SQUIRE PATTON BOGGS

New Jersey and New Hampshire Pass Consumer Privacy Laws – and 11 Other States Are Considering Similar Laws

US – January 2024

The first month of 2024 brought two new state privacy laws. On January 18, the New Hampshire legislature passed the 15th US state consumer privacy law (notably, still subject to some procedural requirements and signature by Governor Chris Sununu before it is officially law).

The New Hampshire law was passed a few days after New Jersey's new consumer privacy law (Approved P.L.2023, c.266) was signed into law on January 16.

Both new state consumer privacy laws follow the now-familiar format, offering consumer privacy rights and requiring role-based data processing agreements, but with a few notable differences. A more detailed comparison follows.

When Are the Two New Privacy Laws in Force?

The New Jersey privacy law was signed by New Jersey's governor on January 16, 2024, and is in force one year after its official enactment by the state of New Jersey in January 2025.

If Governor Sununu signs it in its current form, the New Hampshire law – Chapter 507-H of the New Hampshire Revised Statutes, titled "Expectation of Privacy," will be in force on January 1, 2025.

Who Are "Consumers"?

In both the New Jersey and New Hampshire laws, "consumers" are residents not "acting in a commercial or employment context." New Jersey specifies that a consumer is acting in an "individual or household context" (§1). New Hampshire further specifies that a consumer is not acting as "an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency." (§507-H:1, VIII). Accordingly, the California Consumer Privacy Act (CCPA) is still the only state privacy law that applies to personal data collected in an employment-related context and in a business-to-business context.

What Is "Personal Data"?

In both laws, personal data means information that is linked or reasonably linkable to a consumer, which is a similar definition to the other 13 state privacy laws. Both laws exclude from the definition of personal data (i) de-identified data, i.e., data that is not reasonably linkable to a consumer or device; and (ii) publicly available information, which is defined similarly to the other state consumer privacy laws.

What Are the Minimum Thresholds for Applicability of Each of the Two New Privacy Laws?

New Jersey	New Hampshire*
The New Jersey law directly applies to: A "controller," which is an "individual or legal entity" that determines "the purpose and means" of processing (i.e., operation performed on) personal data (§2) That conducts business in New Jersey or produces products or services that are targeted at New Jersey residents and, during a calendar year, (1) Controls or processes "the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction (2) Controls or processes "the personal data of at least 25,000 consumers and the controller derives revenue or receives a discount on the price of any goods or services, from the sale of personal data" (§2)	The New Hampshire privacy law applies to: "Persons" that conduct business in New Hampshire or produce products or services targeted at New Hampshire residents That during a one year period: (1) "Controlled or processed the personal data of not less than 35,000 [vs. 100,000] unique consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction" (2) "Controlled or processed the personal data of not less than 10,000 [vs. 25,000] unique consumers and derived more than 25 percent of their gross revenue from the sale of personal data (§507-H:2)

Key Differences

The New Jersey privacy law is not directly applicable to a "processor," which is an "entity" that processes personal data on behalf of a controller. That is, a processor that does not meet the threshold processing requirements is not directly subject to the New Jersey privacy law but still must comply with the requirements applicable to processors when acting on behalf of a controller that does meet the threshold above. Although "persons" is not defined in the New Hampshire privacy law, the term is defined in the state's consumer protection law as "natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations, and any other legal entity." As noted below, a violation of the New Hampshire privacy law is a violation of New Hampshire's unfair and deceptive trade practices act.

Also, the two minimum thresholds in each law differ. The first processing threshold is somewhat proportionate to each state's population.[1] The second threshold in the New Hampshire law sets a revenue floor, requiring the control or processing of more than 25% of gross revenue from personal data sales. The New Jersey law does not require a minimum revenue from personal data sales and also counts the receipt of any discount on the price of any goods or services as part of the revenue threshold.

What Organizations Are Not Subject to the Two New Privacy Laws?

Both laws contain several entity-level and data-level exemptions. Like most of the other state privacy laws, both the New Jersey privacy law and New Hampshire privacy law exempt financial institutions and data subject to the Gramm-Leach-Bliley Act; data processed pursuant to the Fair Credit Reporting Act; protected health information as defined in Health Insurance Portability and Accountability Act (HIPAA); identifiable private information as defined in the federal policy for protection of human subjects; and state agencies (NJ §10; NH §507-H:3), among other exemptions.

Key Differences

Absent from the New Jersey law is an entity-level exemption for covered entities and business associates subject to HIPAA, which is set forth in §507-H:3, I, (f) of the New Hampshire privacy law.

The New Hampshire expressly excludes federally exempt nonprofit organizations (§507-H:3-I(b)), but the New Jersey law does not. (Colorado's privacy law also applies to tax-exempt organizations and, as of July 1, 2025, Oregon's privacy law (which is in force on July 1, 2024) specifically applies to federally tax-exempt charitable organizations (§13).)

1 NH Population: 1.4M; NJ Population: 9.3M

What Is a "Sale" of Personal Data?

A sale of personal data is an "exchange … for monetary or other valuable consideration" (in the New Hampshire privacy law) or, in the New Jersey privacy law, "sharing, disclosing or transferring" personal data for "monetary of other valuable consideration" by a controller to a "third party." In both laws, a third party is any natural person or entity that is not a controller, processor or consumer.

The definition of sale in both laws excludes the following disclosures of personal data:

- Disclosures to processors or affiliates of the controller
- Disclosure to a third party for purposes of providing a product of service requested by a consumer
- Consumer-directed disclosures
- Personal data that the consumer intentionally makes available to the general public by mass media disclosures in connection with an actual or proposed merger, acquisition, bankruptcy or similar transaction when a third party assumes control or all of part of the controller's assets

What Rights Are Available for Consumers?

The privacy rights available for consumers are similar for both laws, with some differences noted in in italics.

New Jersey	New Hampshire*
• Right to confirm processing and access personal data • Right to correct inaccuracies in the consumer's personal data • Right to delete personal data *concerning* the consumer • Right to obtain a copy of the consumer's personal data held by the controller in a portable, readily usable/ transferable format • Right to opt out of the processing of the consumer's personal data for purposes of: – Targeted advertising (defined in §1) – Sale of personal data – "Profiling" in furtherance of solely automated "decisions that produce legal or similarly significant effects concerning the consumer" (each defined in §1)	• Right to confirm processing and access personal data • Right to correct inaccuracies in the consumer's personal data • Right to delete personal data provided by or obtained about the consumer • Right to obtain a copy of the consumer's personal data processed by the controller in a portable and readily usable/transferable format if the processing is carried out by automated means • Right to opt out of the processing of the consumer's personal data for purposes of: – Targeted advertising (defined in §507-H:1, XXIX) – Sale of personal data – Profiling" (§507-H:1, XXIII) in furtherance of solely automated "decisions that produce legal or similarly significant effects concerning the consumer" (§507-H:1, XIII)

Authorized agents – Both laws permit a consumer to authorize an agent to exercise rights on the consumer's behalf. In New Jersey, that agent may opt out of the processing and sale of personal data. In New Hampshire however, the consumer can authorize an agent to opt out of targeted advertising, sale and profiling, which is a narrower authority than in New Jersey (§507-H:5). Under both staters' law, the controller must comply with the agent's request if the agent's authority is verifiable with "commercially reasonable effort."

What Obligations Apply to Controllers?

Responding to consumer rights requests – In both laws, a controller has up to 45 days after receipt to respond to a consumer's privacy rights request subject to a 45-day extension when "reasonably necessary" and after informing the consumer of the delay and reason for it. The controller must comply with the request as to personal data processed during the 12 months preceding the request.

Authenticating requests – Under both laws, a controller:

- Must authenticate a privacy rights request (other than an opt-out request) using commercially reasonable efforts and is not required to comply with a request if it is unable to authenticate it
- May deny an opt-out request if it has a good faith, reasonable and documented belief that the request is fraudulent

The controller must notify the consumer if the controller declines to act on the request and the reason for the declination. Both laws offer the consumer the right to appeal, and a controller must inform the consumer in writing of any action taken or not taken in response to the appeal within 45 days (New Jersey §4f) or 60 days (New Hampshire §507-H:4:IV)). The controller also must provide the consumer with an online mechanism to contact the respective state regulator tasked with enforcing the privacy law, i.e., the Division of Consumer Affairs, in New Jersey, or the attorney general, in New Hampshire.

Both laws allow a controller not to comply with requests under other circumstances. For example, in New Jersey, a controller need not comply with a request to confirm or access a consumer's personal data processing if doing so reveals a trade secret of the controller. Under the New Hampshire law, the controller has no obligation to comply with a request for confirmation of processing or access to or portability of personal data if doing so reveals any of the controller's trade secrets.

Universal Opt-Out Mechanism (UOOM) requirements – Under New Jersey's privacy law, starting in July 2025, a controller must respond to a UOOM that enables consumers to opt-out of targeted advertising and the sale of personal data, but not profiling (§8.b.1). Consumers may still "designate an authorized agent using technology, including a link to an Internet website, an Internet browser setting or extension or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt-out of the collection and processing … for profiling … when such technology exists." (§ 8.a). Additionally, "[t]he Division of Consumer Affairs in the Department of Law and Public Safety may adopt rules and regulations that detail the technical specifications for one or more universal opt-out mechanisms … [and] may update the rules … from time to time." (§ 8.c). As for notice, "[c]ontrollers shall inform consumers about the opt-out choices available." (§ 8.b(3)).

The New Hampshire privacy law requires use of a UOOM by January 1, 2025, that allows "a consumer to opt-out of any processing of the consumer's personal data for the purpose of targeted advertising, or any sale of such personal data" (507-H:6:V(1.B). If the opt-out request "conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with such consumer's opt-out preference signal but may notify the consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program." (§507-H:6 (V) (a)(2)).

Like the predecessor state privacy laws, general UOOM requirements include:

- The UOOM must not use default settings unless "the controller has determined that the consumer has selected such default settings and the selection clearly represents the consumer's affirmative, freely given and unambiguous choice to opt into any processing of such consumer's personal data"
- The UOOM must be consumer friendly, clearly described and easy to use, as well as "consistent with any other similar platform, technology or mechanisms"
- The controller must be able to use the UOOM to determine whether the consumer is a resident of New Jersey or New Hampshire (as applicable) and whether the consumer made a legitimate request to opt out (New Jersey §8, New Hampshire, §507-H:6 (V))

Processing obligations related to sensitive data – A controller cannot process sensitive data without obtaining the consumer's consent. (New Jersey §9(a)(4); New Hampshire §507-H:6:I.d).

The two laws have slightly different definitions for "sensitive data." Both laws' definition of sensitive data includes personal data revealing racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; citizenship or immigration status; personal data collected from a known child under age 13; and precise geolocation data.

In the New Jersey privacy law, sensitive data (§1) adds:

- "Health treatment" in addition to health condition and diagnosis.
- "Status as transgender or non-binary" in addition to sex life or sexual orientation.
- "Financial information," which is defined to include "a consumer's account number, account log-in, financial account or credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account." (The definition of financial information in the New Jersey privacy law is materially similar to the definition of personal information in New Jersey's data breach notification law.)

Also, the New Jersey privacy law's definition of sensitive data includes "genetic or biometric data that may be processed for the purpose of uniquely identifying an individual," which is arguably broader than the New Hampshire privacy law's inclusion of the "processing of genetic or biometric data for the purpose of uniquely identifying an individual." (§507-H:1, XXVIII).

Processing obligations related to minors – Both laws require that a controller process sensitive data concerning (vs. collected from as per the sensitive data definition) a known child (i.e., under age 13) in compliance with the Children's Online Privacy Protection Act.

The New Hampshire law specifies that a known child's parent or legal guardian may exercise privacy rights on the child's behalf. (507-H:4 (II)). This right is in addition to the consumer right to designate an authorized agent, as described above.

If a controller has actual knowledge or "willfully disregards" that a consumer is age 13 to 16, the controller must obtain the consumer's consent when processing for the purposes of targeted advertising or for sale of personal data. (New Jersey §9.7, New Hampshire §507-H:6:I.g).

What Are the Privacy Notice Requirements?

In both states' laws, a controller must provide consumers with a privacy notice that includes:

- Categories of personal data processed by the controller
- The purposes for processing the personal data
- The categories of personal data that the controller shares with third parties
- The categories of third parties with which the controller discloses the personal data
- A description of how consumers may exercise their privacy rights and appeal a controller's decision about responding to a consumer privacy right
- Email address or other online method by which a consumer may contact the controller

In New Jersey, the notice also must include the process by which the controller notifies consumers of the material changes to the notification required to be made available pursuant to this subsection, along with the effective date of the notice. (§3a(6)).

Role-based processing – As with all the state consumer privacy laws preceding the New Jersey and New Hampshire laws, a controller must enter into a binding contract with each processor that assists the controller with personal data processing that sets out the nature and purpose of the processing, the type of personal data subject to the processing and the duration of the processing. The processor contract also must require the processor to impose a duty of confidentiality on the processor's personnel and engage sub-processors pursuant to a contract with the same terms as apply to the processor (*inter alia*). The New Hampshire privacy law requires that the processor allow the controller to object to a subcontractor before the subcontractor is engaged (§507-H:7, II(d)), but the New Jersey privacy law does not have a similar requirement. The New Jersey privacy law also requires that the processor and controller establish "a clear allocation of the responsibilities between them to implement [security] measures." (§13.d).

Disclosure requirements for sales of personal data – The requirements in New Jersey's privacy law are broader:

New Jersey	New Hampshire
"If a controller sells personal data to third parties or processes personal data for the purpose of targeted advertising, the sale of personal data or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, the controller shall clearly and conspicuously disclose such sale or processing, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing. (§3.7(b))	"If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt-out of such processing." (§507-H:6:IV)

Are Controllers Required to Conduct Data Protection Assessments?

Both laws require a controller to conduct and document a data protection assessment prior to undertaking a processing activity that presents a heightened risk of harm to a consumer. "Heightened risk" includes:

- Processing personal data for targeted advertising
- Processing personal data for profiling, if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment, (ii) unlawful disparate impact, (iii) financial or physical injury [or reputational injury, in New Hampshire], (iv) physical or other intrusion upon solitude, seclusion, or private affairs that would be offensive to a reasonable person or (v) other substantial injury to consumers
- Selling personal data
- Processing sensitive data

Prior to processing personal data for the above purposes, a controller must identify and weigh the benefits of the processing activity to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer. In this risk-benefit analysis, controllers must also consider how safeguards may mitigate the identified risks and must factor in the use of de-identified data, the reasonable expectations of consumers, the context of processing and the relationship between the controller and the consumer.

Controllers in both states should be prepared to make data protection assessments available to regulators upon request, which are the Division of Consumer Affairs in New Jersey and the Attorney General in New Hampshire. Both the laws in New Jersey and New Hampshire provide that assessments provided to regulators will remain confidential and exempt from disclosure to the public. Additionally, the disclosure of assessments to the respective regulator would not constitute a waiver of attorney-client privilege or work product protection.

Key Differences
The New Hampshire requirement to conduct and document data protection assessments applies to processing activities created or generated after July 1, 2024, while the New Jersey law mandates assessments for processing activities that involve personal data acquired on or after the effective date of the law. Thus, in New Hampshire, it will be imperative for controllers to start the process of conducting data protection assessments for processing activities that were created or generated six months prior to the effective date of the law.

What Are the Consequences of Non-compliance?

Neither the New Jersey privacy law (§16) nor the New Hampshire privacy law (§507-H:11, IV) includes a private right of action. The attorney general in each state is responsible for enforcement.

Time-limited right to cure breaches – In both laws, the attorney general must issue a notice identifying a curable breach and allow a controller the opportunity to cure. The cure period is time-limited as follows.

New Jersey	New Hampshire
Cure period is 18 months following the in-force date of the New Jersy privacy law (i.e., until ~ June 2026). The controller has 30 days after receipt of the notice to cure the breach (§14b).	Cure period is 12 months – from January 1 through December 31, 2025. **Key difference** – A controller has 60 days after receipt of the notice to cure the breach (§507-h:11, II). Beginning January 1, 2026, the attorney general can determine whether to allow a cure period. (§507-h:11, III).

Other differences include:

New Jersey	New Hampshire
A violation of the New Jersey privacy law is a violation of New Jersey's unfair and deceptive trade practices act (NJ Rev Statutes, C. 56: 8-1 et seq.). The attorney general may seek penalties of up to US$10,000 for the first violation and up to US$20,000 for any subsequent violation.	A violation of the New Hampshire privacy law is a violation of New Hampshire's unfair and deceptive trade practices act. The attorney general may seek civil penalties of up to US$10,000 for each violation.
The Director of New Jersey's Division of Consumer Affairs must promulgate "rules and regulations" to "effectuate the purposes" of the New Jersey privacy law (§15), including in particular rules and regulations regarding a universal opt-out mechanism that is as consistent as possible with the approach taken in other states. (§8.b.(2)(d)).	**Key difference** –The New Hampshire privacy law (§507-H:6, III) allows for rule-making only with respect to privacy notice requirements.

Following is our non-inclusive list of comprehensive privacy bills in state legislatures in 2024, roughly organized in order from closest to enactment to furthest from enactment.

State	Name of Bill	Progress
Oklahoma	Oklahoma Computer Data Privacy Act	• Legislature recessed on May 27, 2023, without passing the bill. The bill will carry over to the next legislative session in February 2024. • Track it here.
Hawaii	An Act Relating to Consumer Data Protection	• State legislature adjourned on May 4, 2023, without passing the bill. Bill will be carried over to the next legislative session in January 2024. • Track it here.
Illinois	• Illinois Data Privacy and Protection Act • Right to Know Act	• Legislature recessed on May 28, 2023, without passing the bills. Session will resume in January 2024. • Track the Data Privacy and Protection Act here. • Track the Right to Know Act here.
Minnesota	• Minnesota Consumer Data Privacy Act • Act relating to consumer data privacy (D) • Act relating to consumer data privacy (R)	• State legislature recessed on May 23, 2023, without passing the bills. Bills will be carried over to the next session in February 2024. • Track the Consumer Data Privacy Act *here*, t he (D) bill here, and the (R) bill here.
New York	• Data Privacy and Protection Law • Acquisition and Control of Private and Personal Information; Data Security Protections • New York Privacy Act • Digital Fairness Act • New York Privacy Act (II) • New York Data Protection Act • It's Your Data Act	• All bills were referred to committee on January 3, 2024. • Track Data Privacy and Protection Law here. • Track Acquisition and Control of Private and Personal Information here. • Track New York Privacy Act here. • Track Digital Fairness Act here. • Track New York Privacy Act (II) here. • Track New York Data Protection Act here. • Track It's Your Data Act here.
North Carolina	North Carolina Consumer Privacy Act	• Passed first reading in the Senate and referred to committee on April 4, 2023. • Track it here.
Pennsylvania	Consumer Data Privacy Act	• Referred to committee on January 9, 2024. • Track it here.
Vermont	An act relating to enhancing consumer privacy	• Introduced and referred to committee on January 26, 2023, with no significant progress. • Track it here.
Washington	People's Privacy Act	• Reintroduced on January 8, 2024. • Track it here.
Massachusetts	• Massachusetts Data Privacy Protection Act • Massachusetts Information Privacy and Security act • Internet Bill of Rights	• All three were referred to committee on February 16, 2023, with no significant progress. • A hearing took place on the Data Privacy Protection Act and the Information Privacy and Security Act in joint committees on October 11, 2023. • Track Data Privacy Protection Act here. • Track Information Privacy and Security Act here. • Track Internet Bill of Rights here.

State	Name of Bill	Progress
Kentucky	Act Relating to Consumer Data Privacy	• Introduced and referred to committee on January 2, 2024. • Track it here.
Maine	Consumer Privacy Act	• Introduced and referred to committee on May 18, 2023. • Joint work session held on October 17, 2023. Subsequent work sessions were tabled. • Track it here.
Michigan	Personal Data Privacy Act	• Introduced and referred to committee on November 9, 2023. • Track it here.
Missouri	Act Relating to the Protection of Data	• First reading in the senate held on January 3, 2024, and second reading held on January 8, 2024. • Track it here.
Ohio	Personal Privacy Act	• Introduced on November 29, 2023, and referred to committee on December 6, 2023. • Track it here.
Wisconsin	Act Relating to Consumer Data Protection	• Public hearing in the Senate held on December 19, 2023. • Track it here.

Privacy World will continue to cover updates related to privacy law developments in the US and around the world. Please contact the authors for more information.

*Special thanks to Krista Setera for her contribution to this article.

Contacts

Julia Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Sasha Kiosse
Associate, New York
T +1 212 872 9861
E alexandra.kiosse@squirepb.com

Alan Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com