Privacy Alert

May 2022

Connecticut Passes Consumer Data Privacy Law

Senate Bill 6, known as Public Act No. 22-15 and "An Act Concerning Personal Data Privacy and Online Monitoring," was signed into law by Gov. Ned Lamont on May 12.

The law will largely take effect on July 1, 2023, with additional obligations to recognize a universal opt-out becoming effective on Jan. 1, 2025. The law does not contemplate additional regulations.

Key Takeaways

- The scope, obligations and consumer rights largely reflect the requirements found in the existing state laws.
- The act includes a right to cure, which will sunset on Dec. 31, 2024.
- The law reflects the broad definition of "sale" found in the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA), and reflects the opt-in requirements for sensitive personal information found in Colorado's and Virginia's laws.

A Deeper Dive

The law establishes a framework for businesses in the state that control and process personal data and sets out privacy protection standards and responsibilities for data controllers and processors.

The law also grants consumers the right to:

- Access, correct, delete and obtain a copy of their personal data.
- Opt out of the processing of their personal data for certain purposes, including targeted advertising and some sales of personal data.

Connecticut joins the four states—California, Colorado, Virginia and Utah—that have already enacted comprehensive consumer data privacy laws.

Here are some frequently asked questions about the impact of the law:

How is 'personal data' defined and what does the definition exclude?

A consumer's "personal data" is any information that is linked or reasonably linkable to an identified or identifiable individual. Personal data does not include publicly available information or de-identified data, which is defined as data that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable individual or a device linked to that individual.

Also excluded from the definition of personal data is health information protected by the Health Insurance Portability and Accountability Act (HIPAA) and certain personal information regulated by the Fair Credit Reporting Act and the Family Educational Rights and Privacy Act, among other laws.

Attorney Advertising

Who does the law apply to?

The law applies to entities that conduct business in Connecticut, produce products or services targeted to state residents, and during the preceding calendar year met one of the following criteria:

- Controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.
- Controlled or processed the personal data of at least 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

Unlike other state privacy laws, the Connecticut law does not include gross revenue thresholds.

The law does not apply to certain entities, including:

- State authorities, including boards, commissions and agencies.
- Nonprofit organizations.
- Higher education institutions.
- National securities associations registered under the Securities Exchange Act.
- Financial institutions or data subject to Title V of the Gramm-Leach-Bliley Act, which requires the Federal Trade Commission and federal banking agencies to issue regulations ensuring financial institutions protect the privacy of consumers' personal financial information.
- Certain entities subject to HIPAA

The law also excludes data collection in the business-to-business and employee contexts. While there is no business-to-business or employee exemption like we've seen with the CCPA/CPRA, the Connecticut law defines a "consumer" as a state resident and specifically states that a "consumer" does not include an individual acting (1) in a commercial or employment context or (2) as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the data controller occur solely within the context of that individual's role with the entity.

What are a data controller's responsibilities under this law?

A data controller—defined as an individual or entity that, either alone or jointly, decides why and how consumers' personal data is processed—would be required to:

- **Minimize data**—Limit the collection of personal data to what is "adequate, relevant and reasonably necessary" for the reasons why such data is being processed.
- **Limit the purpose**—Avoid processing personal data for purposes that are not reasonably necessary or compatible with why such personal data is being processed, unless the data controller obtains the consumer's consent.

Businesses must also provide an effective mechanism for a consumer to revoke their consent to having their personal data processed that is at least as easy as the mechanism by which the consumer initially provided consent.

- **Reasonable security controls**—Establish, implement and maintain appropriate reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of consumers' personal data.
- **Opt-in consent required for sensitive data**—Obtain a consumer's consent to process their sensitive data, defined as data that reveals a consumer's racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship status, or immigration status; genetic or biometric data processed for the purpose of uniquely identifying an individual; personal data knowingly collected from a child; or precise geolocation data.
- **Protections for children's data**—Process sensitive data concerning a known child in accordance with the Children's Online Privacy Protection Act (COPPA). Avoid processing a consumer's personal data for targeted advertising or selling the consumer's personal data without their consent when a data controller has actual knowledge—and willfully disregards—that the consumer is at least 13 but under 16 years old.
- **No discrimination**—Avoid discriminating against a consumer for exercising any of their rights under

the law, which includes denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

What rights does this law give consumers regarding their personal data?

The law gives consumers, or a person designated to serve as the consumer's authorized agent, the right to:

- Confirm whether a data controller is processing their personal data.
- Access their personal data, unless such confirmation or access would require the data controller to reveal a trade secret.
- Correct errors in their personal data.
- Delete personal data provided by or obtained about the consumer.
- Obtain a copy of their personal data processed by the data controller in a portable and, to the extent technically feasible, readily usable format.
- Opt out of the processing of their personal data for purposes of targeted advertising, the sale of their personal data with certain exceptions, or profiling to further automated decisions that "produce legal or similarly significant effects concerning the consumer," which include the provision or denial of financial or lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to essential goods or services.

What obligations does a data controller have regarding a consumer's personal data requests?

A data controller must comply with a consumer's request to exercise their rights under this law by:

- Responding to the consumer's request within 45 days of receiving it. The data controller may extend the response period by 45 additional days when reasonably necessary, based on the complexity and number of the consumer's requests. The data controller must inform the consumer of any such extension within the first 45-day response period and give the reason for the extension.
- Informing the consumer within 45 days if the data controller declines the consumer's request. The data controller must also provide its justification for declining to take action and instructions on how to appeal the decision.
- Providing information in response to a consumer request free of charge, once per consumer, during any 12-month period. If a consumer's requests are unfounded, excessive or repetitive, the data controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The law requires that the data controller bear the burden of demonstrating the unfounded, excessive or repetitive nature of the request.

Does the law specify how a data controller should notify consumers about its privacy practices?

Yes. A data controller would have to provide consumers with a "reasonably accessible, clear and meaningful" privacy notice that includes the following:

- Categories of personal data being processed.
- Purpose for processing personal data.
- How consumers may exercise their consumer rights, including how to appeal a data controller's decision about a consumer's request.
- Categories of personal data that the data controller shares with third parties, if any.
- Categories of third parties, if any, with which the data controller shares personal data.
- Contact information for the data controller in the form of an active email address or another online mechanism.
- Description of one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under the law that takes into account how consumers normally interact with the data controller and the data controller's need to verify the identity of the consumer making the request.

The law requires a data controller to conduct a data protection assessment. What does that involve?

A data controller would be mandated to conduct a data protection assessment for each of its processing activities that presents a "heightened risk of harm" to a consumer. According to the law, activities that present a heightened risk of harm to a consumer are processing personal data for targeted advertising, selling personal data, processing sensitive data and processing personal data for profiling that presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.
- Financial, physical or reputational injury to consumers.
- Physical or other intrusion upon the "solitude or seclusion, or the private affairs or concerns," of consumers, where such intrusion would be offensive to a reasonable person.
- Other substantial injuries to consumers.

What must a data protection assessment address?

A data protection assessment must identify the benefits that may flow—both directly and indirectly—from the processing of consumer data to the controller, the consumer, other stakeholders and the public. A data protection assessment must weigh those benefits against the potential risks to consumer rights associated with such processing. Then it must address whether such risks can be mitigated and how.

Additional factors that must be considered by the data protection assessment include whether the data controller uses de-identified data, consumers' reasonable expectations, and the relationship between the data controller and the consumer whose personal data is processed.

Finally, data controllers should be aware that the Connecticut attorney general may require a data controller to disclose any data protection assessment that is relevant to an investigation conducted by the state. Data protection assessments shall remain confidential and exempt from disclosure under the Freedom of Information Act, however.

What is 'de-identified data,' and what are a data controller's obligations regarding this data?

"De-identified data" is defined by the law as data that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable individual or a device linked to that individual.

Data controllers that possess de-identified data must take reasonable measures to ensure that such data cannot be associated with an individual; publicly commit to processing such data only in a "de-identified fashion" and not attempt to re-identify such data; and contractually obligate any recipients of de-identified data to do the same.

Can consumers sue a business under this law?

No. The law does not contain a private right of action.

The state Attorney General has exclusive authority to enforce violations of this law. Between July 1, 2023, and Dec. 31, 2024, before initiating any action for a violation, the attorney general will issue a notice of violation to the data controller if the Attorney General deems that a cure is possible. If the data controller fails to cure the violation within 60 days, the Attorney General may bring an action against the data controller.

By Feb. 1, 2024, the Attorney General will submit a report to a joint standing committee of the General Assembly formed to study issues related to the new law. The report will disclose the number of notices of violation issued, the nature of each violation and the number of violations that were cured during the 60-day cure period.

Starting on Jan. 1, 2025, the Attorney General may, in determining whether to grant a data controller or processor the opportunity to cure an alleged violation of the law, consider the following factors:

- Number of violations committed.
- Size and complexity of the data controller or processor.
- Nature and extent of the data controller's or processor's processing activities.
- Substantial likelihood of injury to the public.
- Safety of individuals or property.
- Whether an alleged violation was likely caused by human or technical error.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Susan E. Israel . . . . . sisrael@loeb.com
Robyn Mohr . . . . . rmohr@loeb.com

6987 REV1 05-18-2022