19.1041.01000

Sixty-sixth
Legislative Assembly
of North Dakota

HOUSE BILL NO. 1524

Introduced by

Representatives Beadle, Bosch, Mock, Toman

Senators Davison, Meyer, Robinson

A BILL for an Act to create and enact chapter 51-30.1 of the North Dakota Century Code, relating to the regulation of data brokers; and to provide a penalty.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. Chapter 51-30.1 of the North Dakota Century Code is created and enacted as follows:

51-30.1-01. Definitions.

As used in this chapter:

1. "Biometric data" means data generated from measurements or technical analysis of human body characteristics used to identify or authenticate the consumer. The term includes a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
2. "Consumer" means an individual residing in this state.
3. "Data broker" means a business, or unit of a business, separately or together, which knowingly collects and sells or which licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.
4. "Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
5. "Personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:
   a. Name;
   b. Address;
   c. Date of birth;

d. Place of birth;

e. Mother's maiden name;

f. Unique biometric data;

g. Name or address of a member of the consumer's immediate family or household;

h. Social security number or other government-issued identification number; or

i. Other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

6. "Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, which compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by a data collector.

51-30.1-02. Registration - Penalty.

1. Annually, before February first following a year in which a person meets the definition of data broker, a data broker shall:

a. Register with the secretary of state;

b. Pay a registration fee of one hundred dollars; and

c. Provide the following information:

(1) The name and primary physical, electronic mail, and internet addresses of the data broker;

(2) If the data broker permits a consumer to opt-out of the data broker's collection of personal information, opt-out of the data broker's databases, or opt out of certain sales of data:

(a) The method for requesting an opt-out;

(b) If the opt-out applies only to certain activities or sales, which activities or sales; and

(c) Whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(3) A statement specifying the data collection, database, or sales activity from which a consumer may not opt-out;

(4) A statement whether the data broker implements a purchaser credentialing process;

(5) The number of data broker security breaches the data broker has experienced during the previous year, and if known, the total number of consumers affected by the breaches;

(6) If the data broker has actual knowledge the data broker possesses the personal information of minors, a separate statement detailing the data collection practice, database, sales activity, and opt-out policy applicable to the personal information of a minor; and

(7) Any additional information or explanation the data broker chooses to provide concerning the data broker's data collection practices.

2. A data broker that fails to register under this subsection is subject to a civil penalty of fifty dollars for each day, not to exceed a total of ten thousand dollars for each year, the data broker fails to register.

51-30.1-03. Comprehensive information security program.

1. A data broker shall develop, implement, and maintain a comprehensive information security program written in one or more readily accessible parts which contains administrative, technical, and physical safeguards appropriate to the:

a. Size, scope, and type of business of the data broker obligated to safeguard the personal information under the comprehensive information security program;

b. Amount of resources available to the data broker;

c. Amount of stored data; and

d. Need for security and confidentiality of personal information.

2. A data broker shall adopt safeguards in the comprehensive security program which are consistent with the safeguards for protection of personal information and information of a similar character set forth in federal regulations applicable to the data broker.

3. A comprehensive information security program must include:

a. Designation of one or more employees to maintain the program;

b. Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information, and a process for evaluating and improving, as necessary, the effectiveness of the safeguards for limiting the risks, including:

(1) Ongoing employee training, including training for temporary and contract employees;

(2) Employee compliance with policies and procedure requirements; and

(3) Means for detecting and preventing security system failures;

c. Security policies for employees relating to the storage, access, and transportation of records containing personal information outside business premises;

d. Disciplinary measures for violations of the comprehensive information security program rules;

e. Measures to prevent a terminated employee from accessing records containing personal information;

f. Supervision of service providers, by:

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

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

g. Reasonable restrictions on physical access to records containing personal information and storage of the records and data in a locked facility, storage area, or container;

h. Regular monitoring to ensure the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit risks;

i. Regular review of the scope of the security measures at least annually or if there is a material change in business practices which may reasonably implicate the security or integrity of records containing personal information; and

j. Documentation of responsive actions taken in connection with any incident involving a breach of security and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

4. A comprehensive information security program required by this section must have, at minimum and to the extent technically feasible, the following elements:

a. Secure user authentication protocols, as follows:

(1) An authentication protocol that has the following features:

(a) Control of user identifications and other identifiers;

(b) A reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(c) Control of data security passwords to ensure 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 active users and active user accounts only; and

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

(2) An authentication protocol providing a higher level of security than the features specified in paragraph 1.

b. Secure access control measures that:

(1) Restrict access to records and files containing personal information to those who need the information to perform job duties; and

(2) Assign to each individual with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, which are reasonably designed to maintain the integrity of the security of the access controls, or a protocol that provides a higher degree of security;

c. Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly, or a protocol that provides a higher degree of security;

d. Reasonable monitoring of systems for unauthorized use of or access to personal information;

e. Encryption of all personal information stored on a laptop or other portable device, or a protocol that provides a higher degree of security;

f. For files containing personal information on a system connected to the internet, reasonably up-to-date firewall protection and operating system security patches reasonably designed to maintain the integrity of the personal information, or a protocol that provides a higher degree of security;

g. Reasonably up-to-date versions of system security agent software that include malware protection and reasonably up-to-date patches and virus definitions, or a version of the software that can be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis, or a protocol that provides a higher degree of security; and

h. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

51-30.1-04. Enforcement - Powers - Remedies - Penalties.

The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.