HB 1694-FN - AS INTRODUCED

2026 SESSION

26-2612
07/06

HOUSE BILL ***1694-FN***

AN ACT relative to the regulation of and protections for personal data obtained by websites and data brokers.

SPONSORS: Rep. Wade, Straf. 15; Rep. Long, Hills. 26; Rep. H. Howard, Straf. 4; Rep. Giasson, Hills. 29; Rep. Barton, Graf. 1

COMMITTEE: Judiciary

ANALYSIS

This bill:

I. Requires data brokers that operate in this state to register with the secretary of state.

II. Requires the secretary of state to create and maintain an online data broker registry portal.

- -

Explanation: Matter added to current law appears in ***bold italics.***
Matter removed from current law appears [~~in brackets and struckthrough.~~]
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

26-2612
07/06

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty-Six

AN ACT relative to the regulation of and protections for personal data obtained by websites and data brokers.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 Actions, Process, and Service of Process; Expectation of Privacy; Consumer Expectation of Privacy. Amend RSA 507-H:4, I(e) to read as follows:

(e) Opt-out of the processing of the personal data for [~~purposes of targeted advertising, the sale of personal data~~] ***any purpose***, except as provided in RSA 507-H:6 ***and RSA 507-H:10***, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

2 New Subparagraph; Actions, Process, and Service of Process; Expectation of Privacy; Consumer Expectation of Privacy. Amend RSA 507-H:4, III by inserting after subparagraph (e) the following new subparagraph:

(f) A controller or registered data broker that receives a request for deletion of data or opt-out of data processing shall notify the consumer, by secure and reliable means, within 15 days of completing the request, confirming that such personal data has been deleted and/or that the consumer has been opted out of any future collection or processing.

3 New Subdivision; Registration of Data Brokers. Amend RSA 507-H by inserting after section 12 the following new subdivision:

Registration of Data Brokers

507-H:13 Definitions. In this subdivision:

I. "Data broker" means a controller or processor that knowingly collects, aggregates, or sells personal data of consumers who are residents of this state, who do not have a direct business relationship with the controller or processor, and who derive more than 25 percent of their gross revenue from the sale of personal data.

II. "Digital service" means a website, an application, a program, or software that collects or processes personal identifying information with Internet connectivity.

III. "Digital service provider" means a person who:

(a) Owns or operates a digital service;

(b) Determines the purpose of collecting and processing the personal identifying information of users of the digital service; and

(c) Determines the means used to collect and process the personal identifying information of users of the digital service.

IV. "Known minor" means a person that a digital service provider knows to be a minor.

V. "Minor" means a child who is younger than 18 years of age who has not had the disabilities of minority removed for general purposes.

VI. "Personal identifying information" means any information, including sensitive information, that is linked or reasonably linkable to an identified or identifiable individual. Personal identifying information shall include pseudonymous information when the information is used by a controller or processor in conjunction with additional information that reasonably links the information to an identified or identifiable individual.

VII. "Verified parent" means the parent or guardian of a known minor whose identity and relationship to the minor have been verified by a digital service provider.

507-H:14 Registration.

I. To conduct business in this state, a data broker to which this chapter applies shall register with the secretary of state by filing a registration statement and paying a registration fee of $300.

II. The registration statement shall include:

(a) The legal name of the data broker;

(b) A contact person and the primary physical address, e-mail address, telephone number, and Internet website address for the data broker;

(c) A description of the categories of data the data broker processes and transfers;

(d) A statement of whether or not the data broker implements a purchaser credentialing process;

(e) If the data broker has actual knowledge that the data broker possesses personal data of a known child:

(1) A statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal data of a known child; and

(2) A statement on how the data broker complies with applicable federal and state law regarding the collection, use, or disclosure of personal data from and about a child on the Internet; and

(f) The number of security breaches the data broker has experienced during the year immediately preceding the year in which the registration is filed, and if known, the total number of consumers affected by each breach.

III. A registration of a data broker may include any additional information or explanation the data broker chooses to provide to the secretary of state concerning the data broker's data collection practices.

IV. A registration certificate expires on the first anniversary of its date of issuance. A data broker may renew a registration certificate by filing a renewal application, in the form prescribed by the secretary of state, and paying a renewal fee in the amount of $300.

507-H:15 Registry of Data Brokers.

I. The secretary of state shall establish and maintain on its website, a searchable, central registry of data brokers registered this subdivision.

II. The registry shall include:

(a) A search feature that allows a person searching the registry to identify a specific data broker; and

(b) For each data broker, the information filed under RSA 507-H:14.

507-H:16 Protection of Personal Data.

I. A data broker conducting business in this state shall have a duty to protect personal data held by that data broker as provided by this section.

II. A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate for:

(a) The data broker's size, scope, and type of business;

(b) The amount of resources available to the data broker;

(c) The amount of data stored by the data broker; and

(d) The need for security and confidentiality of personal data stored by the data broker.

III. The comprehensive information security program required by this section shall:

(a) Incorporate safeguards that are consistent with the safeguards for protection of personal data and information of a similar character under state or federal laws and regulations applicable to the data broker;

(b) Include the designation of one or more employees of the data broker to maintain the program;

(c) Require the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other record containing personal data, and the establishment of a process for evaluating and improving, as necessary, the effectiveness of the current safeguards for limiting those risks, including by:

(1) Requiring ongoing employee and contractor education and training, including education and training for temporary employees and contractors of the data broker, on the proper use of security procedures and protocols and the importance of personal data security;

(2) Mandating employee compliance with policies and procedures established under the program; and

(3) Providing a means for detecting and preventing security system failures;

(d) Include security policies for the data broker's employees relating to the storage, access, and transportation of records containing personal data outside of the broker's physical business premises;

(e) Provide disciplinary measures for violations of a policy or procedure established under the program;

(f) Include measures for preventing a terminated employee from accessing records containing personal data;

(g) Provide policies for the supervision of third-party service providers that include:

(1) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal data consistent with applicable law; and

(2) Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal data;

(h) Provide reasonable restrictions on physical access to records containing personal data, including by requiring the records containing the data to be stored in a locked facility, storage area, or container;

(i) Include regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal data and, as necessary, upgrading information safeguards to limit the risk of unauthorized access to or unauthorized use of personal data;

(j) Require the regular review of the scope of the program's security measures that must occur:

(1) At least annually; and

(2) Whenever there is a material change in the data broker's business practices that may reasonably affect the security or integrity of records containing personal data;

(k) Require the documentation of responsive actions taken in connection with any incident involving a breach of security, including a mandatory post-incident review of each event and the actions taken, if any, to make changes in business practices relating to protection of personal data in response to that event; and

(l) To the extent technically feasible, include the following procedures and protocols with respect to computer system security requirements or procedures and protocols providing a higher degree of security, for the protection of personal data:

(1) The use of secure user authentication protocols that include each of the following features:

(A) Controlling user log-in credentials and other identifiers;

(B) Using a reasonably secure method of assigning and selecting passwords or using unique identifier technologies, which may include biometrics or token devices;

(C) Controlling data security passwords to ensure that the passwords are kept in a location and format that do not compromise the security of the data the passwords protect;

(D) Restricting access to only active users and active user accounts; and

(E) Blocking access to user credentials or identification after multiple unsuccessful attempts to gain access;

(2) The use of secure access control measures that include:

(A) Restricting access to records and files containing personal data to only employees or contractors who need access to that personal data to perform the job duties of the employees or contractors; and

(B) Assigning to each employee or contractor with access to a computer containing personal data unique identification and a password, which may not be a vendor-supplied default password, or using another protocol reasonably designed to maintain the integrity of the security of the access controls to personal data;

(3) Encryption of:

(A) Transmitted records and files containing personal data that will travel across public networks; and

(B) Data containing personal data that is transmitted wirelessly;

(4) Reasonable monitoring of systems for unauthorized use of or access to personal data;

(5) Encryption of all personal data stored on laptop computers or other portable devices;

(6) For files containing personal data on a system that is connected to the Internet, the use of reasonably current firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal data; and

(7) The use of:

(A) A reasonably current version of system security agent software that must include malware protection and reasonably current patches and virus definitions; or

(B) A version of system security agent software that is supportable with current patches and virus definitions and is set to receive the most current security updates on a regular basis.

507-H:17 Online Portal and Forms.

I. The secretary of state shall create and administer an online data broker and registry portal. The portal shall contain a form to process data requests to and from all registered data brokers. The form shall require an individual's contact information to verify their identity.

II. Forms on the online portal shall allow an individual to request a copy of their data, request that their data be deleted, and request to be permanently opted-out of future data processing from all registered data brokers.

III. Upon completion of the form, a copy of the form shall be sent to all registered data brokers in this state, who shall comply with the request or requests of the form filer.

IV. Data brokers who receive a request from a filer pursuant to this section shall inform the filer they have received the request and that they will work to comply with their request in an expeditious manner.

V. Data brokers who receive a request from a filer under this section shall have 15 days process and comply with the request of the filer.

VI. The portal shall allow an individual to request a copy of their data and to delete all of their collected data.

507-H:18 Civil Penalty.

I. A data broker that violates this subdivision shall be liable to the state for a civil penalty as prescribed by this section.

II. A civil penalty imposed against a data broker under this section:

(a) Subject to subparagraph (b), may not be in an amount less than the total of:

(1) $100 for each day the entity is in violation of this subdivision; and

(2) The amount of unpaid registration fees for each year the entity failed to register in violation of this subdivision; and

(b) May not exceed $10,000 assessed against the same data broker in a 12-month period.

III. The attorney general may bring an action to recover a civil penalty imposed under this section. The attorney general may recover reasonable attorney's fees and court costs incurred in bringing the action.

507-H:19 Deceptive Trade Practice. A violation of this subdivision by a data broker shall constitute a deceptive trade practice under RSA 358-A and shall be actionable under that chapter.

507-H:20 Rules. The secretary of state shall adopt rules as necessary to implement this subdivision.

4 Effective Date. This act shall take effect January 1, 2027.

LBA
26-2612
12/1/25

HB 1694-FN- FISCAL NOTE
AS INTRODUCED

AN ACT relative to the regulation of and protections for personal data obtained by websites and data brokers.

FISCAL IMPACT: This bill does not provide funding, nor does it authorize new positions.

Estimated State Impact				
	FY 2026	**FY 2027**	**FY 2028**	**FY 2029**
Revenue	$0	Indeterminable Increase		
Revenue Fund(s)	General Fund & Agency Income			
Expenditures*	$0	$1,000,000 to $2,500,000	Indeterminable Increase	
Funding Source(s)	General Fund			
Appropriations*	$0	$0	$0	$0
Funding Source(s)	None			

***Expenditure = Cost of bill** ***Appropriation = Authorized funding to cover cost of bill**

METHODOLOGY:

This bill requires data brokers operating in the state to register annually with the Secretary of State, which includes paying a $300 fee and providing detailed information about their data practices, including the types of data collected, security breaches, and policies regarding minors. It also requires the Secretary of State to establish and maintain a public, searchable online registry of these data brokers. Additionally, the bill imposes strict data protection standards, requiring brokers to implement security programs, employee training, and breach response protocols. Violations of the law would result in civil penalties and be considered deceptive trade practices.

The Department of State indicates that while the bill could generate indeterminable revenue from registration fees, it would impose significant costs on the agency. The office lacks the internal resources to develop and maintain the required online registration system or the staff to draft the necessary administrative rules. As a result, these tasks would need to be outsourced, with estimated costs ranging from $1 million to $2.5 million.

This could possibly result in an increase in civil cases in the Superior Court, however, there is no way to predict how many such actions would occur so any such increase is indeterminable. The Judicial Branch has provided average cost information for civil cases in the Superior Court:

NH Judicial Branch Average Civil Case Estimates

Judicial Branch Average Cost	FY 2026	FY 2027
Superior Court Complex Civil Case	$1,283	$1,342
Superior Court Routine Civil Case	$476	$495

Common Civil Case Fees

Superior Court Fees	As of 7/1/2025
Original Entry Fee	$325
Third-Party Claim	$325
Motion to Reopen	$195

AGENCIES CONTACTED:

Department of State, Judicial Branch, and Department of Justice