19.0780.03004
Title.

Prepared by the Legislative Council staff for
Representative Kasper
February 11, 2019

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1485

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact chapter 51-37 of the North Dakota Century Code, relating to protection against the disclosure of personal information; to provide for a legislative management study; to provide a penalty; and to provide an effective date.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. Chapter 51-37 of the North Dakota Century Code is created and enacted as follows:

51-37-01. Definitions.

For purposes of this chapter:

1. "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity.

2. "Business associate" has the meaning set forth in title 45, Code of Federal Regulations, part 160, section 103.

3. "Business purpose" means the processing of personal data for the controller's or the controller's processor's operational purposes, or other notified purposes, provided that the processing of personal data must be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected. The term includes:

   a. Auditing related to a current interaction with the consumer and concurrent transactions, including counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

   b. Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

   c. Identifying and repairing errors that impair existing or intended functionality.

   d. Short-term, transient use, provided the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including the contextual customization of ads shown as part of the same interaction.

e. Maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing.

f. Undertaking internal research for technological development.

g. Authenticating a consumer's identity.

4. "Child" means an individual under thirteen years of age.

5. "Consent" means a clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

6. "Consumer" means an individual who is a North Dakota resident. The term does not include an owner, director, sole proprietor, employee, or contractor of a business acting in that role.

7. "Controller" means a person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

8. "Covered entity" has the same meaning set forth in title 45, Code of Federal Regulations, part 160, section 103.

9. "Data broker" means a business, or unit of a business, separately or together, which knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

a. Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker.

b. The phrase "sells or licenses" does not include:

(1) A one-time or occasional sale of assets that is not part of the ordinary conduct of the business.

(2) A sale or license of data that is merely incidental to the business.

10. "Deidentified data" means:

a. Data that cannot be linked to a known individual without additional information kept separately; or

b. Data that has been modified to a degree that the risk of reidentification is small, which is subject to a public commitment by the controller not to attempt to reidentify the data, and to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

11. "Developer" means a person that creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

12. "Direct marketing" means communication with a consumer by a third party, other than the original controller or processor, for advertising purposes or to market goods.

13. "Health care facility" means a hospital, clinic, nursing home, laboratory, office, or similar place where a health care provider provides health care to patients.

14. "Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information.

15. "Health care provider" means a person who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession.

16. "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, specific geolocation data, or a hashed or online identifier.

17. "Personal data" means information that is linked or reasonably linked to an identified or identifiable individual. The term does not include deidentified data or publicly available information. For these purposes, "publicly available information" means information that is lawfully made available from federal, state, or local government records.

18. "Process" or "processing" means collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

19. "Processor" means a person that processes personal data on behalf of the controller.

20. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning the individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

21. "Protected health information" has the same meaning set forth in title 45, Code of Federal Regulations, part 160, section 103.

22. "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of the personal data in the future.

23. "Sale", "sell", or "sold" means the exchange of personal data for monetary consideration by the controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties. The term does not include:

a. The disclosure of personal data to a processor who processes the personal data on behalf of the controller.

b. The disclosure of personal data to a third party with which the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller.

c. The disclosure or transfer of personal data to an affiliate of the controller.

d. 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 in which the third party assumes control of all or part of the controller's assets.

24. "Sensitive data" means:

a. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation.

b. The processing of genetic or biometric data for the purpose of uniquely identifying an individual.

c. The personal data of a known child.

25. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across nonaffiliated websites, applications, or online services to predict user preferences or interests. The term does not include advertising to a consumer based upon the consumer's current visit to a website, application, or online service, or in response to the consumer's request for information or feedback.

26. "Third party" means a person, public authority, agency, or body other than the consumer, controller, or an affiliate of the processor of the controller.

27. "Verified request" means the process through which a consumer may submit a request to exercise a right set forth in this chapter, and by which a controller can reasonably authenticate the request and the consumer making the request using commercially reasonable means.

51-37-02. Scope.

1. This chapter applies to legal entities that conduct business in the state or produce products or services intentionally targeted to residents of the state, and satisfy one or more of the following:

a. Controls or processes data of one hundred thousand consumers or more; or

b. Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more.

2. This chapter does not apply to:

   a. State and local governments.

   b. Municipal corporations.

   c. Protected health information protected under the federal Health Insurance Portability and Accountability Act of 1996 [Pub. L. 104-191; 110 Stat. 1936; 29 U.S.C. 1181 et seq.] and the federal Health Information Technology for Economic and Clinical Health Act [Pub. L. 111-5, 123 Stat. 226, 42 U.S.C. 201 et seq.].

   d. Health care information collected by a health care facility or health care provider.

   e. Identifiable private information collected as part of a clinical trial subject to the federal policy for the protection of human subjects pursuant to good clinical practice guidelines issued by the international council for harmonization or pursuant to human subject protection requirements of the United States food and drug administration.

   f. The sale of personal data to or from a consumer reporting agency if the data is reported in, or used to generate, a consumer report as defined by 15 U.S.C. 1681a(d), and use of the data is limited by the federal Fair Credit Reporting Act [Pub. L. 90-321; 15 U.S.C. 1681 et seq.].

   g. Personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act of 1999 [Pub. L. 106-102; 113 Stat. 1436], if it is in conflict with that law.

   h. Personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994 [Pub. L. 103-322; 18 U.S.C. 2721 et seq.], if the collection, processing, sale, or disclosure is in compliance with that law.

   i. Data maintained for employment records purposes.

51-37-03. Responsibilities.

1. Controllers are responsible for meeting the obligations set forth under this chapter.

2. Processors are responsible under this chapter for adhering to the instructions of the controller and assisting the controller to meet the controller's obligations under this chapter.

3. Processing by a processor is governed by a contract between the controller and the processor. The contract is binding on the processor and sets out the processing instructions to which the processor is bound.

51-37-04. Consumer rights.

1. Controllers shall facilitate verified requests to exercise the consumer rights set forth in subsections 2 through 7.

2. Upon a verified request from a consumer, a controller shall confirm whether personal data concerning the consumer is being processed by the controller, including whether the personal data is sold to data brokers, and, when personal data concerning the consumer is being processed by the controller, provide access to the personal data that the controller maintains in identifiable form concerning the consumer.

   a. Upon a verified request from a consumer, a controller shall provide a copy of the personal data that the controller maintains in identifiable form undergoing processing. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. If the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information must be provided in a commonly used electronic form.

   b. This subsection may not affect the rights or freedoms of others adversely.

3. Upon a verified request from a consumer, the controller, without undue delay, shall correct inaccurate personal data that the controller maintains in identifiable form concerning the consumer. Taking into account the business purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement when appropriate.

4. a. Upon a verified request from a consumer, a controller shall delete the consumer's personal data the controller maintains in identifiable form without undue delay if one of the following grounds applies:

      (1) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer;

      (2) For processing that requires consent under subsection 3 of section 51-37-06, the consumer withdraws consent to processing and there are no business purposes for the processing;

      (3) The consumer objects to the processing pursuant to subsection 7 and:

         (a) There are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public, for which the processing is necessary; or

         (b) The processing is for direct marketing purposes;

      (4) The personal data has been unlawfully processed; or

      (5) The personal data must be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject.

   b. If the controller is obliged to delete personal data that the controller maintains in identifiable form under this section which has been disclosed to third parties by the controller, including data brokers that

received the personal data through a sale, the controller shall take reasonable steps, which may include technical measures, to inform other controllers of which it is aware that are processing the personal data, and that received the personal data from the controller or are processing the personal data on behalf of the controller, that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must take into account available technology and cost of implementation.

c. This subsection does not apply to the extent processing is necessary:

(1) For exercising the right of free speech.

(2) For compliance with a legal obligation which requires processing of personal data by federal, state, or local law or regulation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(3) For reasons of public interest in the area of public health, when the processing is subject to suitable and specific measures to safeguard the rights of the consumer; and is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

(4) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, when the deletion of the personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing.

(5) For the establishment, exercise, or defense of legal claims.

(6) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity.

5. a. Upon a verified request from a consumer, the controller shall restrict processing of personal data the controller maintains in identifiable form if the purpose for which the personal data is:

(1) Not consistent with a purpose for which the personal data was collected;

(2) Not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or

(3) Unlawful.

b. If personal data is subject to a restriction of processing under this subsection, the personal data must be processed, with the exception of storage, only:

(1) With the consumer's consent;

(2) For the establishment, exercise, or defense of legal claims;

(3) For the protection of the rights of another natural or legal person;

(4) For reasons of important public interest under federal, state, or local law;

(5) To provide products or services requested by the consumer; or

(6) For another purpose set forth in subdivision d of subsection 4.

c. A consumer who has obtained restriction of processing pursuant to this subsection must be informed by the controller before the restriction of processing is lifted.

6. a. Upon a verified request from a consumer, the controller shall provide the consumer, if technically feasible and commercially reasonable, any personal data the controller maintains in identifiable form concerning the consumer which the consumer has provided to the controller in a structured, commonly used, and machine-readable format if:

(1) The processing of the personal data requires consent under subsection 3 of section 51-37-06, the processing of the personal data is necessary for the performance of a contract to which the consumer is a party, or to take steps at the request of the consumer prior to entering a contract; and

(2) The processing is carried out by automated means.

b. Requests for personnel data under this subsection must be without prejudice to the other rights granted in this chapter.

c. The rights provided in this subsection do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not affect the rights of others adversely.

7. a. A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of personal data concerning the consumer.

b. If a consumer objects to direct marketing, which includes the sale of personal data concerning the consumer to third parties for direct marketing purposes or profiling to the extent it is related to the direct marketing and targeted advertising, the controller may not process the personal data subject to the objection for that purpose and must communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for those purposes to any third parties to which the controller sold the consumer's personal data for those purposes. Third parties shall honor objection requests pursuant to this subsection received from third-party controllers.

c. If a consumer objects to processing for any purpose, other than direct marketing, the controller may continue processing the personal data subject to the objection if the controller can demonstrate a compelling

business purpose to process the personal data, or if another exemption in this chapter applies.

8. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subsections 3, 4, or 5 to each third-party recipient to which the controller knows the personal data has been disclosed, including third parties that received the data through a sale, within one year preceding the verified request unless this proves functionally impractical, technically infeasible, or involves disproportionate effort. The controller shall inform the consumer about third-party recipients or categories, if any, if the consumer requests the information.

9. A controller shall provide information on action taken on a verified request under subsections 2 through 7 without undue delay and in any event within thirty days of receipt of the request. The period may be extended by sixty additional days when reasonably necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any extension within thirty days of receipt of the request, together with the reasons for the delay. If the consumer makes the request by electronic means, the information must be provided by electronic means when possible, unless otherwise requested by the consumer.

   a. If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

   b. Information provided under this section must be provided by the controller free of charge to the consumer. If requests from a consumer are manifestly unfounded or excessive, in particular because of the repetitive character, the controller either may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

   c. If the controller has reasonable doubts concerning the identity of the consumer making a request under subsections 2 through 7, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

51-37-05. Transparency.

1. A controller must be transparent and accountable for the controller's processing of personal data, by making available in a form reasonably accessible to consumers a clear, meaningful privacy notice that includes:

   a. The categories of personal data collected by the controller;

   b. The purposes for which the categories of personal data is used and disclosed to third parties, if any;

   c. The rights consumers may exercise pursuant to section 51-37-04, if any;

d. The categories of personal data the controller shares with third parties, if any; and

e. The categories of third parties, if any, with which the controller shares personal data.

2. If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted marketing, the controller shall disclose the processing, as well as the manner in which a consumer may exercise the right to object to the processing, in a clear and conspicuous manner.

51-37-06. Documented risk assessments.

1. A controller shall conduct, to the extent not previously conducted, a risk assessment of each of the controller's processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. Risk assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is to be processed.

2. Risk assessments conducted under subsection 1 must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce those risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, must factor into this assessment by the controller.

3. If the risk assessment conducted under subsection 1 determines the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller only may engage in the processing with the consent of the consumer or if another exemption under this chapter applies. To the extent the controller seeks consumer consent for processing, the consent must be as easy to withdraw as to give.

4. Processing for a business purpose is permissible unless:

   a. It involves the processing of sensitive data; and

   b. The risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.

5. The controller shall make the risk assessment available to the attorney general upon request. Risk assessments are confidential.

51-37-07. Deidentified data.

A controller or processor that uses deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and shall take appropriate steps to address any breaches of contractual commitments.

51-37-08. Exemptions.

1. The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

   a. Comply with federal, state, or local laws, rules, or regulations;

   b. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

   c. Cooperate with law enforcement agencies concerning conduct or activity the controller or processor reasonably and in good faith believes may violate federal, state, or local law;

   d. Investigate, exercise, or defend legal claims;

   e. Prevent or detect identity theft, fraud, or other criminal activity or verify identities;

   f. Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer before entering a contract;

   g. Protect the vital interests of the consumer or of another individual;

   h. Perform a task carried out in the public interest or in the exercise of official authority vested in the controller; or

   i. Process personal data of a consumer for one or more specific purposes when the consumer has given their consent to the processing.

2. The obligations imposed on controllers or processors under this chapter do not apply if compliance by the controller or processor with this chapter would violate an evidentiary privilege under state law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under state law as part of a privileged communication.

3. A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter is not in violation of this chapter if the recipient processes the personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor is likewise not liable under this chapter for the obligations of a controller or processor to which it provides services.

4. This chapter does not require a controller or processor to:

a. Reidentify deidentified data.

b. Retain, link, or combine personal data concerning a consumer the controller or processor would not otherwise retain, link, or combine in the ordinary course of business.

c. Comply with a request to exercise any of the rights under subsections 2 through 7 of section 51-37-04 if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

5. Obligations imposed on controllers and processors under this chapter do not:

a. Adversely affect the rights or freedoms of any persons; or

b. Apply to the processing of personal data by an individual in the course of a purely personal or household activity.

51-37-09. Liability.

1. This chapter does not serve as the basis for a private right of action under this chapter or any other law.

2. If more than one controller or processor, or both a controller and a processor, involved in the same processing, are in violation of this chapter, the liability is allocated among the parties according to principles of comparative fault, unless the liability is otherwise allocated by contract among the parties.

51-37-10. Enforcement.

1. A violation of this chapter is an unfair or deceptive act in trade or commerce and an unfair method of competition under title 51.

2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter.

3. A controller or processor is in violation of this chapter if the controller or processor fails to cure any alleged violation of sections 51-37-04 through 51-37-08 within thirty days after receiving notice of alleged noncompliance. A controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars for each violation or seven thousand five hundred dollars for each intentional violation.

51-37-11. Preemption.

1. This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by a controller or processor.

2. This chapter is intended to supplement federal and state law and do not apply if such application is preempted by or in conflict with federal law.

SECTION 2. LEGISLATIVE MANAGEMENT STUDY - CONSUMER PERSONAL DATA DISCLOSURES. During the 2019-20 interim, the legislative management shall study protections, enforcement, and remedies regarding the disclosure of consumers' personal data. The study must include a review of privacy laws of other states and applicable federal law. The legislative management shall report its findings and recommendations, together with any legislation required to implement the recommendations, to the sixty-seventh legislative assembly.

SECTION 3. EFFECTIVE DATE. Section 1 of this Act becomes effective on August 1, 2021."

Renumber accordingly