Connecticut Legislature Passes Comprehensive Privacy Legislation, Awaiting Governor's Signature

05.04.22

On April 28, the Connecticut House passed Senate Bill 6, an act concerning personal data privacy and online monitoring (SB 6 or Connecticut Act). The Senate unanimously passed SB 6 on April 20, and is now currently under consideration by Governor Ned Lamont. If the bill becomes law, it will go into effect on July 1, 2023, making Connecticut the fifth state to enact a comprehensive data privacy law.

Who Must Comply?

The Connecticut Act would apply primarily to "controllers" and "processors."

SB 6 defines a "controller" as any "individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data." Under the Connecticut Act, a "processor" means an individual who, or legal entity that, processes personal data on behalf of a controller.

SB 6 would apply to individuals or entities that (1) conduct business in Connecticut and (2) control or process personal data during the preceding year of at least either:

- 100,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction, or
- 25,000 consumers who derived more than 25% of their gross revenue from selling personal data.

What Is Protected?

The Connecticut Act protects "personal data" and "sensitive data."

"Personal data" means any information linked or reasonably linked to an identified or identifiable individual. The definition does not include de-identified data or publicly available information.

"Sensitive data" means personal data that includes (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; (2) the processing of genetic or biometric data for the purpose of uniquely identifying any individual; (3) personal data collected from a known child; or (4) precise geolocation data.

Exempted Data

Various information is exempted under the Connecticut Act, including, information collected under the Health Information Portability and Accountability Act (HIPAA), information bearing on a consumer's credit worthiness to the extent such activity is regulated by and authorized under the Fair Credit Reporting Act (FCRA), and financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA).

Information controlled or processed solely for the purpose of completing a payment transaction is exempted, which is an exemption that differs from other state laws.

Key Definitions

"Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. It does not include (1) disclosure of personal data to a processor that processes the personal data on behalf of the controller; (2) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (3) the disclosure or transfer of personal data to an affiliate of the controller; (4) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; (5) the disclosure of personal data that the consumer (a) intentionally made available to the general public via a channel of mass media and (b) did not restrict to a specific audience; or (6) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Targeted advertising" means 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 services or online applications to predict such consumer's preferences or interests. It does not include (1) advertisements based on activities within a controller's own internet websites or online applications; (2) advertisements based on the context of a consumer's current search query, visit to an internet website, or online application; (c) advertisement based on a consumer's request for information or feedback; or (d) processing personal data solely to measure or report advertising frequency, performance, or reach.

What Rights Are Granted to Consumers?

The Connecticut Act grants consumers a number of rights, including, among others: (1) the right to confirm whether or not a controller is processing the consumer's personal data and the right to access their personal data; (2) the right to correct inaccuracies in the consumer's personal data; (3) the right to delete the personal data; (4) the right to obtain a copy of the consumer's personal data that is portable and easily transferrable; and (5) the right to opt out of the process of personal data for (a) targeted advertising, (b) the sale of personal data, or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

What Obligations Apply to Controllers?

- **Data Minimization.** A controller shall "limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed."
- **Duty to Avoid Secondary Use.** A controller shall "not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent."
- **Security Practices.** A controller shall "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue."

- **Consent.** A controller shall "not process sensitive data concerning a consumer without first obtaining the consumer's consent, or in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA." A controller also must provide an effective mechanism for a consumer to revoke consent.

- **Discrimination.** A controller must "not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers." A controller also shall not discriminate against a consumer for exercising any of his/her rights under the Connecticut Act.

- **Data Protection Assessments.** A controller shall "conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer," which includes any processing of personal data for the purposes of targeted advertising, the sale of personal information, or profiling.

- **Privacy Notices.** A controller shall "provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) The categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active electronic mail address that the consumer may use to contact the controller."

What Obligations Apply to Processors?

- **Data Processing Agreements.** A processor must be governed by a contract that must "set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties."

- **Data Subject Request.** A processor have processes "taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests."

- **Duty of Care.** A processor shall assist "the controller in meeting the controller's obligation in relation to the security of processing the personal data and in relation to the notification of a breach of security."

- **Data Protection Assessments.** A processor shall provide the necessary information to "enable the controller to conduct and document data protection assessments."

- **Confidentiality.** A processor must ensure "that each person processing personal data is subject to a duty of confidentiality with respect to the data."

- **Subcontractors.** A processor must "engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data."

Who Can Enforce the Connecticut Act?

The Connecticut Act does not create a private right of action. The Connecticut attorney general shall have exclusive authority to enforce violations of the Connecticut Act. Prior to any such enforcement action, the attorney general shall provide a 60-day notice to allow the business the opportunity to cure any alleged violations. This notice to cure provision will sunset on December 31, 2024.

What's Next?

If signed by the governor (which is expected to occur), SB 6 will become law. If the governor vetoes the bill, it will be returned to the Senate to be reconsidered. If the governor fails to act within five days during legislative session or 15 days after adjournment from the day it was presented, it will become law automatically. If it becomes law, Connecticut will be the fifth state to adopt a comprehensive privacy law following California, Virginia, Colorado, and Utah.