New Hampshire Data Privacy Act

On January 1, 2025, the New Hampshire Data Privacy Act ("NHDPA"), RSA 507-H, came into effect. This statute is the result of two bills, SB 255-FN and HB 1220-FN. Former Governor Chris Sununu signed SB 255-FN into law on March 6, 2024, and HB 1220-FN into law on July 19, 2024.

The following contains a summary of rights for New Hampshire consumers and a list of frequently asked questions for businesses. The information contained herein is not legal advice or an opinion from the Attorney General and should not be considered comprehensive. If consumers or businesses have questions regarding the requirements of RSA 507-H, they are encouraged to review the statute or speak with a private attorney.

If you would like to report a violation of the NHDPA, please fill out a Consumer Protection complaint form at this link or email DOJ-CPB@doj.nh.gov.

Consumer Data Privacy Rights

What are New Hampshire consumers' new data privacy rights?

As a New Hampshire consumer, starting on January 1, 2025, you have the following rights:

- **Confirm** whether or not certain businesses are **processing** your personal data;
- **Obtain Access** to your personal data being **processed** by those businesses;
- **Correct inaccuracies** in your personal data being **processed** by those businesses;
- **Delete** personal data provided by, or obtained about, you by those businesses;
- **Obtain a copy** of your personal data in a portable format; and
- **Opt-out of the future processing of personal data** for purposes of:
    - **targeted advertising**,
    - the **sale** of personal data, or
    - certain types of **automated profiling**.

Businesses cannot discriminate against you, deny you service, or charge you different rates if you exercise your rights. You have a right to receive information under these rights free of charge at least once during any twelve-month period.

Once the business receives your request exercise any of the above rights, it must respond to you within 45 days. The business can extend its time to reply by up to an additional 45 days. If this occurs, the business must inform you of the extension within the initial 45-day response period and provide a reason for the extension.

A business must seek your consent if it processes your data in certain specified ways. The following are examples of data processing that require consent:

- Processing your data outside of the purposes of collection the business disclosed to you;
- Processing "sensitive data" concerning you;
- Selling personal data or processing personal data for targeted advertising of a consumer known to be at least 13 years old and less than 16 years old.

A business must provide a mechanism for you to revoke consent "that is at least as easy" as the mechanism by which you provided consent. Once the business receives your request to revoke consent, it must stop processing your data within 15 days.

How can New Hampshire consumers exercise their data privacy rights?

- You may exercise your rights by any secure and reliable means described to you in the business' privacy notice. This notice must be clear, meaningful, and reasonably accessible.

- Businesses that control data must "clearly and conspicuously" disclose how to opt out of data sales and targeted advertising. Such businesses must also provide a "clear and conspicuous" link on their website to a webpage that enables you or your agent to opt out of targeted advertising and sales of your personal data.

- You may designate an agent to exercise your opt-out rights for you. You may also opt out of targeted advertising and data sales through an opt-out preference signal or global device setting.

- A parent or legal guardian may exercise consumer rights on their child's behalf. For consumers subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

The attorney general has exclusive authority to enforce NHDPA violations. **If you believe the NHDPA has been violated, please submit a complaint to the New Hampshire Attorney General.** Fill out a Consumer Protection complaint form at this link or email CPB-DOJ@doj.nh.gov.

What are some issues that New Hampshire consumers might encounter while trying to exercise their rights?

- Certain businesses and types of information are exempted from the NHDPA (See Below FAQs for a list of exempt businesses).

- A business which controls data can deny your rights request if it is unable to authenticate a rights request. If this happens, the business must provide you notice that it is unable to authenticate the request until you provide additional information reasonably necessary to authenticate the request. A business cannot require you to create a new account to exercise your rights.

- A business which controls data may deny an opt-out request if it has a good faith, reasonable and documented belief that your request is fraudulent. If this occurs after you try to exercise your opt-out rights, the business must send you a notice explaining that it

believes your request is fraudulent, explain why it believes your request is fraudulent, and state that it will not comply with your request.

- If a business which controls data declines to take action regarding your request, the business must inform you not later than 45 days after it receives your request, of the justification for declining to take action and instructions for how to appeal the decision.

- If your request is denied, you have a right to appeal the denial through a process established by the business. This appeal process must be conspicuously available and similar to the process for submitting requests. A business has 60 days after receiving your appeal to inform you in writing of any action taken or not taken in response to your appeal, and to provide a written explanation of the reasons for its decisions. If the appeal is denied, the business must provide you with a method for you to contact the attorney general to submit a complaint.

Frequently Asked Questions for Businesses

When did the NHDPA take effect?

RSA 507-H took effect on **January 1, 2025**.

What does the NHDPA do?

The NHDPA gives New Hampshire residents certain rights over their personal data and establishes responsibilities and privacy protection standards for entities which handle personal data (data controllers and processors).

What is "Personal Data?"

"Personal Data" is 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. RSA 507-H:1, XIX.

What rights can New Hampshire residents exercise under the NHDPA?

New Hampshire consumers have the following rights:

- **Confirm** whether or not a controller is **processing** the consumer's personal data;
- **Access** the consumer's 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; and
- **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.

RSA 507-H:4, I.

What persons must comply with the NHDPA?

The NHDPA applies to persons that **conduct business in this state** or persons that **produce products or services** that are **targeted to residents of this state** that during a one 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**.

RSA 507-H:2, I.

What is a "Controller?"

A "controller" is any person or legal entity, that either alone or with others, determines the purpose and means of processing personal data. RSA 507-H:1, IX.

In addition to the other rights and responsibilities outlined in RSA 507-H, controllers may wish to take special notice of RSA 507-H:6 and RSA 507-H:10, which describe controller responsibilities.

What is a "Processor?"

A "processor" is any person or legal entity that processes personal data on behalf of a controller. RSA 507-H:1, XXII.

In addition to the other rights and responsibilities outlined in RSA 507-H, processors may wish to take special notice of RSA 507-H:7, which describes processor responsibilities.

What does it mean to "Process" data?

"Processing" means any manual or automatic operation or set of operations on personal data. Examples include the collection, use, storage, disclosure, analysis, deletion or modification of personal data. RSA 507-H:1, XXI.

What is "Sensitive Data?"

"Sensitive Data" is a subset of personal data that includes data revealing:

- Racial or ethnic origin;

- Religious beliefs;

- Mental or physical health condition or diagnosis;
- Sex life or sexual orientation;
- 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.

RSA 507-H:1, XXVIII.

What are the NHDPA requirements for processing "Sensitive Data"?

"Sensitive Data" is subject to additional restrictions under RSA 507-H. For example,

- Controllers may not process sensitive data concerning a consumer without obtaining the consumer's consent,
- Controllers may not process sensitive data concerning a known child without processing such data in accordance with COPPA, and
- Controllers must conduct and document a data protection assessment for each of the controller's processing activities that include processing sensitive data.

RSA 507-H:6, I (d), RSA 507-H:8, I.

Who is exempt from complying with the NHDPA?

The following entities are exempt from the NHDPA:

- Any State of New Hampshire body, authority, board, bureau, commission, district or agency or any political subdivision thereof;
- Any nonprofit organization;
- Any institution of higher education;
- Any national securities association that is registered under 15 U.S.C. section 78o-3 of the Securities Exchange Act of 1934;

- Any financial institution or data subject to Title V of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. 6801 et seq.; or,

- Any covered entity or business associate, as defined in 45 C.F.R. 160.103.(b).

RSA 507-H:3, I.

What information and data is exempt from the NHDPA?

The NHDPA does not apply to the following information and data:

Certain Health Information and Data

- Protected health information under HIPAA; RSA 507-H:3, II (a);

- Patient-identifying information for purposes of 42 U.S.C. section 290dd-2; RSA 507-H:3, II (b);

- 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; RSA 507-H:3, II (h);

- 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; RSA 507-H:3, II (i);

- Information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; RSA 507-H:3, II (j);

- 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). RSA 507-H:3, II (r).

Certain Information and Data on Human Research Subjects

- Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. 46; RSA 507-H:3, II (c);

- 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; RSA 507-H:3, II (d);

- 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; RSA 507-H:3, II (e);

Certain Information and Data Regarding Professional Review Activities

- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq.; RSA 507-H:3, II (f);

- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq., as amended; RSA 507-H:3, II (g);

Certain Information about Applicants, Employees, Agents, or Independent Contractors

- 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; RSA 507-H:3, II (o);

Certain Information and Data Subject to Other Federal Laws

- 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.; RSA 507-H:3, II (k);

- 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; RSA 507-H:3, II (l);

- Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq., as amended; RSA 507-H:3, II (m);

- Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. 2001 et seq., as amended; RSA 507-H:3, II (n);

- 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; RSA 507-H:3, II (p);

- 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; RSA 507-H:3, II (q);

RSA 507-H:3, II.

How can a consumer exercise rights under the NHDPA?

- A consumer may exercise the NHDPA rights by any secure and reliable means described to the consumer in the controller's privacy notice.

- A consumer may designate an authorized agent in accordance with RSA 507-H:5 to exercise the rights of such consumer to opt-out of the processing of such consumer's personal data for purposes of RSA 507-H:4, III(e) on behalf of the consumer.

- In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf.

- In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

RSA 507-H:4, II.

How can a consumer designate an agent to opt-out of targeted advertising, sale of personal data, and automated profiling?

A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt-out of the processing of such consumer's personal data for 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.

The consumer may designate such authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt-out of such processing.

A controller must comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

RSA 507-H:5.

Can a consumer opt-out of the sale of personal data to third parties?

Yes, a consumer can opt-out of the sale of personal data to third parties. The controller must provide a process for submitting an opt-out request. A consumer can also designate a third party to opt-out on his or her behalf and can use an opt-out preference signal.

Can a controller deny a consumer rights request?

Yes, under certain circumstances.

If a controller is unable to authenticate a request to exercise any of the rights afforded under RSA 507-H:4, I(a)-(d) using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate the requested action. The controller must provide notice to the consumer that the controller is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the request. RSA 507-H:4, III (d).

A controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes it is fraudulent, the controller must send a notice to the person who made the request explaining that the controller believes the request is fraudulent, why the controller believes it is fraudulent and that the controller will not comply with a fraudulent request. RSA 507-H:4, III (d).

If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision. RSA 507-H:4, III (b).

Does a consumer have a right to appeal a denial?

Yes.

A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests. A controller has 60 days after receiving the appeal to inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

RSA 507-H:4, IV.

How often can a consumer request information about their personal data from a controller? Is there a cost?

Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period.

If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

RSA 507-H:4, III (c).

How long does a controller have to respond to a consumer's request?

Controllers must respond to the consumer "without undue delay, but not later than 45 days after receipt of the request." This time period may be extended "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."

RSA 507-H:4, III (a).

What must a controller disclose to consumers?

Privacy notice

Controllers must provide a clear, accessible privacy notice and disclose the following in that notice:

- The categories of data processed. RSA 507-H:6, III (a).
- The purpose of processing. RSA 507-H:6, III (b).
- How consumers may exercise their consumer rights. RSA 507-H:6, III (c), V. (a).
- How a consumer may appeal a decision regarding a request. RSA 507-H:6, III (c).
- Categories of data shared with third parties. RSA 507-H:6, III (d).
- Categories of third parties with whom data is shared. RSA 507-H:6, III (e).
- An online mechanism to contact the controller. RSA 507-H:6, III (f).

- The date the privacy notice was last updated. RSA 507-H:6, III (g).

Controllers must also clearly and conspicuously disclose the following:

- All personal data sales and targeted advertising. RSA 507-H:6, IV.
- How a consumer may opt out of data sales and targeted advertising. RSA 507-H:6, IV.
- A link on the controller's website to a targeted advertising and data sales opt-out webpage. RSA 507-H:6, V (a)(1)(A).

When must a controller seek consent before processing data?

- A controller must only process a consumer's data outside of the controller's disclosed purposes of collection if the consumer consents. RSA 507-H:6, I (b).
- A controller must only process sensitive data of a consumer if the consumer consents. RSA 507-H:6, I (d).
- A controller must allow consumer to revoke consent easily and stop processing within 15 days of consumer's revocation. RSA 507-H:6, I (f).

When must a controller conduct a data protection assessment?

If a controller processes data or causes data to be processed after July 1, 2024, that controller must 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.

Processing that presents a heightened risk of harm to a consumer includes:

- The processing of personal data for the purposes of **targeted advertising**, RSA 507-H:8, I (a);
- The **sale** of personal data, RSA 507-H:8, I (b);
- The processing of personal data for the purposes of certain types of **profiling**, RSA 507-H:8, I (c); and
- The processing of **sensitive data**. RSA 507-H:8, I (d).

What are other controller obligations?

- There are limits on a controller's collection of data. RSA 507-H:6, I (a).
- Controllers must implement reasonable data safeguards. RSA 507-H:6, I (c).
- There are antidiscrimination requirements for controllers. RSA 507-H:6, I (e).
- Controllers may not engage in targeted advertising or selling personal data for subjects ≥13 and <16 without consent. RSA 507-H:6, I (g).
- Controllers cannot discriminate against a consumer if the consumer exercises consumer rights. Such discrimination could include denying services or charging different rates. RSA 507-H:6, I (g).
- Controllers must establish one or more means to submit a request to exercise rights. These must include at least:
    - Providing a clear and conspicuous link on the controller's website to a targeted advertising and data sales opt-out webpage, RSA 507-H:6, V (a); and
    - Allowing targeted advertising and data sales opt-outs through an opt-out preference signal. RSA 507-H:6, V (b).

What are the responsibilities of a processor?

A processor must adhere to the instructions of a controller and assist the controller in meeting the controller's obligations under RSA 507-H. RSA 507-H:7, I.

Such assistance must include:

- Assisting the controller in responding to consumer rights requests, RSA 507-H:7, I(a);
- Assisting the controller in ensuring the security of processing, RSA 507-H:7, I(b);
- Assisting the controller in relation to the notification of security breaches, RSA 507-H:7, I(b);
- Providing necessary information to enable the controller to conduct and document data protection assessments, RSA 507-H:7, I(c).

What must a controller-processor contract include?

A contract between a controller and a processor must govern the processor's data processing procedures. This contract must clearly set forth:

- Instructions for processing data,
- The nature and purpose of processing,
- The type of data subject to processing,
- The duration of processing, and
- The rights and obligations of both parties. RSA 507-H:7, II.

The controller-processor contract must also require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data, RSA 507-H:7, II(a);
- 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, RSA 507-H:7, II(b);
- 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, RSA 507-H:7, II(c);
- 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, RSA 507-H:7, II(d); 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 this 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. RSA 507-H:7, II(e).

Who can enforce the NHDPA?

The attorney general has exclusive authority to enforce NHDPA violations. RSA 507-H:11, I. The NHDPA does not provide for a private right of action. RSA 507-H:11, IV.

Is there a cure period?

Between January 1, 2025 and December 31, 2025

Prior to initiating an action for a violation of RSA 507-H, if the attorney general determines that a cure is possible, the attorney general will issue a notice of violation to a controller. 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. RSA 507-H:11, II.

Beginning January 1, 2026

The attorney general **may** issue a notice of violation with a cure period but is not required to do so. The attorney general may consider certain criteria in determining whether to grant an opportunity to cure. RSA 507-H:11, III.

What are the penalties for failing to comply with the NHDPA?

A violation of the NHDPA is considered an unlawful act under RSA 358-A:2, the New Hampshire Consumer Protection Act. Civil penalties for violating RSA 358-A:2 may be **up to $10,000 for each violation**. RSA 358-A:4, III (b).

Pursuant to RSA 358-A, the Attorney General may also seek:

- Temporary or permanent injunctive relief; RSA 358-A:4, III (a);
- Restitution to any person or class of persons injured; RSA 358-A:4, III (a);
- All legal costs and expenses incurred by the state; RSA 358-A:6, IV;
- Appointment of a receiver; RSA 358-A:4, III-a.
- If the violator acts purposely, they may also face criminal penalties. Such penalties include a misdemeanor criminal conviction for a violator who is a natural person or a felony criminal conviction for a violator who is not a natural person. RSA 358-A:6, I.

The Attorney General may also take other enforcement measures pursuant to RSA 358-A.