SENATE
STATE OF MINNESOTA
NINETY-THIRD SESSION

S.F. No. 2915

(SENATE AUTHORS: WESTLIN)

DATE	D-PG	OFFICIAL STATUS
03/15/2023	1793	Introduction and first reading Referred to Commerce and Consumer Protection

A bill for an act

relating to consumer data privacy; giving various rights to consumers regarding personal data; placing obligations on certain businesses regarding consumer data; providing for enforcement by the attorney general; proposing coding for new law in Minnesota Statutes, chapter 13; proposing coding for new law as Minnesota Statutes, chapter 325O.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[13.6505] ATTORNEY GENERAL DATA CODED ELSEWHERE.**

Subdivision 1. **Scope.** The sections referred to in this section are codified outside this chapter. Those sections classify attorney general data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. **Data privacy and protection assessments.** A data privacy and protection assessment collected or maintained by the attorney general is classified under section 325O.08.

Sec. 2. **[325O.01] CITATION.**

This chapter may be cited as the "Minnesota Consumer Data Privacy Act."

Sec. 3. **[325O.02] DEFINITIONS.**

(a) For purposes of this chapter, the following terms have the meanings given.

(b) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, that other legal entity. For these purposes, "control" or "controlled" means: ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(c) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 325O.05, subdivision 1, paragraphs (b) to (e), is being made by the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(d) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, including a face, fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. Biometric data does not include:

(1) a digital or physical photograph;

(2) an audio or video recording; or

(3) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(e) "Child" has the meaning given in United States Code, title 15, section 6501.

(f) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, consent cannot be obtained through a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice. A consumer may revoke consent previously given, consistent with this chapter.

(g) "Consumer" means a natural person who is a Minnesota resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

(h) "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(i) "Decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

(j) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller that possesses the data:

(1) takes reasonable measures to ensure that the data cannot be associated with a natural person;

(2) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and

(3) contractually obligates any recipients of the information to comply with all provisions of this paragraph.

(k) "Delete" means to remove or destroy information such that it is not maintained in human- or machine-readable form and cannot be retrieved or utilized in the course of business.

(l) "Genetic information" has the meaning given in section 13.386, subdivision 1.

(m) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

(n) "Known child" means a person under circumstances where a controller has actual knowledge of, or willfully disregards, that the person is under 18 years of age.

(o) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information. For purposes of this paragraph, "publicly available information" means information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, and (2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(p) "Process" or "processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(q) "Processor" means a natural or legal person who processes personal data on behalf of a controller.

(r) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(s) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(t) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. Sale does not include the following:

(1) the disclosure of personal data to a processor who processes the personal data on behalf of the controller;

(2) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer;

(3) the disclosure or transfer of personal data to an affiliate of the controller;

(4) the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience; or

(5) the disclosure or transfer of personal data to a third party as an asset that is part of a completed or proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(u) Sensitive data is a form of personal data. "Sensitive data" means:

(1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status;

(2) the processing of biometric data or genetic information;

(3) the personal data of a known child; or

(4) specific geolocation data.

(v) "Specific geolocation data" means information derived from technology, including but not limited to global positioning system level latitude, longitude, or altitude coordinates; cellular phone system coordinates; internet protocol device addresses; or other mechanisms that can be used to identify a specific street or postal address associated with the consumer. Specific geolocation data excludes the content of communications and the contents of databases containing name and address information which are accessible to the public as authorized by law.

(w) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. It does not include advertising:

(1) based on activities within a controller's own websites or online applications;

(2) based on the context of a consumer's current search query or visit to a website or online application; or

(3) to a consumer in response to the consumer's request for information or feedback.

(x) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

(y) "Trade secret" has the meaning given in section 325C.01, subdivision 5.

Sec. 4. **[325O.03] SCOPE; EXCLUSIONS.**

Subdivision 1. **Scope.** (a) This chapter applies to legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota, and that satisfy one or more of the following thresholds:

(1) during a calendar year, controls or processes personal data of 100,000 consumers or more; or

(2) derives over 25 percent of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.

(b) A controller or processor acting as a technology provider under section 13.32 shall comply with both this chapter and section 13.32, except that, when the provisions of section 13.32 conflict with this chapter, section 13.32 prevails.

Subd. 2. **Exclusions.** (a) This chapter does not apply to the following entities or types of information:

(1) a government entity, as defined by section 13.02, subdivision 7a;

(2) a federally recognized Indian tribe;

(3) information that meets the definition of:

(i) protected health information as defined by and for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(ii) health records, as defined in section 144.291, subdivision 2;

(iii) patient identifying information for purposes of Code of Federal Regulations, title 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;

(iv) identifiable private information for purposes of the federal policy for the protection of human subjects, Code of Federal Regulations, title 45, part 46; 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 Harmonisation; the protection of human subjects under Code of Federal Regulations, title 21, parts 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this paragraph;

(v) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, Public Law 99-660, and related regulations; or

(vi) patient safety work product for purposes of Code of Federal Regulations, title 42, part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;

(4) information that is derived from any of the health care-related information listed in clause (3), but that has been deidentified in accordance with the requirements for deidentification set forth in Code of Federal Regulations, title 45, part 164;

(5) information originating from, and intermingled to be indistinguishable with, any of the health care-related information listed in clause (3) that is maintained by:

(i) a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(ii) a health care provider, as defined in section 144.291, subdivision 2; or

(iii) a program or a qualified service organization as defined by Code of Federal Regulations, title 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;

(6) information used only for public health activities and purposes as described in Code of Federal Regulations, title 45, section 164.512;

(7) an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data 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, as defined in United States Code, title 15, section 1681a(f), by a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who provides information for use in a consumer report, as defined in United States Code, title 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,

title 15, section 1681b, except that information is only excluded under this paragraph to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the federal Fair Credit Reporting Act, United States Code, title 15, sections 1681 to 1681x, and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act;

(8) personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

(9) personal data collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, United States Code, title 18, sections 2721 to 2725, if the collection, processing, sale, or disclosure is in compliance with that law;

(10) personal data regulated by the federal Family Educations Rights and Privacy Act, United States Code, title 20, section 1232g, and its implementing regulations;

(11) personal data collected, processed, sold, or disclosed pursuant to the federal Farm Credit Act of 1971, as amended, United States Code, title 12, sections 2001 to 2279cc, and its implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection, processing, sale, or disclosure is in compliance with that law;

(12) data collected or maintained:

(i) in the course of an individual acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of that business if it is collected and used solely within the context of that role;

(ii) as the emergency contact information of an individual under item (i) if used solely for emergency contact purposes; or

(iii) that is necessary for the business to retain to administer benefits for another individual relating to the individual under item (i) if used solely for the purposes of administering those benefits;

(13) personal data collected, processed, sold, or disclosed pursuant to the Minnesota Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505; or

(14) data collected, processed, sold, or disclosed as part of a payment-only credit, check, or cash transaction where no data about consumers, as defined in section 325O.02, are retained.

(b) Controllers that are in compliance with the Children's Online Privacy Protection Act, United States Code, title 15, sections 6501 to 6506, and its implementing regulations, shall be deemed compliant with any obligation to obtain parental consent under this chapter.

Sec. 5. **[325O.04] RESPONSIBILITY ACCORDING TO ROLE.**

(a) Controllers and processors are responsible for meeting their respective obligations established under this chapter.

(b) Processors are responsible under this chapter for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. Such assistance shall include the following:

(1) taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 325O.05; and

(2) taking into account the nature of processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 325E.61, and shall provide information to the controller necessary to enable the controller to conduct and document any data privacy and protection assessments required by section 325O.08.

(c) Notwithstanding the instructions of the controller, a processor shall:

(1) ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

(2) engage a subcontractor only (i) after providing the controller with an opportunity to object, and (ii) pursuant to a written contract in accordance with paragraph (e) that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(d) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between the controller and the processor to implement such measures.

(e) Processing by a processor shall be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties. In addition, the contract shall include the requirements imposed by this paragraph, paragraphs (c) and (d), as well as the following requirements:

(1) at the choice of the controller, the processor shall 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;

(2) the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and

(3) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this chapter. The auditor must use an appropriate and accepted control standard or framework and audit procedure for such audits as applicable, and shall provide a report of such audit to the controller upon request.

(f) In no event shall any contract relieve a controller or a processor from the liabilities imposed on them by virtue of their roles in the processing relationship under this chapter.

(g) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions, or that fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to such processing.

Sec. 6. **[325O.05] CONSUMER PERSONAL DATA RIGHTS.**

Subdivision 1. **Consumer rights provided.** (a) Except as provided in this chapter, a controller must comply with a request to exercise the consumer rights provided in this subdivision.

(b) A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing.

(c) A consumer has the right to correct inaccurate personal data concerning the consumer, taking into account the nature of the personal data and the purposes of the processing of the personal data.

(d) A consumer has the right to delete personal data concerning the consumer.

(e) A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(f) A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

(g) If a consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of such profiling and be informed of the reason that the profiling resulted in the decision, as well as the actions that the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The consumer has the right to review the customer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

Subd. 2. **Exercising consumer rights.** (a) A consumer may exercise the rights set forth in this section by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise.

(b) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child may exercise the rights of this chapter on the child's behalf.

(c) In the case of processing personal data concerning a consumer legally subject to guardianship or conservatorship under sections 524.5-101 to 524.5-502, the guardian or the conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

Subd. 3. **Universal opt-out mechanisms.** (a) A controller must allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. The platform, technology, or mechanism must:

(1) not unfairly disadvantage another controller;

(2) not make use of a default setting, but require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of any processing of the consumer's personal data;

(3) be consumer-friendly and easy to use by the average consumer;

(4) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation; and

(5) enable the controller to accurately determine whether the consumer is a Minnesota resident and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

(b) If a consumer's opt-out request is exercised through the platform, technology, or mechanism required under paragraph (a), and the 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 must comply with the consumer's opt-out preference signal but may also notify the consumer of the conflict and provide the consumer a choice to confirm the controller-specific privacy setting or participation in such program.

(c) The platform, technology, or mechanism required under paragraph (a) is subject to the requirements of subdivision 4.

Subd. 4. **Controller response to consumer requests.** (a) Except as provided in this chapter, a controller must comply with a request to exercise the rights pursuant to subdivision 1.

(b) A controller must provide one or more secure and reliable means for consumers to submit a request to exercise their rights under this section. These means must take into account the ways in which consumers interact with the controller and the need for secure and reliable communication of the requests.

(c) A controller may not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this section.

(d) A controller must comply with a request to exercise the right in subdivision 1, paragraph (f), as soon as feasibly possible, but no later than 15 days of receipt of the request.

(e) A controller must inform a consumer of any action taken on a request under subdivision 1 without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(f) If a controller does not take action on a consumer's request, the controller must inform the consumer without undue delay and at the latest within 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subdivision 3.

(g) Information provided under this section must be provided by the controller free of charge, up to twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a reasonable fee to cover the administrative costs of complying with the request, or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(h) A controller is not required to comply with a request to exercise any of the rights under subdivision 1, if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to authenticate the request. A controller is not required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller must notify the person who made the request that the request was denied due to the controller's belief that the request was fraudulent and state the controller's basis for that belief.

(i) In response to a consumer request under subdivision 1, a controller must not disclose the following information about a consumer, but must instead inform the consumer with sufficient particularity that it has collected that type of information:

(1) Social Security number;

(2) driver's license number or other government-issued identification number;

(3) financial account number;

(4) health insurance account number or medical identification number;

(5) account password, security questions, or answers; or

(6) biometric data.

(j) In response to a consumer request under subdivision 1, a controller is not required to reveal any trade secret.

Subd. 5. **Appeal process required.** (a) A controller must establish an internal process whereby a consumer may appeal a refusal to take action on a request to exercise any of the rights under subdivision 1 within a reasonable period of time after the consumer's receipt of the notice sent by the controller under subdivision 3, paragraph (f).

(b) The appeal process must be conspicuously available. The process must include the ease of use provisions in subdivision 3 applicable to submitting requests.

(c) Within 30 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any such extension within 30 days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an e-mail address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to paragraph (c), the controller must clearly and prominently provide the consumer with information about how to file a complaint with the Office of the Attorney General. The controller must maintain records of all such appeals and the controller's responses for at least 24 months and shall, upon request by a consumer or by the attorney general, compile and provide a copy of the records to the attorney general.

Sec. 7. **[325O.06] PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA.**

(a) This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:

(1) reidentify deidentified data;

(2) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data; or

(3) comply with an authenticated consumer request to access, correct, delete, or port personal data pursuant to section 325O.05, subdivision 1, if all of the following are true:

(i) the controller is not reasonably capable of associating the request with the personal data, or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(iii) the controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(b) The rights contained in section 325O.05, subdivision 1, do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(c) A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject, and must take appropriate steps to address any breaches of contractual commitments.

(d) A processor or third party must not attempt to identify the subjects of deidentified or pseudonymous data without the express authority of the controller that caused the data to be deidentified or pseudonymized.

(e) A controller, processor, or third party must not attempt to identify the subjects of data that has been collected with only pseudonymous identifiers.

Sec. 8. **[325O.07] RESPONSIBILITIES OF CONTROLLERS.**

Subdivision 1. **Transparency obligations.** (a) Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) the categories of personal data processed by the controller;

(2) the purposes for which the categories of personal data are processed;

(3) an explanation of the rights contained in section 325O.05 and how and where consumers may exercise those rights, including how a consumer may appeal a controller's action with regard to the consumer's request;

(4) the categories of personal data that the controller sells to or shares with third parties, if any;

(5) the categories of third parties, if any, with whom the controller sells or shares personal data;

(6) the controller's contact information, including an active email address or other online mechanism that the consumer may use to contact the controller;

(7) the length of time the controller intends to retain each category of personal data or the criteria used to determine the length of time the controller intends to retain categories of personal data;

(8) if a controller engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer:

(i) what decisions are subject to such profiling;

(ii) how profiling is used in the decision-making process, including the role of human involvement, if any; and

(iii) the benefits and potential consequences of the decision concerning the consumer; and

(9) the date the privacy notice was last updated.

(b) If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, it must disclose such processing in the privacy notice and provide access to a clear and conspicuous method outside the privacy notice for a consumer to opt out of the sale, processing, or profiling. This method may include but is not limited to an internet hyperlink clearly labeled

"Your Opt-Out Rights" or "Your Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.

(c) The privacy notice must be made available to the public in each language in which the controller provides a product or service that is subject to the privacy notice or carries out activities related to such product or service.

(d) The controller must provide the privacy notice in a manner that is reasonably accessible to and usable by individuals with disabilities.

(e) Before a controller makes a material change to its privacy notice or practices, the controller must notify each consumer affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for each consumer to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to each affected consumer, taking into account available technology and the nature of the relationship.

(f) A controller is not required to provide a separate Minnesota-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this section.

(g) The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website home page or on a mobile application's app store page or download page. A controller that maintains an application on a mobile or other device shall also include a hyperlink to the privacy notice in the application's settings menu. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including but not limited to mail.

Subd. 2. **Use of data.** (a) A controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which such data are processed.

(b) A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.

(c) Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(d) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

(e) Except as otherwise provided in this act, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the requirement of the Children's Online Privacy Protection Act, United States Code, title 15, sections 6501 to 6506, and its implementing regulations.

(f) A controller shall provide an effective mechanism for a consumer, or, in the case of the processing of personal data concerning a known child, the child's parent or lawful guardian, to revoke previously given consent under this subdivision. The mechanism provided shall be at least as easy as the mechanism by which the consent was previously given. Upon revocation of consent, a controller shall cease to process the applicable data as soon as practicable, but not later than 15 days after the receipt of such request.

(g) A controller may not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where the consumer is a known child between the ages of 13 and 16.

Subd. 3. **Nondiscrimination.** (a) A controller shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: housing, employment, credit, or education; or the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.

(b) A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subdivision does not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(c) A controller may not sell personal data to a third-party controller as part of a bona fide loyalty, rewards, premium features, discounts, or club card program under paragraph (b) unless:

(1) the sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled;

(2) the sale of personal data to third parties is clearly disclosed in the terms of the program; and

(3) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

Subd. 4. **Waiver of rights unenforceable.** Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable.

Sec. 9. **[325O.08] DATA PRIVACY AND PROTECTION ASSESSMENTS.**

(a) A controller must conduct, document, and maintain a data privacy and protection assessment that describes the policies and procedures it has adopted to comply with the provisions of this act. This assessment must include:

(1) the name and contact information for the controller's chief privacy officer or other officer with primary responsibility for directing the policies and procedures implemented to comply with the provisions of this chapter;

(2) a description of the controller's data privacy policies and procedures which ensure compliance with section 325O.07, and any policies and procedures designed to:

(i) reflect the requirements of this act in the design of its systems from their inception;

(ii) identify and provide personal data to a consumer as required by this act;

(iii) maintain the accuracy and integrity of personal data subject to this act;

(iv) prevent the collection of personal data that is not necessary to provide services which have been requested by the consumer;

(v) prevent the retention of personal data that is no longer needed to provide services to the consumer; and

(vi) identify and remediate violations of this act;

(3) a description of the controller's data protection processes and procedures for each of the following processing activities involving personal data:

(i) the processing of personal data for purposes of targeted advertising;

(ii) the sale of personal data;

(iii) the processing of sensitive data;

(iv) any processing activities involving personal data that present a heightened risk of harm to consumers; and

(v) the processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers; and

(4) a description of the data dictionary, metadata catalog, or other means by which the controller maintains its inventory of data that must be managed to exercise its responsibilities under section 325O.05.

(b) A data privacy and protection assessment must take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the personal data are to be processed.

(c) A data privacy and protection assessment 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 such processing, as mitigated by safeguards that can be employed by the controller to reduce such 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 be factored into this assessment by the controller.

(d) The attorney general may request, in writing, that a controller disclose any data privacy and protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data privacy and protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data privacy and protection assessments for compliance with the responsibilities contained in section 325O.07 and with other laws. Data privacy and protection assessments are classified as nonpublic data, as defined by section 13.02, subdivision 9. The disclosure of a data privacy and protection assessment pursuant to a request from the attorney general under this paragraph does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(e) Data privacy and protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under this section if they have a similar scope and effect.

Sec. 10. **[325O.09] LIMITATIONS AND APPLICABILITY.**

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

(1) comply with federal, state, or local laws, rules, or regulations;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(4) investigate, establish, exercise, prepare for, or defend legal claims;

(5) provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(6) take immediate steps to protect an interest that is essential for the life of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity

or security of systems; or investigate, report, or prosecute those responsible for any such action;

(8) assist another controller, processor, or third party with any of the obligations under this paragraph; or

(9) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity which has determined that:

(i) the research is likely to provide substantial benefits that do not exclusively accrue to the controller;

(ii) the expected benefits of the research outweigh the privacy risks; and

(iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(b) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) identify and repair technical errors that impair existing or intended functionality; or

(2) perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party when those internal operations are performed during, and not following, the consumer's relationship with the controller.

(c) The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under Minnesota 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 Minnesota law as part of a privileged communication.

(d) 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 such 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 that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the obligations of the controller or processor from which it receives such personal data.

(e) Obligations imposed on controllers and processors under this chapter shall not:

(1) adversely affect the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment of the United States Constitution; or

(2) apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

(f) Personal data that are processed by a controller pursuant to this section must not be processed for any purpose other than those expressly listed in this section. Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such processing is:

(1) necessary, reasonable, and proportionate to the purposes listed in this section;

(2) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section; and

(3) insofar as possible, taking into account the nature and purpose of processing the personal data, subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in paragraph (f).

(h) Processing personal data solely for the purposes expressly identified in paragraph (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to such processing.

Sec. 11. **[325O.10] ATTORNEY GENERAL ENFORCEMENT.**

(a) In the event that a controller or processor violates this chapter, the attorney general, prior to filing an enforcement action under paragraph (b), must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the attorney general believes the controller or processor has failed to cure any alleged violation, the attorney general may bring an enforcement action under paragraph (b). This paragraph expires January 31, 2026.

(b) The attorney general may bring a civil action against a controller or processor to enforce a provision of this chapter in accordance with section 8.31. If the state prevails in an action to enforce this chapter, the state may, in addition to penalties provided by paragraph (c) or other remedies provided by law, be allowed an amount determined by the court to be the reasonable value of all or part of the state's litigation expenses incurred.

(c) Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation.

Sec. 12. **[325O.11] PREEMPTION OF LOCAL LAW; SEVERABILITY.**

(a) This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local government regarding the processing of personal data by controllers or processors.

(b) If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

Sec. 13. **EFFECTIVE DATE.**

This act is effective July 31, 2024, except that postsecondary institutions regulated by the Office of Higher Education and nonprofit corporations governed by Minnesota Statutes, chapter 317A, are not required to comply with this act until July 31, 2028.