SENATE
STATE OF MINNESOTA
NINETY-FOURTH SESSION

S.F. No. 2940

(SENATE AUTHORS: WESTLIN, Wiklund, Oumou Verbeten and Latz)

DATE	D-PG	OFFICIAL STATUS
03/24/2025	1015	Introduction and first reading Referred to Commerce and Consumer Protection
04/22/2025	3722	Author added Oumou Verbeten
02/26/2026	6418	Author added Latz

A bill for an act

relating to consumer protection; modifying the Minnesota Consumer Data Privacy Act to make consumer health data a form of sensitive data; adding additional protections for sensitive data; amending Minnesota Statutes 2024, sections 325M.11; 325M.12; 325M.16, subdivision 2; 325M.18; 325M.20; proposing coding for new law in Minnesota Statutes, chapter 325M; repealing Minnesota Statutes 2024, section 325M.17.

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

Section 1. Minnesota Statutes 2024, section 325M.11, is amended to read:

325M.11 DEFINITIONS.

(a) For purposes of sections 325M.10 to 325M.21, the following terms have the meanings given.

(b) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity. For purposes of this paragraph, "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 under section 325M.14, subdivision 1, paragraphs (b) to (h), is being made by or rightfully on behalf of the consumer who is entitled to exercise the 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 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 the 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. 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. A consent is not valid when the consumer's indication has been obtained by a dark pattern. A consumer may revoke consent previously given, consistent with sections 325M.10 to 325M.21.

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

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

(i) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.

(j) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(k) "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 an identified or identifiable natural 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 process 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.

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

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

(n) "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, or any other form of spatial or location detection to establish a virtual boundary, with an accuracy of more than three decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system, around the perimeter of a specific physical location or to locate a consumer within the virtual boundary.

(o) "Health care services or supplies" means any service, surgery, procedure, treatment, or product, including medication or medical devices, that a person may use to assess, measure, improve, or learn about a person's past, present, or future mental or physical health.

(p) "Health data" means personal data that identifies a consumer's past, present, or future mental or physical health status. For purposes of this definition, mental or physical health status includes but is not limited to:

(1) individual health conditions, treatments, diseases, or diagnoses;

(2) social, psychological, behavioral, and medical interventions;

(3) health-related surgeries or procedures;

(4) use or purchase of medication;

(5) bodily functions, vital signs, symptoms, or measurements of the information described in this paragraph;

(6) diagnoses or diagnostic testing, treatment, or medication;

(7) biometric data;

(8) genetic information;

(9) specific geolocation data that could reasonably indicate a consumer's seeking or obtaining past, present, or future health care services or supplies;

(10) data that identifies a consumer's seeking or obtaining health care services or supplies in the past, present, or future;

(11) data that identifies a consumer's seeking or obtaining information about health care services or supplies in the past, present, or future; or

(12) any information that is derived or extrapolated from personal data but that is not itself health data that a controller or processor uses by any means, including algorithms, machine learning, or profiling, to associate or identify a consumer with the data described in clauses (1) to (11), such as proxy, derivative, inferred, or emergent data.

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

~~(o)~~ (r) "Known child" means a person under circumstances where a controller has actual knowledge of, or willfully disregards, that the person is under 13 years of age.

~~(p)~~ (s) "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, or (2) a controller has a reasonable basis to believe has lawfully been made available to the general public.

~~(q)~~ (t) "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, including but not limited to the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

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

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

~~(t)~~ (w) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the 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.

~~(u)~~ (x) "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 sharing as defined in this section. 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 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;

(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; or

(6) the exchange of personal data between the producer of a good or service and authorized agents of the producer who sell and service the goods and services, to enable the cooperative provisioning of goods and services by both the producer and the producer's agents.

~~(v)~~ (y) 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 for the purpose of uniquely identifying an individual;

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

(4) specific geolocation data; or

(5) health data.

(z) "Share" or "sharing" means to release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, personal data. Share includes selling as defined in this section. Sharing does not include:

(1) the disclosure of personal data by a controller to a processor when the sharing is to provide goods or services in a manner consistent with the purpose for which the health data was collected and that was disclosed to the consumer;

(2) the disclosure of personal data to a third party with whom the consumer has a direct relationship when:

(i) the disclosure is for purposes of providing a product or service requested by the consumer;

(ii) the controller or processor maintains control and ownership of the data; and

(iii) the third party uses the personal data only as directed by the controller or processor and consistent with the purpose consented to by the consumer; or

(3) 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 or processor's assets and complies with the requirements and obligations in this chapter.

~~(w)~~ (aa) "Specific geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the geographic coordinates of a consumer or a device linked to a consumer with an accuracy of more than three decimal degrees of latitude and longitude or the equivalent in an alternative geographic coordinate system, or a street address derived from the coordinates. Specific geolocation data does not include the content of communications, the contents of databases containing street address information which are accessible to the public as authorized by law, or any data generated by or connected to advanced utility metering infrastructure systems or other equipment for use by a public utility.

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

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

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

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

(4) processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

~~(y)~~ (cc) "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.

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

Sec. 2. Minnesota Statutes 2024, section 325M.12, is amended to read:

325M.12 SCOPE; EXCLUSIONS.

Subdivision 1. **Scope.** (a) Except as specified under section 325M.175, sections 325M.10 to 325M.21 apply 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, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; 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 sections 13.32 and 325M.10 to 325M.21, except that when the provisions of section 13.32 conflict with sections 325M.10 to 325M.21, section 13.32 prevails.

Subd. 2. **Exclusions.** (a) Sections 325M.10 to 325M.21 do not apply to the following entities, activities, 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, if it is maintained by a covered entity or business associate subject to that law and its related regulations;

(ii) health records, as defined in section 144.291, subdivision 2, if it is maintained by a provider or other entity subject to the Minnesota Health Records Act;

(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 that is:

(i) maintained by an entity that meets the definition of health care provider under Code of Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the information in the manner required of covered entities with respect to protected health information for purposes of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

(ii) included in a limited data set, as described under Code of Federal Regulations, title 45, part 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by that part;

(iii) maintained by, or maintained to comply with the rules or orders of, a self-regulatory organization as defined by United States Code, title 15, section 78c(a)(26);

(iv) originated from, or intermingled with, information described in clause (9) and that a licensed residential mortgage originator, as defined under section 58.02, subdivision 19, or residential mortgage servicer, as defined under section 58.02, subdivision 20, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9); or

(v) originated from, or intermingled with, information described in clause (9) and that a nonbank financial institution, as defined by section 46A.01, subdivision 12, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9);

(7) information used only for public health activities and purposes, as described under Code of Federal Regulations, title 45, part 164.512;

(8) 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 the activity involving the collection, maintenance, disclosure, sale, communication, or use of the information by the 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;

(9) 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;

(10) 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;

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

(12) 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 implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection, processing, sale, or disclosure is in compliance with that law;

(13) 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 a business if the data is collected and used solely within the context of the 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;

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

(15) 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 325M.11, are retained;

(16) a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in United States Code, title 12, section 1843(k);

(17) information that originates from, or is intermingled so as to be indistinguishable from, information described in clause (8) and that a person licensed under chapter 56 collects, processes, uses, or maintains in the same manner as is required under the laws and regulations specified in clause (8);

(18) an insurance company, as defined in section 60A.02, subdivision 4, an insurance producer, as defined in section 60K.31, subdivision 6, a third-party administrator of

self-insurance, or an affiliate or subsidiary of any entity identified in this clause that is principally engaged in financial activities, as described in United States Code, title 12, section 1843(k), except that this clause does not apply to a person that, alone or in combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance;

~~(19) a small business, as defined by the United States Small Business Administration under Code of Federal Regulations, title 13, part 121, except that a small business identified in this clause is subject to section 325M.17;~~

~~(20)~~ (19) a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance; and

~~(21)~~ (20) an air carrier subject to the federal Airline Deregulation Act, Public Law 95-504, only to the extent that an air carrier collects personal data related to prices, routes, or services and only to the extent that the provisions of the Airline Deregulation Act preempt the requirements of sections 325M.10 to 325M.21.

(b) Controllers that are in compliance with the Children's Online Privacy Protection Act, United States Code, title 15, sections 6501 to 6506, and implementing regulations, shall be deemed compliant with any obligation to obtain parental consent under ~~sections 325M.10 to 325M.21~~ section 325M.16, subdivision 2, paragraph (g).

Sec. 3. Minnesota Statutes 2024, section 325M.16, subdivision 2, is amended to read:

Subd. 2. **Use of data.** (a) A controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed, which must be disclosed to the consumer.

(b) Except as provided in sections 325M.10 to 325M.21, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(c) 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, including the maintenance of an inventory of the data that must be managed to exercise these responsibilities. The data security practices shall be appropriate to the volume and nature of the personal data at issue.

(d) ~~Except as otherwise provided in sections 325M.10 to 325M.21,~~ A controller may not process sensitive data concerning a consumer ~~without obtaining the consumer's consent,~~

~~or, in the case of the processing of~~ except with the consumer's consent to the processing for a specified purpose.

(e) A controller may not share a consumer's sensitive data with any party other than the consumer except with the consumer's consent to the specified sharing.

(f) A consumer's consent to share sensitive data under paragraph (e) must be separate and distinct from a consumer's consent to process the consumer's health data under paragraph (d). A consent under this subdivision must be obtained prior to the processing or sharing, as applicable, of the sensitive data. Any request for consent under this subdivision must clearly and conspicuously disclose:

(1) the categories of sensitive data processed or shared, as applicable;

(2) the purpose of the processing or sharing, as applicable, of the sensitive data, including the specific ways in which it will be used;

(3) the categories of entities with which the sensitive data is shared; and

(4) how the consumer can withdraw consent from future processing or sharing of the consumer's sensitive data.

(g) A controller may not process 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, rules, and exemptions.

~~(e)~~ (h) 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 the request.

~~(f)~~ (i) 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 controller knows that the consumer is between the ages of 13 and 16.

~~(g)~~ (j) A controller may not retain personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under section 325M.19.

Sec. 4. **[325M.175] REQUIREMENTS FOR THE SALE OF SENSITIVE DATA.**

Subdivision 1. **Scope; exclusions.** (a) Notwithstanding section 325M.12, subdivision 1, a legal entity must comply with sections 325M.10 to 325M.21 as if it were a controller or processor if that legal entity:

(1) conducts business in Minnesota or produces products or services that are targeted to residents of Minnesota; and

(2) is a controller or processor of sensitive data.

(b) The requirements and restrictions specific to sensitive data in this section are in addition to the requirements and restrictions in sections 325M.10 to 325M.21 for personal data generally, including the requirements for sensitive data under section 325M.16, subdivision 2, paragraphs (d) to (f).

(c) The exclusions in section 325M.12, subdivision 2, apply to this section.

Subd. 2. **Requirements specific to the sale of sensitive data.** (a) It is unlawful for any person to sell or offer to sell a consumer's sensitive data without first obtaining valid authorization from the consumer. The sale of a consumer's sensitive data must be consistent with the valid authorization signed by the consumer. This authorization must be separate and distinct from a consent obtained by a controller to process or share sensitive data under section 325M.16, subdivision 2, paragraphs (d) to (f).

(b) A valid authorization to sell a consumer's sensitive data is a document consistent with this subdivision and must be written in plain language. A valid authorization to sell a consumer's sensitive data must contain the following:

(1) the specific sensitive data, concerning the specific consumer, that the person intends to sell;

(2) the name and contact information of the person collecting and selling the sensitive data;

(3) the name and contact information of the person purchasing the sensitive data from the seller identified in clause (2);

(4) a description of the purpose for the sale, including how the sensitive data will be gathered and how it will be used by the purchaser identified in clause (3) when sold;

(5) a statement that the provision of goods or services to the consumer may not be conditioned on the consumer signing the valid authorization;

(6) a statement that the consumer has a right to revoke the valid authorization at any time and a description of how to submit a revocation of the valid authorization;

(7) a statement that the consumer's sensitive data sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by this section;

(8) an expiration date for the valid authorization that expires one year from when the consumer signs the valid authorization; and

(9) the signature of the consumer and date.

(c) An authorization is not valid if the document has any of the following defects:

(1) the expiration date has passed;

(2) the authorization does not contain all of the information required under this subdivision;

(3) the authorization has been revoked by the consumer;

(4) the authorization has been combined with other documents to create a compound authorization; or

(5) the provision of goods or services to the consumer is conditioned on the consumer signing the authorization.

(d) A copy of the signed valid authorization must be provided to the consumer.

(e) The seller and purchaser of the sensitive data must retain a copy of all valid authorizations for sale of sensitive data for six years from the date of its signature or the date when it was last in effect, whichever is later.

Sec. 5. **[325M.178] GEOFENCE RESTRICTIONS.**

It is unlawful for any person to implement a geofence around an entity that provides in-person health care services or supplies where the geofence is used to:

(1) identify or track a consumer seeking health care services or supplies;

(2) collect health data from a consumer; or

(3) send notifications, messages, or advertisements to a consumer related to the consumer's health data or health care services or supplies.

Sec. 6. Minnesota Statutes 2024, section 325M.18, is amended to read:

325M.18 DATA PRIVACY POLICIES; DATA PRIVACY AND PROTECTION ASSESSMENTS.

(a) A controller must document and maintain a description of the policies and procedures the controller has adopted to comply with sections 325M.10 to 325M.21. The description must include, where applicable:

(1) the name and contact information for the controller's chief privacy officer or other individual with primary responsibility for directing the policies and procedures implemented to comply with the provisions of sections 325M.10 to 325M.21; and

(2) a description of the controller's data privacy policies and procedures which reflect the requirements in ~~section~~ sections 325M.16 and, where applicable, 325M.175, and any policies and procedures designed to:

(i) reflect the requirements of sections 325M.10 to 325M.21 in the design of the controller's systems;

(ii) identify and provide personal data to a consumer as required by sections 325M.10 to 325M.21;

(iii) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, including the maintenance of an inventory of the data that must be managed to exercise the responsibilities under this item;

(iv) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data are processed;

(v) prevent the retention of personal data that is no longer relevant and reasonably necessary in relation to the purposes for which the data were collected and processed, unless retention of the data is otherwise required by law or permitted under section 325M.19; and

(vi) identify and remediate violations of sections 325M.10 to 325M.21.

(b) A controller must conduct and document a data privacy and protection assessment for each of the following processing activities involving personal data:

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

(2) the sale of personal data;

(3) the processing, sharing, or sale of sensitive data;

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

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

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

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

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

(iv) other substantial injury to consumers.

(c) 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.

(d) 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 the processing, as mitigated by safeguards that can be employed by the controller to reduce the potential 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.

(e) A data privacy and protection assessment must include the description of policies and procedures required by paragraph (a).

(f) As part of a civil investigative demand, 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 a request made under this paragraph. The attorney general may evaluate the data privacy and protection assessments for compliance with sections 325M.10 to 325M.21. 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.

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

(h) A single data protection assessment may address multiple sets of comparable processing operations that include similar activities.

Sec. 7. Minnesota Statutes 2024, section 325M.20, is amended to read:

325M.20 ATTORNEY GENERAL ENFORCEMENT.

(a) In the event that a controller or processor violates sections 325M.10 to 325M.21, 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 sections 325M.10 to 325M.21 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 sections 325M.10 to 325M.21 in accordance with section 8.31. If the state prevails in an action to enforce sections 325M.10 to 325M.21, 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 sections 325M.10 to 325M.21 is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation.

(d) Nothing in sections 325M.10 to 325M.21 establishes a private right of action, including under section 8.31, subdivision 3a, for a violation of sections 325M.10 to 325M.21 or any other law.

(e) A person that violates an applicable provision of sections 325M.10 to 325M.21, but that is not a controller or processor, is subject to enforcement by the attorney general under this section as if the person were a controller or processor.

Sec. 8. **REPEALER.**

Minnesota Statutes 2024, section 325M.17, is repealed.

Sec. 9. **EFFECTIVE DATE.**

This act is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply with this act until July 31, 2029.

325M.17 REQUIREMENTS FOR SMALL BUSINESSES.

(a) A small business, as defined by the United States Small Business Administration under Code of Federal Regulations, title 13, part 121, that conducts business in Minnesota or produces products or services that are targeted to residents of Minnesota, must not sell a consumer's sensitive data without the consumer's prior consent.

(b) Penalties and attorney general enforcement procedures under section 325M.20 apply to a small business that violates this section.