New Hampshire Comprehensive Privacy Bill Signed into Law

On March 6, New Hampshire joined the growing list of states that have enacted a comprehensive consumer privacy statute when Governor Chris Sununu signed into law Senate Bill 255 (the Act). Generally, the Act follows the privacy laws enacted by other states, so businesses that are compliant with those laws should not find it difficult to comply with the Act's obligations. The Act will take effect on **January 1, 2025**.

Applicability Thresholds and Exemptions

The Act applies to any person who conducts business in the State of New Hampshire or produces products or services that are targeted to residents of the state and, during a one year period, controlled or processed the personal data of either of the following:

- At least 35,000 unique consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction).
- At least 10,000 unique consumers and derived more than 25% of its gross revenue from the sale of personal data.

It is notable that the 35,000 consumer threshold is lower than those generally found under other state laws. A similar, lower threshold is found under Delaware's privacy law, and presumably, the lower thresholds for these states are based on their smaller populations.

The Act contains the typical exemptions seen in other states' laws, including entity exemptions for nonprofit organizations, Gramm–Leach–Bliley Act (GLBA) financial institutions (both entity and data level), institutions of higher education, and HIPAA-covered entities and business associates. The Act also contains data level exemptions generally seen in other states' laws, including PHI, as well as data controlled or processed in compliance with the Family Education Rights and Privacy Act, the Farm Credit Act, the Fair Credit Reporting Act, or the Driver's Privacy Protection Act. Like other privacy statutes, the Act does not cover personal data relating to employment or contracted services.

Consumer Rights and Controller Obligations

In alignment with the privacy frameworks of other states, the Act provides consumers with a standard set of rights with respect to their personal data held by "Controllers" – defined as individuals or entities who determine the purposes and means of processing personal data. Consumers under the Act have the right to do the following:

- Confirm whether 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 in a portable and readily usable format that allows the consumer to easily transmit the data to another controller.
- Opt out of the processing of personal data for targeted advertising, the sale of personal data,

or profiling "in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."

Additionally, the Act provides consumers with the ability to transfer their respective "opt out rights" to another person as an "authorized agent". This is intended to include browser settings, internet links, and other technologies by which individuals can designate an agent. The authorized agent can act on the consumer's behalf to opt out of the processing of the consumer's personal data. Interestingly, it is not explicit that an individual can designate an agent to make other requests (e.g., for deletion or a copy of the individual's personal data), as individuals can in other states.

As is typical with recent privacy laws, the Act requires Controllers to recognize universal opt-out mechanisms (UOOMs) used by consumers to opt out of the sale of their personal data or the use of such data for targeted advertising. Unlike other privacy laws, which set a later date by which controllers must recognize UOOMs, the Act requires Controllers to recognize UOOMs no later than January 1, 2025 – the Act's effective date.

Privacy Notice

Controllers under the Act must provide consumers with a "privacy notice" that is reasonably accessible, clear, and meaningful. The notice must include all of the following:

- The categories of personal data processed.
- The purpose(s) for such processing.
- The way in which a consumer can exercise their rights and appeal a decision made by a Controller with regard to the consumer's request.
- The categories of personal data that the Controller shares with third parties.
- The categories of third parties to whom the Controller shares personal data.
- An email address or other online mechanism through which consumers can contact the Controller.

These components are similar to other state privacy laws, so Controllers that are already complying with the law of another state should find it relatively simple to make any updates needed to comply with the Act.

Consent for Processing of Sensitive Data

The Act includes a broad definition of "sensitive data," including genetic or biometric data, precise geolocation data, and the personal data of a known child. While this definition does not include transgender or nonbinary status as found in other recent privacy laws, the Act's generally broad definition continues to demonstrate a trend toward a more encompassing definition for sensitive data. Controllers are not permitted to process sensitive data under the Act without first obtaining the consumer's consent. If the consumer is a known child, the Controllers must process such data in accordance with the Children's Online Privacy Protection Rule (COPPA). As we have noted elsewhere, this exemption can be confusing, as it exempts businesses that comply with COPPA, but in many cases, COPPA does not apply to much of the processing of children's data by companies. The statute is not clear whether processing children's data not subject to COPPA meets this exemption.

Data Protection Assessments

The Act requires Controllers to conduct data protection assessments (DPAs) for processing that

presents a "heightened risk of harm to a consumer." Examples of "heightened risk" under the statute include processing sensitive data and the sale of personal data. The Act's DPA requirements apply to processing activities created or generated after July 1, 2024, and are not retroactive. The language of these requirements mirrors other states, including a close match to Delaware's privacy law, however, Delaware's DPA requirements apply to processing activities created or generated six months *after* that law's effective date. The most straightforward reading of the statute is that any processing use cases that begin on or after July of this year must be subject to a DPA. Activities before that time do not require a retroactive DPA. Businesses not already conducting DPAs for relevant data (e.g., for New Hampshire-specific use cases) should plan to have DPAs in place on or before the effective date of the Act.

Children's Data

Under the Act, and typical among recent privacy laws, Controllers may not process personal data for purposes of targeted advertising and may not sell personal data without the consumer's consent if the Controller knows, or willfully disregards, that the consumer is between the ages of 13 and 16. As noted above, Controllers are not permitted to process the sensitive data of any known child unless in accordance with COPPA, though what constitutes compliance with COPPA can be difficult to determine in some contexts.

Enforcement

The Act does not contain a private right of action, and the New Hampshire Attorney General's office has sole enforcement authority. The Act includes a right to cure violations (if capable of cure) which right sunsets on December 31, 2025. Controllers will have 60 days to cure the violation if a cure is possible. This aligns with the cure periods of other states, which range from 30 to 90 days.

Important Dates

- **January 1, 2025**: The Act goes into effect, and Controllers must recognize UUOMs.
- **December 31, 2025**: The right to cure sunsets.

Our team will continue to monitor the Act. If you have any questions about the Act or other state privacy laws and how they could affect your business, please contact the authors.