SENATE
STATE OF MINNESOTA
NINETY-SECOND SESSION

S.F. No. 1408

1.1   A bill for an act

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

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

1.7   Section 1. **[325O.01] CITATION.**

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

1.9   Sec. 2. **[325O.02] DEFINITIONS.**

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

1.11   (b) "Affiliate" means a legal entity that controls, is controlled by, or is under common

1.12   control with, that other legal entity. For these purposes, "control" or "controlled" means:

1.13   ownership of, or the power to vote, more than 50 percent of the outstanding shares of any

1.14   class of voting security of a company; control in any manner over the election of a majority

1.15   of the directors or of individuals exercising similar functions; or the power to exercise a

1.16   controlling influence over the management of a company.

1.17   (c) "Authenticate" means to use reasonable means to determine that a request to exercise

1.18   any of the rights in section 325O.05, subdivision 1, paragraphs (b) to (e), is being made by

1.19   the consumer who is entitled to exercise such rights with respect to the personal data at

1.20   issue.

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

2.1   (e) "Consent" means any freely given, specific, informed, and unambiguous indication

2.2   of the consumer's wishes by which the consumer signifies agreement to the processing of

2.3   personal data relating to the consumer for a narrowly defined particular purpose. Acceptance

2.4   of a general or broad terms of use or similar document that contains descriptions of personal

2.5   data processing along with other, unrelated information does not constitute consent. Hovering

2.6   over, muting, pausing, or closing a given piece of content does not constitute consent.

2.7   Likewise, consent cannot be obtained through a user interface designed or manipulated with

2.8   the substantial effect of subverting or impairing user autonomy, decision making, or choice.

2.9   (f) "Consumer" means a natural person who is a Minnesota resident acting only in an

2.10   individual or household context. It does not include a natural person acting in a commercial

2.11   or employment context.

2.12   (g) "Controller" means the natural or legal person which, alone or jointly with others,

2.13   determines the purposes and means of the processing of personal data.

2.14   (h) "Decisions that produce legal effects concerning a consumer or similarly significant

2.15   effects concerning a consumer" means decisions that result in the provision or denial of

2.16   financial and lending services, housing, insurance, education enrollment, criminal justice,

2.17   employment opportunities, health care services, or access to basic necessities, such as food

2.18   and water.

2.19   (i) "Deidentified data" means data that cannot reasonably be used to infer information

2.20   about, or otherwise be linked to, an identified or identifiable natural person, or a device

2.21   linked to such person, provided that the controller that possesses the data:

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

2.23   person;

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

2.25   attempt to reidentify the data; and

2.26   (3) contractually obligates any recipients of the information to comply with all provisions

2.27   of this paragraph.

2.28   (j) "Delete" means to remove or destroy information such that it is not maintained in

2.29   human- or machine-readable form and cannot be retrieved or utilized in the course of

2.30   business.

2.31   (k) "Identified or identifiable natural person" means a person who can be readily

2.32   identified, directly or indirectly.

3.1   (l) "Known child" means a child under circumstances where a controller has actual

3.2   knowledge of, or willfully disregards, the child's age.

3.3   (m) "Personal data" means any information that is linked or reasonably linkable to an

3.4   identified or identifiable natural person. Personal data does not include deidentified data or

3.5   publicly available information. For purposes of this paragraph, "publicly available

3.6   information" means information that is lawfully made available from federal, state, or local

3.7   government records.

3.8   (n) "Process" or "processing" means any operation or set of operations that are performed

3.9   on personal data or on sets of personal data, whether or not by automated means, such as

3.10   the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

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

3.12   of a controller.

3.13   (p) "Profiling" means any form of automated processing of personal data to evaluate,

3.14   analyze, or predict personal aspects concerning an identified or identifiable natural person's

3.15   economic situation, health, personal preferences, interests, reliability, behavior, location,

3.16   or movements.

3.17   (q) "Pseudonymous data" means personal data that cannot be attributed to a specific

3.18   natural person without the use of additional information, provided that such additional

3.19   information is kept separately and is subject to appropriate technical and organizational

3.20   measures to ensure that the personal data are not attributed to an identified or identifiable

3.21   natural person.

3.22   (r) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other

3.23   valuable consideration by the controller to a third party. Sale does not include the following:

3.24   (1) the disclosure of personal data to a processor who processes the personal data on

3.25   behalf of the controller;

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

3.27   relationship for purposes of providing a product or service requested by the consumer;

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

3.29   (4) the disclosure of information that the consumer intentionally made available to the

3.30   general public via a channel of mass media, and did not restrict to a specific audience; or

4.1   (5) the disclosure or transfer of personal data to a third party as an asset that is part of a

4.2   merger, acquisition, bankruptcy, or other transaction in which the third party assumes control

4.3   of all or part of the controller's assets.

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

4.5   (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical

4.6   health condition or diagnosis, sexual orientation, or citizenship or immigration status;

4.7   (2) the processing of genetic or biometric data for the purpose of uniquely identifying

4.8   a natural person;

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

4.10   (4) specific geolocation data.

4.11   (t) "Specific geolocation data" means information derived from technology including

4.12   but not limited to global positioning system level latitude and longitude coordinates or other

4.13   mechanisms that can be used to identify a natural person's specific location. Specific

4.14   geolocation data excludes the content of communications.

4.15   (u) "Targeted advertising" means displaying advertisements to a consumer where the

4.16   advertisement is selected based on personal data obtained from a consumer's activities over

4.17   time and across nonaffiliated websites or online applications to predict such consumer's

4.18   preferences or interests. It does not include advertising:

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

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

4.21   online application; or

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

4.23   (v) "Third party" means a natural or legal person, public authority, agency, or body other

4.24   than the consumer, controller, processor, or an affiliate of the processor or the controller.

4.25   Sec. 3. **[325O.03] SCOPE; EXCLUSIONS.**

4.26   Subdivision 1. **Scope.** This chapter applies to legal entities that conduct business in

4.27   Minnesota or produce products or services that are targeted to residents of Minnesota, and

4.28   that satisfy one or more of the following thresholds:

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

4.30   more; or

5.1   (2) derives over 25 percent of gross revenue from the sale of personal data and processes

5.2   or controls personal data of 25,000 consumers or more.

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

5.4   of information:

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

5.6   (2) a federally recognized Indian tribe;

5.7   (3) information that meets the definition of:

5.8   (i) protected health information as defined by and for purposes of the Health Insurance

5.9   Portability and Accountability Act of 1996, Public Law 104-191, and related regulations;

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

5.11   (iii) patient identifying information for purposes of Code of Federal Regulations, title

5.12   42, part 2, established pursuant to United States Code, title 42, section 290dd-2;

5.13   (iv) identifiable private information for purposes of the federal policy for the protection

5.14   of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private

5.15   information that is otherwise information collected as part of human subjects research

5.16   pursuant to the good clinical practice guidelines issued by the International Council for

5.17   Harmonisation; the protection of human subjects under Code of Federal Regulations, title

5.18   21, parts 50 and 56; or personal data used or shared in research conducted in accordance

5.19   with one or more of the requirements set forth in this paragraph;

5.20   (v) information and documents created for purposes of the federal Health Care Quality

5.21   Improvement Act of 1986, Public Law 99-660, and related regulations; or

5.22   (vi) patient safety work product for purposes of Code of Federal Regulations, title 42,

5.23   part 3, established pursuant to United States Code, title 42, sections 299b-21 to 299b-26;

5.24   (4) information that is derived from any of the health care-related information listed in

5.25   clause (3), but that has been deidentified in accordance with the requirements for

5.26   deidentification set forth in Code of Federal Regulations, title 45, part 164;

5.27   (5) information originating from, and intermingled to be indistinguishable with, any of

5.28   the health care-related information listed in clause (3) that is maintained by:

5.29   (i) a covered entity or business associate as defined by the Health Insurance Portability

5.30   and Accountability Act of 1996, Public Law 104-191, and related regulations;

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

6.1   (iii) a program or a qualified service organization as defined by Code of Federal

6.2   Regulations, title 42, part 2, established pursuant to United States Code, title 42, section

6.3   290dd-2;

6.4   (6) information used only for public health activities and purposes as described in Code

6.5   of Federal Regulations, title 45, section 164.512;

6.6   (7) an activity involving the collection, maintenance, disclosure, sale, communication,

6.7   or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit

6.8   capacity, character, general reputation, personal characteristics, or mode of living by a

6.9   consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by

6.10   a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who

6.11   provides information for use in a consumer report, as defined in United States Code, title

6.12   15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,

6.13   title 15, section 1681b, except that information is only excluded under this paragraph to the

6.14   extent that such activity involving the collection, maintenance, disclosure, sale,

6.15   communication, or use of such information by that agency, furnisher, or user is subject to

6.16   regulation under the federal Fair Credit Reporting Act, United States Code, title 15, sections

6.17   1681 to 1681x, and the information is not collected, maintained, used, communicated,

6.18   disclosed, or sold except as authorized by the Fair Credit Reporting Act;

6.19   (8) personal data collected, processed, sold, or disclosed pursuant to the federal

6.20   Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the

6.21   collection, processing, sale, or disclosure is in compliance with that law;

6.22   (9) personal data collected, processed, sold, or disclosed pursuant to the federal Driver's

6.23   Privacy Protection Act of 1994, United States Code, title 18, sections 2721 to 2725, if the

6.24   collection, processing, sale, or disclosure is in compliance with that law;

6.25   (10) personal data regulated by the federal Family Educations Rights and Privacy Act,

6.26   United States Code, title 20, section 1232g, and its implementing regulations;

6.27   (11) personal data collected, processed, sold, or disclosed pursuant to the federal Farm

6.28   Credit Act of 1971, as amended, United States Code, title 12, sections 2001 to 2279cc, and

6.29   its implementing regulations, Code of Federal Regulations, title 12, part 600, if the collection,

6.30   processing, sale, or disclosure is in compliance with that law;

6.31   (12) data collected or maintained:

7.1 (i) in the course of an individual acting as a job applicant to or an employee, owner,

7.2 director, officer, medical staff member, or contractor of that business if it is collected and

7.3 used solely within the context of that role;

7.4 (ii) as the emergency contact information of an individual under item (i) if used solely

7.5 for emergency contact purposes; or

7.6 (iii) that is necessary for the business to retain to administer benefits for another individual

7.7 relating to the individual under item (i) if used solely for the purposes of administering those

7.8 benefits;

7.9 (13) personal data collected, processed, sold, or disclosed pursuant to the Minnesota

7.10 Insurance Fair Information Reporting Act in sections 72A.49 to 72A.505; or

7.11 (14) data collected, processed, sold, or disclosed as part of a payment-only credit, check,

7.12 or cash transaction where no data about consumers, as defined in section 325O.02, are

7.13 retained.

7.14 (b) Controllers that are in compliance with the Children's Online Privacy Protection Act,

7.15 United States Code, title 15, sections 6501 to 6506, and its implementing regulations, shall

7.16 be deemed compliant with any obligation to obtain parental consent under this chapter.

7.17 Sec. 4. **[325O.04] RESPONSIBILITY ACCORDING TO ROLE.**

7.18 (a) Controllers and processors are responsible for meeting their respective obligations

7.19 established under this chapter.

7.20 (b) Processors are responsible under this chapter for adhering to the instructions of the

7.21 controller and assisting the controller to meet its obligations under this chapter. Such

7.22 assistance shall include the following:

7.23 (1) taking into account the nature of the processing, the processor shall assist the controller

7.24 by appropriate technical and organizational measures, insofar as this is possible, for the

7.25 fulfillment of the controller's obligation to respond to consumer requests to exercise their

7.26 rights pursuant to section 325O.05; and

7.27 (2) taking into account the nature of processing and the information available to the

7.28 processor, the processor shall assist the controller in meeting the controller's obligations in

7.29 relation to the security of processing the personal data and in relation to the notification of

7.30 a breach of the security of the system pursuant to section 325E.61, and shall provide

7.31 information to the controller necessary to enable the controller to conduct and document

7.32 any data protection assessments required by section 325O.08.

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

8.2   (1) ensure that each person processing the personal data is subject to a duty of

8.3   confidentiality with respect to the data; and

8.4   (2) engage a subcontractor only (i) after providing the controller with an opportunity to

8.5   object, and (ii) pursuant to a written contract in accordance with paragraph (e) that requires

8.6   the subcontractor to meet the obligations of the processor with respect to the personal data.

8.7   (d) Taking into account the context of processing, the controller and the processor shall

8.8   implement appropriate technical and organizational measures to ensure a level of security

8.9   appropriate to the risk and establish a clear allocation of the responsibilities between the

8.10   controller and the processor to implement such measures.

8.11   (e) Processing by a processor shall be governed by a contract between the controller and

8.12   the processor that is binding on both parties and that sets out the processing instructions to

8.13   which the processor is bound, including the nature and purpose of the processing, the type

8.14   of personal data subject to the processing, the duration of the processing, and the obligations

8.15   and rights of both parties. In addition, the contract shall include the requirements imposed

8.16   by this paragraph, paragraphs (c) and (d), as well as the following requirements:

8.17   (1) at the choice of the controller, the processor shall delete or return all personal data

8.18   to the controller as requested at the end of the provision of services, unless retention of the

8.19   personal data is required by law;

8.20   (2) the processor shall make available to the controller all information necessary to

8.21   demonstrate compliance with the obligations in this chapter; and

8.22   (3) the processor shall allow for, and contribute to, reasonable audits and inspections by

8.23   the controller or the controller's designated auditor. Alternatively, the processor may, with

8.24   the controller's consent, arrange for a qualified and independent auditor to conduct, at least

8.25   annually and at the processor's expense, an audit of the processor's policies and technical

8.26   and organizational measures in support of the obligations under this chapter. The auditor

8.27   must use an appropriate and accepted control standard or framework and audit procedure

8.28   for such audits as applicable, and shall provide a report of such audit to the controller upon

8.29   request.

8.30   (f) In no event shall any contract relieve a controller or a processor from the liabilities

8.31   imposed on them by virtue of their roles in the processing relationship under this chapter.

8.32   (g) Determining whether a person is acting as a controller or processor with respect to

8.33   a specific processing of data is a fact-based determination that depends upon the context in

9.1 which personal data are to be processed. A person that is not limited in the person's processing

9.2 of personal data pursuant to a controller's instructions, or that fails to adhere to such

9.3 instructions, is a controller and not a processor with respect to a specific processing of data.

9.4 A processor that continues to adhere to a controller's instructions with respect to a specific

9.5 processing of personal data remains a processor. If a processor begins, alone or jointly with

9.6 others, determining the purposes and means of the processing of personal data, it is a

9.7 controller with respect to such processing.

9.8 Sec. 5. **[325O.05] CONSUMER PERSONAL DATA RIGHTS.**

9.9 Subdivision 1. **Consumer rights provided.** (a) Except as provided in this chapter, a

9.10 controller must comply with a request to exercise the consumer rights provided in this

9.11 subdivision.

9.12 (b) A consumer has the right to confirm whether or not a controller is processing personal

9.13 data concerning the consumer and access the categories of personal data the controller is

9.14 processing.

9.15 (c) A consumer has the right to correct inaccurate personal data concerning the consumer,

9.16 taking into account the nature of the personal data and the purposes of the processing of the

9.17 personal data.

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

9.19 (e) A consumer has the right to obtain personal data concerning the consumer, which

9.20 the consumer previously provided to the controller, in a portable and, to the extent technically

9.21 feasible, readily usable format that allows the consumer to transmit the data to another

9.22 controller without hindrance, where the processing is carried out by automated means.

9.23 (f) A consumer has the right to opt out of the processing of personal data concerning

9.24 the consumer for purposes of targeted advertising, the sale of personal data, or profiling in

9.25 furtherance of decisions that produce legal effects concerning a consumer or similarly

9.26 significant effects concerning a consumer.

9.27 Subd. 2. **Exercising consumer rights.** (a) A consumer may exercise the rights set forth

9.28 in this section by submitting a request, at any time, to a controller specifying which rights

9.29 the consumer wishes to exercise.

9.30 (b) In the case of processing personal data concerning a known child, the parent or legal

9.31 guardian of the known child may exercise the rights of this chapter on the child's behalf.

10.1   (c) In the case of processing personal data concerning a consumer legally subject to

10.2   guardianship or conservatorship under sections 524.5-101 to 524.5-502, the guardian or the

10.3   conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

10.4   Subd. 3. **Controller response to consumer requests.** (a) Except as provided in this

10.5   chapter, a controller must comply with a request to exercise the rights pursuant to subdivision

10.6   1.

10.7   (b) A controller must provide one or more secure and reliable means for consumers to

10.8   submit a request to exercise their rights under this section. These means must take into

10.9   account the ways in which consumers interact with the controller and the need for secure

10.10   and reliable communication of the requests.

10.11   (c) A controller may not require a consumer to create a new account in order to exercise

10.12   a right, but a controller may require a consumer to use an existing account to exercise the

10.13   consumer's rights under this section.

10.14   (d) A controller must comply with a request to exercise the right in subdivision 1,

10.15   paragraph (e), as soon as feasibly possible, but no later than 15 days of receipt of the request.

10.16   (e) A controller must inform a consumer of any action taken on a request under

10.17   subdivision 1, paragraphs (b) to (d), without undue delay and in any event within 45 days

10.18   of receipt of the request. That period may be extended once by 45 additional days where

10.19   reasonably necessary, taking into account the complexity and number of the requests. The

10.20   controller must inform the consumer of any such extension within 45 days of receipt of the

10.21   request, together with the reasons for the delay.

10.22   (f) If a controller does not take action on a consumer's request, the controller must inform

10.23   the consumer without undue delay and at the latest within 45 days of receipt of the request

10.24   of the reasons for not taking action and instructions for how to appeal the decision with the

10.25   controller as described in subdivision 3.

10.26   (g) Information provided under this section must be provided by the controller free of

10.27   charge, up to twice annually to the consumer. Where requests from a consumer are manifestly

10.28   unfounded or excessive, in particular because of their repetitive character, the controller

10.29   may either charge a reasonable fee to cover the administrative costs of complying with the

10.30   request, or refuse to act on the request. The controller bears the burden of demonstrating

10.31   the manifestly unfounded or excessive character of the request.

10.32   (h) A controller is not required to comply with a request to exercise any of the rights

10.33   under subdivision 1, paragraphs (b) to (e), if the controller is unable to authenticate the

11.1   request using commercially reasonable efforts. In such cases, the controller may request

11.2   the provision of additional information reasonably necessary to authenticate the request.

11.3   Subd. 4. **Appeal process required.** (a) A controller must establish an internal process

11.4   whereby a consumer may appeal a refusal to take action on a request to exercise any of the

11.5   rights under subdivision 1 within a reasonable period of time after the consumer's receipt

11.6   of the notice sent by the controller under subdivision 3, paragraph (f).

11.7   (b) The appeal process must be conspicuously available. The process must include the

11.8   ease of use provisions in subdivision 3 applicable to submitting requests.

11.9   (c) Within 30 days of receipt of an appeal, a controller must inform the consumer of any

11.10   action taken or not taken in response to the appeal, along with a written explanation of the

11.11   reasons in support thereof. That period may be extended by 60 additional days where

11.12   reasonably necessary, taking into account the complexity and number of the requests serving

11.13   as the basis for the appeal. The controller must inform the consumer of any such extension

11.14   within 30 days of receipt of the appeal, together with the reasons for the delay. The controller

11.15   must also provide the consumer with an e-mail address or other online mechanism through

11.16   which the consumer may submit the appeal, along with any action taken or not taken by the

11.17   controller in response to the appeal and the controller's written explanation of the reasons

11.18   in support thereof, to the attorney general.

11.19   (d) When informing a consumer of any action taken or not taken in response to an appeal

11.20   pursuant to paragraph (c), the controller must clearly and prominently provide the consumer

11.21   with information about how to file a complaint with the Office of the Attorney General.

11.22   The controller must maintain records of all such appeals and the controller's responses for

11.23   at least 24 months and shall, upon request by a consumer or by the attorney general, compile

11.24   and provide a copy of the records to the attorney general.

11.25   Sec. 6. **[325O.06] PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS**

11.26   **DATA.**

11.27   (a) This chapter does not require a controller or processor to do any of the following

11.28   solely for purposes of complying with this chapter:

11.29   (1) reidentify deidentified data;

11.30   (2) maintain data in identifiable form, or collect, obtain, retain, or access any data or

11.31   technology, in order to be capable of associating an authenticated consumer request with

11.32   personal data; or

12.1   (3) comply with an authenticated consumer request to access, correct, delete, or port

12.2 personal data pursuant to section 325O.05, subdivision 1, paragraphs (b) to (e), if all of the

12.3 following are true:

12.4   (i) the controller is not reasonably capable of associating the request with the personal

12.5 data, or it would be unreasonably burdensome for the controller to associate the request

12.6 with the personal data;

12.7   (ii) the controller does not use the personal data to recognize or respond to the specific

12.8 consumer who is the subject of the personal data, or associate the personal data with other

12.9 personal data about the same specific consumer; and

12.10   (iii) the controller does not sell the personal data to any third party or otherwise

12.11 voluntarily disclose the personal data to any third party other than a processor, except as

12.12 otherwise permitted in this section.

12.13   (b) The rights contained in section 325O.05, subdivision 1, paragraphs (b) to (e), do not

12.14 apply to pseudonymous data in cases where the controller is able to demonstrate any

12.15 information necessary to identify the consumer is kept separately and is subject to effective

12.16 technical and organizational controls that prevent the controller from accessing such

12.17 information.

12.18   (c) A controller that uses pseudonymous data or deidentified data must exercise reasonable

12.19 oversight to monitor compliance with any contractual commitments to which the

12.20 pseudonymous data or deidentified data are subject, and must take appropriate steps to

12.21 address any breaches of contractual commitments.

12.22   Sec. 7. **[325O.07] RESPONSIBILITIES OF CONTROLLERS.**

12.23   Subdivision 1. **Transparency obligations.** (a) Controllers shall provide consumers with

12.24 a reasonably accessible, clear, and meaningful privacy notice that includes:

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

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

12.27   (3) how and where consumers may exercise the rights contained in section 325O.05,

12.28 including how a consumer may appeal a controller's action with regard to the consumer's

12.29 request;

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

12.31 and

12.32   (5) the categories of third parties, if any, with whom the controller shares personal data.

13.1   (b) If a controller sells personal data to third parties or processes personal data for targeted

13.2   advertising, it must clearly and conspicuously disclose such processing, as well as the manner

13.3   in which a consumer may exercise the right to opt out of such processing, in a clear and

13.4   conspicuous manner.

13.5   Subd. 2. **Use of data.** (a) A controller's collection of personal data must be limited to

13.6   what is reasonably necessary in relation to the purposes for which such data are processed.

13.7   (b) A controller's collection of personal data must be adequate, relevant, and limited to

13.8   what is reasonably necessary in relation to the purposes for which such data are processed,

13.9   as disclosed to the consumer.

13.10   (c) Except as provided in this chapter, a controller may not process personal data for

13.11   purposes that are not reasonably necessary to, or compatible with, the purposes for which

13.12   such personal data are processed, as disclosed to the consumer, unless the controller obtains

13.13   the consumer's consent.

13.14   (d) A controller shall establish, implement, and maintain reasonable administrative,

13.15   technical, and physical data security practices to protect the confidentiality, integrity, and

13.16   accessibility of personal data. Such data security practices shall be appropriate to the volume

13.17   and nature of the personal data at issue.

13.18   (e) Except as otherwise provided in this act, a controller may not process sensitive data

13.19   concerning a consumer without obtaining the consumer's consent, or, in the case of the

13.20   processing of personal data concerning a known child, without obtaining consent from the

13.21   child's parent or lawful guardian, in accordance with the requirement of the Children's

13.22   Online Privacy Protection Act, United States Code, title 15, sections 6501 to 6506, and its

13.23   implementing regulations.

13.24   Subd. 3. **Nondiscrimination.** (a) A controller shall not process personal data on the

13.25   basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity,

13.26   religion, national origin, sex, gender, gender identity, sexual orientation, familial status,

13.27   lawful source of income, or disability in a manner that unlawfully discriminates against the

13.28   consumer or class of consumers with respect to the offering or provision of: housing,

13.29   employment, credit, or education; or the goods, services, facilities, privileges, advantages,

13.30   or accommodations of any place of public accommodation.

13.31   (b) A controller may not discriminate against a consumer for exercising any of the rights

13.32   contained in this chapter, including denying goods or services to the consumer, charging

13.33   different prices or rates for goods or services, and providing a different level of quality of

13.34   goods and services to the consumer. This subdivision does not prohibit a controller from

14.1   offering a different price, rate, level, quality, or selection of goods or services to a consumer,

14.2   including offering goods or services for no fee, if the offering is in connection with a

14.3   consumer's voluntary participation in a bona fide loyalty, rewards, premium features,

14.4   discounts, or club card program.

14.5   (c) A controller may not sell personal data to a third-party controller as part of a bona

14.6   fide loyalty, rewards, premium features, discounts, or club card program under paragraph

14.7   (b) unless:

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

14.9   the consumer is entitled;

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

14.11   program; and

14.12   (3) the third party uses the personal data only for purposes of facilitating such a benefit

14.13   to which the consumer is entitled and does not retain or otherwise use or disclose the personal

14.14   data for any other purpose.

14.15   Subd. 4. **Waiver of rights unenforceable.** Any provision of a contract or agreement of

14.16   any kind that purports to waive or limit in any way a consumer's rights under this chapter

14.17   shall be deemed contrary to public policy and shall be void and unenforceable.

14.18   Sec. 8. **[325O.08] DATA PROTECTION ASSESSMENTS.**

14.19   (a) A controller must conduct and document a data protection assessment of each of the

14.20   following processing activities involving personal data:

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

14.22   (2) the sale of personal data;

14.23   (3) the processing of sensitive data;

14.24   (4) any processing activities involving personal data that present a heightened risk of

14.25   harm to consumers; and

14.26   (5) the processing of personal data for purposes of profiling, where such profiling presents

14.27   a reasonably foreseeable risk of:

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

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

15.1   (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or

15.2   concerns, of consumers, where such intrusion would be offensive to a reasonable person;

15.3   or

15.4   (iv) other substantial injury to consumers.

15.5   (b) A data protection assessment must take into account the type of personal data to be

15.6   processed by the controller, including the extent to which the personal data are sensitive

15.7   data, and the context in which the personal data are to be processed.

15.8   (c) A data protection assessment must identify and weigh the benefits that may flow

15.9   directly and indirectly from the processing to the controller, consumer, other stakeholders,

15.10   and the public against the potential risks to the rights of the consumer associated with such

15.11   processing, as mitigated by safeguards that can be employed by the controller to reduce

15.12   such risks. The use of deidentified data and the reasonable expectations of consumers, as

15.13   well as the context of the processing and the relationship between the controller and the

15.14   consumer whose personal data will be processed, must be factored into this assessment by

15.15   the controller.

15.16   (d) The attorney general may request, in writing, that a controller disclose any data

15.17   protection assessment that is relevant to an investigation conducted by the attorney general.

15.18   The controller must make a data protection assessment available to the attorney general

15.19   upon such a request. The attorney general may evaluate the data protection assessments for

15.20   compliance with the responsibilities contained in section 325O.07 and with other laws. Data

15.21   protection assessments are classified as nonpublic data, as defined by section 13.02,

15.22   subdivision 9. The disclosure of a data protection assessment pursuant to a request from the

15.23   attorney general under this paragraph does not constitute a waiver of the attorney-client

15.24   privilege or work product protection with respect to the assessment and any information

15.25   contained in the assessment.

15.26   (e) Data protection assessments conducted by a controller for the purpose of compliance

15.27   with other laws or regulations may qualify under this section if they have a similar scope

15.28   and effect.

15.29   Sec. 9. **[325O.09] LIMITATIONS AND APPLICABILITY.**

15.30   (a) The obligations imposed on controllers or processors under this chapter do not restrict

15.31   a controller's or a processor's ability to:

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

16.1   (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or

16.2   summons by federal, state, local, or other governmental authorities;

16.3   (3) cooperate with law enforcement agencies concerning conduct or activity that the

16.4   controller or processor reasonably and in good faith believes may violate federal, state, or

16.5   local laws, rules, or regulations;

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

16.7   (5) provide a product or service specifically requested by a consumer, perform a contract

16.8   to which the consumer is a party, or take steps at the request of the consumer prior to entering

16.9   into a contract;

16.10   (6) take immediate steps to protect an interest that is essential for the life of the consumer

16.11   or of another natural person, and where the processing cannot be manifestly based on another

16.12   legal basis;

16.13   (7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud,

16.14   harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity

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

16.16   action;

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

16.18   this paragraph; or

16.19   (9) engage in public or peer-reviewed scientific, historical, or statistical research in the

16.20   public interest that adheres to all other applicable ethics and privacy laws and is approved,

16.21   monitored, and governed by an institutional review board, human subjects research ethics

16.22   review board, or a similar independent oversight entity which has determined that:

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

16.24   the controller;

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

16.26   (iii) the controller has implemented reasonable safeguards to mitigate privacy risks

16.27   associated with research, including any risks associated with reidentification.

16.28   (b) The obligations imposed on controllers or processors under this chapter do not restrict

16.29   a controller's or processor's ability to collect, use, or retain data to:

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

16.31   (2) perform solely internal operations that are reasonably aligned with the expectations

16.32   of the consumer based on the consumer's existing relationship with the controller, or are

17.1   otherwise compatible with processing in furtherance of the provision of a product or service

17.2   specifically requested by a consumer or the performance of a contract to which the consumer

17.3   is a party when those internal operations are performed during, and not following, the

17.4   consumer's relationship with the controller.

17.5   (c) The obligations imposed on controllers or processors under this chapter do not apply

17.6   where compliance by the controller or processor with this chapter would violate an

17.7   evidentiary privilege under Minnesota law and do not prevent a controller or processor from

17.8   providing personal data concerning a consumer to a person covered by an evidentiary

17.9   privilege under Minnesota law as part of a privileged communication.

17.10   (d) A controller or processor that discloses personal data to a third-party controller or

17.11   processor in compliance with the requirements of this chapter is not in violation of this

17.12   chapter if the recipient processes such personal data in violation of this chapter, provided

17.13   that, at the time of disclosing the personal data, the disclosing controller or processor did

17.14   not have actual knowledge that the recipient intended to commit a violation. A third-party

17.15   controller or processor receiving personal data from a controller or processor in compliance

17.16   with the requirements of this chapter is likewise not in violation of this chapter for the

17.17   obligations of the controller or processor from which it receives such personal data.

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

17.19   (1) adversely affect the rights or freedoms of any persons, such as exercising the right

17.20   of free speech pursuant to the First Amendment of the United States Constitution; or

17.21   (2) apply to the processing of personal data by a natural person in the course of a purely

17.22   personal or household activity.

17.23   (f) Personal data that are processed by a controller pursuant to this section must not be

17.24   processed for any purpose other than those expressly listed in this section. Personal data

17.25   that are processed by a controller pursuant to this section may be processed solely to the

17.26   extent that such processing is:

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

17.28   (2) adequate, relevant, and limited to what is necessary in relation to the specific purpose

17.29   or purposes listed in this section; and

17.30   (3) insofar as possible, taking into account the nature and purpose of processing the

17.31   personal data, subjected to reasonable administrative, technical, and physical measures to

17.32   protect the confidentiality, integrity, and accessibility of the personal data, and to reduce

17.33   reasonably foreseeable risks of harm to consumers.

18.1   (g) If a controller processes personal data pursuant to an exemption in this section, the

18.2   controller bears the burden of demonstrating that such processing qualifies for the exemption

18.3   and complies with the requirements in paragraph (f).

18.4   (h) Processing personal data solely for the purposes expressly identified in paragraph

18.5   (a), clauses (1) to (7), does not, by itself, make an entity a controller with respect to such

18.6   processing.

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

18.8   (a) In the event that a controller or processor violates this chapter, the attorney general,

18.9   prior to filing an enforcement action under paragraph (b), must provide the controller or

18.10   processor with a warning letter identifying the specific provisions of this chapter the attorney

18.11   general alleges have been or are being violated. If, after 30 days of issuance of the warning

18.12   letter, the attorney general believes the controller or processor has failed to cure any alleged

18.13   violation, the attorney general may bring an enforcement action under paragraph (b).

18.14   (b) The attorney general may bring a civil action against a controller or processor to

18.15   enforce a provision of this chapter in accordance with section 8.31. If the state prevails in

18.16   an action to enforce this chapter, the state may, in addition to penalties provided by paragraph

18.17   (c) or other remedies provided by law, be allowed an amount determined by the court to be

18.18   the reasonable value of all or part of the state's litigation expenses incurred.

18.19   (c) Any controller or processor that violates this chapter is subject to an injunction and

18.20   liable for a civil penalty of not more than $7,500 for each violation.

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

18.22   (a) This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent

18.23   adopted by any local government regarding the processing of personal data by controllers

18.24   or processors.

18.25   (b) If any provision of this act or its application to any person or circumstance is held

18.26   invalid, the remainder of the act or the application of the provision to other persons or

18.27   circumstances is not affected.

18.28   Sec. 12. **EFFECTIVE DATE.**

18.29   This act is effective July 31, 2022, except that postsecondary institutions regulated by

18.30   the Office of Higher Education, air carriers as defined in United States Code, title 49, section

19.1   40102, and nonprofit corporations governed by Minnesota Statutes, chapter 317A, are not

19.2   required to comply with this act until July 31, 2026.