provides carve-outs for certain types of data used by credit and consumer reporting agencies; and
- does not apply to several broad categories of entities, including institutions of higher education, nonprofits, and certain government entities.

The law also explicitly protects companies from being compelled to disclose trade secrets.

Enforcement and Penalties

Connecticut's law will be enforced by the state Attorney General. The Act creates **no private right of action**.

One of the more notable features of the law is the law's limited cure provision. Initially, the law provides companies with the right to cure violations *if the Attorney General determines that a cure is possible*. In such instances, the AG will send companies a notice of noncompliance, after which controllers will have 60 days to cure the violation before the Attorney General may bring an enforcement action.

This right to cure will be more limited beginning in 2025. Starting January 1, 2025, the Attorney General will have discretion to offer the opportunity to cure alleged violations. The AG will make this determination not based on whether a cure is possible, but instead based on consideration of a number of factors including the number of violations, the size and complexity of the processing entity, and the likelihood of injury to the public.

Violations of the act will constitute unfair trade practices under Connecticut general statutes 42-110b and will be subject to a civil penalties, plus actual and punitive damages.

CONCLUSION

Though Connecticut's new law hews closely to the template created by other state consumer privacy laws, there are certain unique provisions of the law that create additional compliance burdens for covered entities. From its comprehensive opt-out scheme, including the need to recognize global preference signals, to its codification of the right for consumers to revoke their consent to certain types of processing, Connecticut's law underscores the need for controllers and processors—especially those that are subject to several different state regimes—to maintain comprehensive privacy compliance programs that take into account the increasingly-complicated web of overlapping U.S. domestic legislation.

CLIFFORD
CHANCE

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Thomas Chapman
Associate

T +1 202 912 5921
E thomas.chapman
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP