New Hampshire Data Privacy Law (S.255) Summary

On March 6, 2024, Governor Chris Sununu (R) signed S. 255, which relates to the expectation of data privacy, into law. The law will become effective on January 1, 2025. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	Applies to persons that conduct business in New Hampshireor persons that produce products or services that are targeted to residents of New Hampshire that during a one year period: (a) 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 (b) 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.
Covered Data	***"Personal data":*** any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information. ***"Sensitive Data"***: 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. "***Biometric data"****:* data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns, or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; hovering over, muting, pausing or closing a given piece of content; or, an agreement obtained through the use of deceptive design patterns (also known as "dark patterns")." ***"Dark Pattern":*** "means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern"." ***"De-Identified Data"***: "means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data takes reasonable measures to ensure that such data cannot be associated with an individual; publicly commits to process such data only in a de-identified way and not attempt to re-identify such data; and, contractually obligates any recipients of such data to satisfy the criteria under this paragraph." ***"Publicly available information":*** "means information that is lawfully made available through federal, state, municipal government records, or widely distributed media, and a controller has a reasonable basis to believe a consumer has lawfully made available to the general public." ***"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 websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include:(a) advertisements based on activities within a controller's own Internet websites or online applications; (b) advertisements based on the context of a consumer's current search query, visit to an Internet website, or online application;(c) advertisements directed to a consumer in response to the consumer's request for information or feedback; or, (d) processing personal data solely to measure or report advertising frequency, performance, or reach." ***"Sale of personal data":*** the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include: (a) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) 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; (e) the disclosure of personal data that the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience; or, (f) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets."
Consumer Rights	**Access:** A consumer shall have the right to "confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret". **Correction:** A consumer shall have the right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data". **Deletion**: A consumer shall have the right to "delete personal data provided by, or obtained about, the consumer". **Portability:** A consumer shall have the right to "obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret". **Opt Out Rights**: A consumer shall have the right to "opt-out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, except as provided in RSA 507-H:6, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer." **Opt-In Rights for Users between 13-15**: Controllers shall 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 wilfully disregards, that the consumer is at least 13 years of age but younger than 16 years of age."

Business Obligations	**Data Collection**: 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, as disclosed to the consumer; (b) Except as otherwise provided in this chapter, 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". **Responding to Consumer Requests**: "A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period and of the reason for the extension." **Data Security**: "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". **No Unlawful Discrimination:** "A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, 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. **Recognizing Opt-Out Signals: " Not later than January 1, 2025, allowing a consumer to opt-out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt-out of any such processing or sale." Any approval mechanism must adhere to five requirements outlined in the 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. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (a) The processing of personal data for the purposes of targeted advertising; (b) The sale of personal data; (c) The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, consumers, financial, physical or reputational injury to consumers, a 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, or other substantial injury to consumers; and (d) The processing of sensitive data." ***Sharing Data Protection Assessments with the Attorney General:*** "The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. Data protection assessments shall be confidential and shall be exempt from disclosure under RSA 91-A. To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection."

Controller / Processor Distinction	***"Controller"*:** an individual who, or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data. ***"Processor"*:** an individual who, or legal entity that processes personal data on behalf of a controller.
Exceptions and Exemptions	The law does not apply to: • Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; • Nonprofit organizations; • Institutions of higher education; • National securities association that is registered under 15 U.S.C. section 78o-3 of the Securities Exchange Act of 1934, as amended; • Financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq.; or, • A covered entity or business associate, as defined in 45 C.F.R. 160.103.(b). II. The following information and data shall be exempt from this chapter: • Protected health information under HIPAA; • Patient-identifying information for purposes of 42 U.S.C. section 290dd-2; • Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. 46; • Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use. • The protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards set forth in this chapter, or other research conducted in accordance with applicable law; • Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq.; • Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq., as amended; • Information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; • Information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 U.S.C. 290dd-2, as amended; • Information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; • The collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.; • Personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended; • Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq., as amended;

	• Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. 2001 et seq., as amended; • Data processed or maintained in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; as the emergency contact information of an individual under this chapter used for emergency contact purposes; or, that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under HIPPA and used for the purposes of administering such benefits; • Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq., as amended, by an air carrier subject to the act, to the extent this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. 41713, as amended; • Personal information maintained or used for purposes of compliance with the regulation of listed chemicals under the federal Controlled Substances Act, 21 U.S.C. section 830; and • Information included in a limited data set as described at 45 C.F.R. 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified at 45 C.F.R. 164.514(e).”
Enforcement	The Attorney General has sole enforcement authority over the Act. **Cure Period:** “During the period beginning January 1, 2025 and ending December 31, 2025, the attorney general shall, and following said period the attorney general may, prior to initiating any action for a violation under this chapter, issue a notice of violation to the controller if the attorney general determines that a cure is possible. If the controller fails to cure such violation within 60 days of receipt of the notice of violation, the attorney general may bring an action pursuant to this section.”
Rulemaking Authority	The Secretary of State has limited rulemaking authority to (1) provide the standards for privacy notices and (2) establish “secure and reliable means” for consumers to exercise their rights.