Published on *The National Law Review* https://natlawreview.com

New Hampshire Passes Comprehensive Consumer Data Privacy Law

Article By:

Jason C. Gavejian

Joseph J. Lazzarotti

On March 6, 2024, New Hampshire's Governor signed Senate Bill 255, which establishes a consumer data privacy law for the state. The Granite State joins the myriad of state consumer data privacy laws. It is the second state in 2024 to pass a privacy law, following New Jersey. The law shall take effect **January 1, 2025.**

To whom does the law apply?

The law applies to persons who conduct business in the state or persons who produce products or services targeted to residents of the state that during a year period:

- Controlled or processed the personal data of not less than 35,000 unique consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or,
- Controlled or processed the personal data of not less than 10,000 unique consumers and derived more than 25 percent of their gross revenue from the sale of personal data.

The law excludes certain entities such as non-profit organizations, entities subject to the Gramm-Leach-Bliley Act, and covered entities and business associates under HIPAA.

Who is protected by the law?

The law protects consumers defined as a resident of New Hampshire. However, it does not include an individual acting in a commercial or employment context.

What data is protected by the law?

The law protects personal data defined as any information linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information. Other exempt categories of data include without limitation personal data collected under the Family Educational Rights and Privacy Act (FERPA), protected health information

under HIPAA, and several other categories of health information.

What are the rights of consumers?

Consumers have the right under the law to:

- Confirm whether or not a controller is processing the consumer's personal data and accessing such personal data
- Correct inaccuracies in the consumer's personal data
- Delete personal data provided by, or obtained about, the consumer
- Obtain a copy of the consumer's personal data processed by the controller
- Opt-out of the processing of the personal data for purposes of target advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Although subject to some exceptions, a "sale" of personal data under the New Hampshire law includes the exchange of personal data for monetary or other valuable consideration by the controller to a third party, language similar to the California Consumer Privacy Act (CCPA).

When consumers seek to exercise these rights, controllers shall respond without undue delay, but no later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary. A controller must establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of the decision. As with the CCPA, controllers generally may authenticate a request to exercise these rights and are not required to comply with the request if they cannot authenticate, provided they notify the requesting party.

What obligations do controllers have?

Controllers have several obligations under the New Hampshire law. A significant obligation is the requirement to provide a "reasonably accessible, clear and meaningful privacy notice" that meets standards established by the secretary of state and that includes the following content:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;
- The categories of personal data that the controller shares with third parties, if any;
- The categories of third parties, if any, with which the controller shares personal data; and
- An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

This means that the controller needs to do some due diligence in advance of preparing the notice to understand the nature of the personal information it collects, processes, and maintains.

Controllers also must:

- 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, as disclosed to the consumer. As with other state data privacy laws, this means that controllers must give some thought to what they are collecting and whether they need to collect it;

- 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;
- 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. What is interesting about this requirement, which exists in several other privacy laws, is that this security requirement applies beyond more sensitive personal information, such as social security numbers, financial account numbers, health information, etc.;
- Not process sensitive data concerning a consumer without 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. Sensitive data means personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or, precise geolocation data;
- Not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;
- Provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and
- Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and willfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age.
- Not discriminate against a consumer for exercising any of the consumer rights contained in the New Hampshire law, including 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.

In some cases, such as when a controller processes sensitive personal information as discussed above or for purposes of profiling, it must conduct and document a data protection assessment for those activities. Such assessments are required for the processing of data that presents a heightened risk of harm to a consumer.

Are controllers required to have agreements with processors?

As with the CCPA and other comprehensive data privacy laws, the law appears to require that a contract between a controller and a processor govern the processor's data processing procedures with respect to processing performed on behalf of the controller.

Among other things, the contract must require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations

in this chapter;
- After providing the controller an opportunity to object, 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; and
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under the law, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

Other provisions might be appropriate in an agreement between a controller and a processor, such as terms addressing responsibility in the event of a data breach and specific record retention obligations.

How is the law enforced?

The attorney general shall have sole and exclusive authority to enforce a violation of the statute.

National Law Review, Volume XIV, Number 67