CHAPTER 325M

CONSUMER DIGITAL AND DATA PRIVACY

INTERNET PRIVACY

325M.01 DEFINITIONS.

Subdivision 1. **Scope.** The terms used in sections 325M.01 to 325M.09 have the meanings given them in this section.

Subd. 2. **Consumer.** "Consumer" means a person who agrees to pay a fee to an Internet service provider for access to the Internet for personal, family, or household purposes, and who does not resell access.

Subd. 3. **Internet service provider.** "Internet service provider" means a business or person who provides consumers authenticated access to, or presence on, the Internet by means of a switched or dedicated telecommunications channel upon which the provider provides transit routing of Internet Protocol (IP) packets for and on behalf of the consumer. Internet service provider does not include the offering, on a common carrier basis, of telecommunications facilities or of telecommunications by means of these facilities.

Subd. 4. **Ordinary course of business.** "Ordinary course of business" means debt-collection activities, order fulfillment, request processing, or the transfer of ownership.

Subd. 5. **Personally identifiable information.** "Personally identifiable information" means information that identifies:

(1) a consumer by physical or electronic address or telephone number;

(2) a consumer as having requested or obtained specific materials or services from an Internet service provider;

(3) Internet or online sites visited by a consumer; or

(4) any of the contents of a consumer's data-storage devices.

History: *2002 c 395 art 1 s 1*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.02 WHEN DISCLOSURE OF PERSONAL INFORMATION PROHIBITED.

Except as provided in sections 325M.03 and 325M.04, an Internet service provider may not knowingly disclose personally identifiable information concerning a consumer of the Internet service provider.

History: *2002 c 395 art 1 s 2*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.03 WHEN DISCLOSURE OF PERSONAL INFORMATION REQUIRED.

An Internet service provider shall disclose personally identifiable information concerning a consumer:

(1) pursuant to a grand jury subpoena;

(2) to an investigative or law enforcement officer as defined in section 626A.01, subdivision 7, while acting as authorized by law;

(3) pursuant to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by other means;

(4) to a court in a civil action for conversion commenced by the Internet service provider or in a civil action to enforce collection of unpaid subscription fees or purchase amounts, and then only to the extent necessary to establish the fact of the subscription delinquency or purchase agreement, and with appropriate safeguards against unauthorized disclosure;

(5) to the consumer who is the subject of the information, upon written or electronic request and upon payment of a fee not to exceed the actual cost of retrieving the information;

(6) pursuant to subpoena, including an administrative subpoena, issued under authority of a law of this state or another state or the United States; or

(7) pursuant to a warrant or court order.

History: *2002 c 395 art 1 s 3*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.04 WHEN DISCLOSURE OF PERSONAL INFORMATION PERMITTED; AUTHORIZATION.

Subdivision 1. **Conditions of disclosure.** An Internet service provider may disclose personally identifiable information concerning a consumer to:

(1) any person if the disclosure is incident to the ordinary course of business of the Internet service provider;

(2) another Internet service provider for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the Internet service provider; except that the recipient may further disclose the personally identifiable information only as provided by sections 325M.01 to 325M.09;

(3) any person with the authorization of the consumer; or

(4) as provided by section 626A.27.

Subd. 2. **Authorization.** The Internet service provider may obtain the consumer's authorization of the disclosure of personally identifiable information in writing or by electronic means. The request for authorization must reasonably describe the types of persons to whom personally identifiable information may be disclosed and the anticipated uses of the information. In order for an authorization to be effective, a contract between an Internet service provider and the consumer must state either that the authorization will be obtained by an affirmative act of the consumer or that failure of the consumer to object after the request has been made constitutes authorization of disclosure. The provision in the contract must be conspicuous. Authorization may be obtained in a manner consistent with self-regulating guidelines issued by representatives of the Internet service provider or online industries, or in any other manner reasonably designed to comply with this subdivision.

History: *2002 c 395 art 1 s 4*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.05 SECURITY OF INFORMATION.

The Internet service provider shall take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information. The Internet service provider is not liable for actions that would constitute a violation of section 609.88, 609.89, or 609.891, if the Internet service provider does not participate in, authorize, or approve the actions.

History: *2002 c 395 art 1 s 5*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.06 EXCLUSION FROM EVIDENCE.

Except for purposes of establishing a violation of sections 325M.01 to 325M.09, personally identifiable information obtained in any manner other than as provided in sections 325M.01 to 325M.09 may not be received in evidence in a civil action.

History: *2002 c 395 art 1 s 6*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.07 ENFORCEMENT; CIVIL LIABILITY; DEFENSE.

A consumer who prevails or substantially prevails in an action brought under sections 325M.01 to 325M.09 is entitled to the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded to a party awarded damages for a violation of this section. No class action shall be brought under sections 325M.01 to 325M.09.

In an action under sections 325M.01 to 325M.09, it is a defense that the defendant has established and implemented reasonable practices and procedures to prevent violations of sections 325M.01 to 325M.09.

History: *2002 c 395 art 1 s 7*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.08 OTHER LAW.

Sections 325M.01 to 325M.09 do not limit any greater protection of the privacy of information under other law, except that:

(1) nothing in sections 325M.01 to 325M.09 limits the authority under other state or federal law of law enforcement or prosecuting authorities to obtain information; and

(2) if federal law is enacted that regulates the release of personally identifiable information by Internet service providers but does not preempt state law on the subject, the federal law supersedes any conflicting provisions of sections 325M.01 to 325M.09.

History: *2002 c 395 art 1 s 8*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

325M.09 APPLICATION.

Sections 325M.01 to 325M.09 apply to Internet service providers in the provision of services to consumers in this state.

History: *2002 c 395 art 1 s 9*

NOTE: This section expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

CONSUMER DATA PRIVACY

325M.10 CITATION.

Sections 325M.10 to 325M.21 may be cited as the "Minnesota Consumer Data Privacy Act."

History: *2024 c 121 art 5 s 2*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 2, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

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

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

(s) "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) "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) "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 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) 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.

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

History: *2024 c 121 art 5 s 3*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 3, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.12 SCOPE; EXCLUSIONS.

Subdivision 1. **Scope.** (a) 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;

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

(21) 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.

History: *2024 c 121 art 5 s 4*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 4, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.13 RESPONSIBILITY ACCORDING TO ROLE.

(a) Controllers and processors are responsible for meeting the respective obligations established under sections 325M.10 to 325M.21.

(b) Processors are responsible under sections 325M.10 to 325M.21 for adhering to the instructions of the controller and assisting the controller to meet the controller's obligations under sections 325M.10 to 325M.21. Assistance under this paragraph 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 325M.14; 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 325M.18.

(c) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also require that the processor:

(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 the technical and organizational 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. 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) upon a reasonable request from the controller, the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in sections 325M.10 to 325M.21; and

(3) the processor shall allow for, and contribute to, reasonable assessments and inspections by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct, at least annually and at the processor's expense, an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 325M.10 to 325M.21. The assessor must use an appropriate and accepted control standard or framework and assessment procedure for assessments as applicable, and shall provide a report of an assessment to the controller upon request.

(f) In no event shall any contract relieve a controller or a processor from the liabilities imposed on a controller or processor by virtue of the controller's or processor's roles in the processing relationship under sections 325M.10 to 325M.21.

(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 a controller's 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, the processor is a controller with respect to the processing.

History: *2024 c 121 art 5 s 5*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 5, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.14 CONSUMER PERSONAL DATA RIGHTS.

Subdivision 1. **Consumer rights provided.** (a) Except as provided in sections 325M.10 to 325M.21, 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 automated 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 the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions 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 consumer's personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

(h) A consumer has a right to obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.

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 under sections 325M.10 to 325M.21 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 under sections 325M.10 to 325M.21 on the consumer's behalf.

(d) A consumer may designate another person as the consumer's authorized agent to exercise the consumer's right to opt out of the processing of the consumer's personal data for purposes of targeted advertising and sale under subdivision 1, paragraph (f), on the consumer's behalf. A consumer may designate an authorized agent by way of, among other things, a technology, including but not limited to an Internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act 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 the consumer's personal data through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the 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 the 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 the consumer's personal data or targeted advertising. For purposes of this paragraph, the use of an Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence.

(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 the controller's program.

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

(d) A controller that recognizes opt-out preference signals that have been approved by other state laws or regulations is in compliance with this subdivision.

Subd. 4. **Controller response to consumer requests.** (a) Except as provided in sections 325M.10 to 325M.21, 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 the consumer's rights under this section. The means made available 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 45 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 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 5.

(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 the repetitive character of the requests, 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, paragraphs (b) to (e) and (h), 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 the request is fraudulent. If a controller denies an opt-out request because the controller believes a 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 the controller 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.

(k) A controller that has obtained personal data about a consumer from a source other than the consumer may comply with a consumer's request to delete the consumer's personal data pursuant to subdivision 1, paragraph (d), by either:

(1) retaining a record of the deletion request, retaining the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records, and not using the retained data for any other purpose pursuant to the provisions of sections 325M.10 to 325M.21; or

(2) opting the consumer out of the processing of personal data for any purpose except for the purposes exempted pursuant to the provisions of sections 325M.10 to 325M.21.

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 4, 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 45 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 extension within 45 days of receipt of the appeal, together with the reasons for the delay.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to paragraph (c), the controller must provide a written explanation of the reasons for the controller's decision and 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 appeals and the controller's responses for at least 24 months and shall, upon written request by the attorney general as part of an investigation, compile and provide a copy of the records to the attorney general.

History: *2024 c 121 art 5 s 6*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 6, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.15 PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA.

(a) Sections 325M.10 to 325M.21 do not require a controller or processor to do any of the following solely for purposes of complying with sections 325M.10 to 325M.21:

(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 325M.14, 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 325M.14, subdivision 1, paragraphs (b) to (e) and (h), 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 the 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.

History: *2024 c 121 art 5 s 7*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 7, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.16 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 325M.14 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) a description of the controller's retention policies for personal data; and

(8) 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, the controller must disclose the 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 in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer. 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 the 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) Whenever a controller makes a material change to the controller's privacy notice or practices, the controller must notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers 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 notification regarding material changes to affected consumers, 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 or in a similarly conspicuous and accessible location. 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 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 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) 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) 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) 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.

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 sections 325M.10 to 325M.21, 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: (1) require a controller to provide a good or service that requires the consumer's personal data that the controller does not collect or maintain; or (2) 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.

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 sections 325M.10 to 325M.21 is contrary to public policy and is void and unenforceable.

History: *2024 c 121 art 5 s 8*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 8, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

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.

History: *2024 c 121 art 5 s 9*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 9, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

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 325M.16, 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 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.

History: *2024 c 121 art 5 s 10*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 10, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.19 LIMITATIONS AND APPLICABILITY.

(a) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not restrict a controller's or a processor's ability to:

(1) comply with federal, state, or local laws, rules, or regulations, including but not limited to data retention requirements in state or federal law notwithstanding a consumer's request to delete personal data;

(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, including fulfilling the terms of a written warranty; 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 or physical safety 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;

(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 that has determined:

(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; or

(10) process personal data for the benefit of the public in the areas of public health, community health, or population health, but only to the extent that the processing is:

(i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(ii) under the responsibility of a professional individual who is subject to confidentiality obligations under federal, state, or local law.

(b) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) effectuate a product recall or identify and repair technical errors that impair existing or intended functionality;

(2) perform 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; or

(3) conduct internal research to develop, improve, or repair products, services, or technology.

(c) The obligations imposed on controllers or processors under sections 325M.10 to 325M.21 do not apply where compliance by the controller or processor with sections 325M.10 to 325M.21 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 sections 325M.10 to 325M.21 is not in violation of sections 325M.10 to 325M.21 if the recipient processes the personal data in violation of sections 325M.10 to 325M.21, 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 sections 325M.10 to 325M.21 is not in violation of sections 325M.10 to 325M.21 for the obligations of the controller or processor from which the third-party controller or processor receives the personal data.

(e) Obligations imposed on controllers and processors under sections 325M.10 to 325M.21 shall not:

(1) adversely affect the rights or freedoms of any persons, including 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 may be processed solely to the extent that the 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 the 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 the processing.

History: *2024 c 121 art 5 s 11*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 11, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

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.

History: *2024 c 121 art 5 s 12*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 12, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

325M.21 PREEMPTION OF LOCAL LAW; SEVERABILITY.

(a) Sections 325M.10 to 325M.21 supersede and preempt 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 sections 325M.10 to 325M.21 or the application of sections 325M.10 to 325M.21 to any person or circumstance is held invalid, the remainder of sections 325M.10 to 325M.21 or the application of the provision to other persons or circumstances is not affected.

History: *2024 c 121 art 5 s 13*

NOTE: This section, as added by Laws 2024, chapter 121, article 5, section 13, is effective July 31, 2025, except that postsecondary institutions regulated by the Office of Higher Education are not required to comply until July 31, 2029. Laws 2024, chapter 121, article 5, section 14.

SOCIAL MEDIA MANIPULATION

325M.30 CITATION.

Sections 325M.30 to 325M.34 may be cited as the "Prohibiting Social Media Manipulation Act."

History: *2024 c 114 art 3 s 63*

NOTE: This section, as added by Laws 2024, chapter 114, article 3, section 63, is effective July 1, 2025. Laws 2024, chapter 114, article 3, section 63, the effective date.

325M.31 DEFINITIONS.

(a) For purposes of sections 325M.30 to 325M.34, the following terms have the meanings given.

(b) "Accessible user interface" means a way for a user to input data, make a choice, or take an action on a social media platform in two clicks or fewer.

(c) "Account holder" means a natural person or legal person who holds an account or profile with a social media platform.

(d) "Account interactions" means any action that a user can make within a social media platform that could have a negative impact on another account holder. Account interactions include but are not limited to:

(1) sending messages or invitations to users;

(2) reporting users;

(3) commenting on, resharing, liking, voting, or otherwise reacting to users' user-generated content; and

(4) posting user-generated content or disseminating user-generated content to users.

Actions that have no impact on other users, including viewing user-generated content or public content, are not account interactions.

(e) "Algorithmic ranking system" means a computational process, including one derived from algorithmic decision making, machine learning, statistical analysis, or other data processing or artificial intelligence techniques, used to determine the selection, order, relative prioritization, or relative prominence of content from a set of information that is provided to a user on a social media platform, including search results ranking, content recommendations, content display, or any other automated content selection method.

(f) "Conspicuously" means the information is presented in a manner, given the information's size, color, contrast, location, and proximity to any related information, as to be readily noticed and understood by a reasonable user.

(g) "Content" means any media, including but not limited to written posts, images, visual or audio recordings, notifications, and games, that a user views, reads, watches, listens to, or otherwise interacts or engages with on a social media platform. Content includes other account holders' accounts or profiles when recommended to a user by the social media platform.

(h) "Engage" or "engagement" means a user's utilization of the social media platform.

(i) "Expressed preferences" means a freely given, considered, specific, and unambiguous indication of a user's preferences regarding the user's engagement with a social media platform. Expressed preferences must not be based on the user's time spent engaging with content on the social media platform or on the use of features that do not indicate explicit preference, including comments made, posts reshared, or similar actions that may be taken on content the user perceives to be of low quality. Expressed preferences must not be obtained through a user interface designed or manipulated with the substantial effect of subverting or impairing a user's decision making.

(j) "Social media platform" means an electronic medium, including a browser-based or application-based interactive computer service, Internet website, telephone network, or data network, that allows an account holder to create, share, and view user-generated content for a substantial purpose of social interaction, sharing user-generated content, or personal networking. Social media platform does not include:

(1) an Internet search provider;

(2) an Internet service provider;

(3) an email service;

(4) a streaming service, online video game, e-commerce, or other Internet website where the content is not user generated but where interactive functions enable chat, comments, reviews, or other interactive functionality that is incidental to, directly related to, or dependent upon providing the content;

(5) a communication service, including text, audio, or video communication technology, provided by a business to the business's employees and clients for use in the course of business activities and not for public distribution, except that social media platform includes a communication service provided by a social media platform;

(6) an advertising network with the sole function of delivering commercial content;

(7) a telecommunications carrier, as defined in United States Code, title 47, section 153;

(8) a broadband service, as defined in section 116J.39, subdivision 1;

(9) single-purpose community groups for education or public safety;

(10) teleconferencing or video-conferencing services that allow reception and transmission of audio and video signals for real-time communication, except that social media platform includes teleconferencing or video-conferencing services provided by a social media platform;

(11) cloud computing services, which may include cloud storage and shared document collaboration;

(12) providing or obtaining technical support for a platform, product, or service; or

(13) a platform designed primarily and specifically for creative professional users, as distinct from the general public, to share their portfolio and creative content, engage in professional networking, acquire clients, and market the creative professional user's creative content and creative services through facilitated transactions.

(k) "Time sensitive" means content that is welcomed under a user's expressed preferences and that has significantly reduced value to the user with the passing of time.

(l) "User" means a natural person who is located in Minnesota and who holds an account or profile with a social media platform.

(m) "User-generated content" means any content created by an account holder that is uploaded, posted, shared, or disseminated on the social media platform.

History: *2024 c 114 art 3 s 64*

NOTE: This section, as added by Laws 2024, chapter 114, article 3, section 64, is effective July 1, 2025. Laws 2024, chapter 114, article 3, section 64, the effective date.

325M.32 SCOPE; EXCLUSIONS.

(a) A social media platform is subject to sections 325M.30 to 325M.34 if the social media platform:

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

(2) has more than 10,000 monthly active account holders located in Minnesota.

(b) For purposes of sections 325M.30 to 325M.34, a social media platform may determine whether an account holder is located in Minnesota based on:

(1) the account holder's own supplied address or location;

(2) global positioning system-level latitude, longitude, or altitude coordinates;

(3) cellular phone system coordinates;

(4) Internet protocol device address; or

(5) other mechanisms that can be used to identify an account holder's location.

History: *2024 c 114 art 3 s 65*

NOTE: This section, as added by Laws 2024, chapter 114, article 3, section 65, is effective July 1, 2025. Laws 2024, chapter 114, article 3, section 65, the effective date.

325M.33 TRANSPARENCY REQUIREMENTS FOR SOCIAL MEDIA PLATFORMS.

A social media platform must publicly and conspicuously post the following information on the social media platform's website:

(1) an explanation of how the social media platform limits excessive account interactions, including:

(i) the maximum limit on the number of times that a user can engage in each specific kind of account interaction in an hour, day, week, and month; and

(ii) whether and how the platform engages in any reduction in the ability of accounts to affect other users when the user engages in a high number of account interactions that is below the maximum limit;

(2) an explanation detailing how the platform:

(i) assesses the quality of content;

(ii) assesses users' expressed preferences regarding content; and

(iii) utilizes the assessments under items (i) and (ii) in each of the social media platform's algorithmic ranking system, including how the assessments are weighted in relation to other signals in the algorithmic ranking system;

(3) statistics on the platform's use with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders for each distinct type of account interaction or engagement, including but not limited to:

(i) sending invitations or messages to other platform account holders;

(ii) commenting on, resharing, liking, voting for, or otherwise reacting to content;

(iii) posting new user-generated content;

(iv) disseminating user-generated content to other platform account holders; and

(v) time spent on the platform;

(4) an explanation of how the platform determines whether a notification is time sensitive and how many time-sensitive and non-time-sensitive notifications are sent to users including:

(i) how many time-sensitive and non-time-sensitive notifications are sent with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders in a given day; and

(ii) how many time-sensitive and non-time-sensitive notifications are sent with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders during each hour between the hours of 11:00 p.m. and 7:00 a.m.; and

(5) a description of all product experiments that have been conducted on 1,000 or more users, including a description of the experimental conditions and the results of the product experiment for all experimental conditions on users' viewing or engaging with content that:

(i) users indicate to be high or low quality;

(ii) users indicate complies or does not comply with the users' expressed preferences; or

(iii) violates platform policies.

History: *2024 c 114 art 3 s 66*

NOTE: This section, as added by Laws 2024, chapter 114, article 3, section 66, is effective July 1, 2025. Laws 2024, chapter 114, article 3, section 66, the effective date.

325M.34 ENFORCEMENT AUTHORITY.

(a) The attorney general may investigate and bring an action against a social media platform for an alleged violation of section 325M.33.

(b) Nothing in sections 325M.30 to 325M.34 creates a private cause of action in favor of a person injured by a violation of section 325M.33.

History: *2024 c 114 art 3 s 67*

NOTE: This section, as added by Laws 2024, chapter 114, article 3, section 67, is effective July 1, 2025. Laws 2024, chapter 114, article 3, section 67, the effective date.