

This Document can be made available in alternative formats upon request

State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-THIRD SESSION

H. F. No. 2309

- 03/01/2023 Authored by Elkins, Bahner, Noor and Feist
The bill was read for the first time and referred to the Committee on Commerce Finance and Policy
- 02/26/2024 Adoption of Report: Amended and re-referred to the Committee on Judiciary Finance and Civil Law
- 03/07/2024 Adoption of Report: Amended and re-referred to the Committee on State and Local Government Finance and Policy

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 in Minnesota Statutes, chapter 13; proposing coding for new law as Minnesota

1.6 Statutes, chapter 325O.

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

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

1.9 Subdivision 1. Scope. The sections referred to in this section are codified outside this

1.10 chapter. Those sections classify attorney general data as other than public, place restrictions

1.11 on access to government data, or involve data sharing.

1.12 Subd. 2. Data privacy and protection assessments. A data privacy and protection

1.13 assessment collected or maintained by the attorney general is classified under section

1.14 325O.08.

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

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

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

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

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

1.20 control with, another legal entity. For these purposes, "control" or "controlled" means:

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

2.1 class of voting security of a company; control in any manner over the election of a majority
2.2 of the directors or of individuals exercising similar functions; or the power to exercise a
2.3 controlling influence over the management of a company.

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

2.8 (d) "Biometric data" means data generated by automatic measurements of an individual's
2.9 biological characteristics, including a fingerprint, a voiceprint, eye retinas, irises, or other
2.10 unique biological patterns or characteristics that are used to identify a specific individual.

2.11 Biometric data does not include:

2.12 (1) a digital or physical photograph;

2.13 (2) an audio or video recording; or

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

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

2.17 (f) "Consent" means any freely given, specific, informed, and unambiguous indication
2.18 of the consumer's wishes by which the consumer signifies agreement to the processing of
2.19 personal data relating to the consumer. Acceptance of a general or broad terms of use or
2.20 similar document that contains descriptions of personal data processing along with other,
2.21 unrelated information does not constitute consent. Hovering over, muting, pausing, or closing
2.22 a given piece of content does not constitute consent. A consent is not valid when the
2.23 consumer's indication has been obtained by a dark pattern. A consumer may revoke consent
2.24 previously given, consistent with this chapter.

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

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

2.30 (i) "Decisions that produce legal or similarly significant effects concerning the consumer"
2.31 means decisions made by the controller that result in the provision or denial by the controller
2.32 of financial or lending services, housing, insurance, education enrollment or opportunity,

3.1 criminal justice, employment opportunities, health care services, or access to essential goods
3.2 or services.

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

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

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

3.10 (2) publicly commits to process the data only in a deidentified fashion and not attempt
3.11 to reidentify the data; and

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

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

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

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

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

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

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

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

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

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

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

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

4.14 (2) the disclosure of personal data to a third party for purposes of providing a product
4.15 or service requested by the consumer;

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

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

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

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

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

4.25 (2) the processing of biometric data or genetic information for the purpose of uniquely
4.26 identifying an individual;

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

4.28 (4) specific geolocation data.

4.29 (w) "Specific geolocation data" means information derived from technology, including,
4.30 but not limited to, global positioning system level latitude and longitude coordinates or
4.31 other mechanisms, that directly identifies the geographic coordinates of a consumer or a
4.32 device linked to a consumer with an accuracy of more than three decimal degrees of latitude

5.1 and longitude or the equivalent in an alternative geographic coordinate system, or a street
5.2 address derived from these coordinates. Specific geolocation data does not include the
5.3 content of communications, the contents of databases containing street address information
5.4 which are accessible to the public as authorized by law, or any data generated by or connected
5.5 to advanced utility metering infrastructure systems or other equipment for use by a public
5.6 utility.

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

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

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

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

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

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

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

5.22 **Sec. 4. [3250.03] SCOPE; EXCLUSIONS.**

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

5.26 (1) during a calendar year, controls or processes personal data of 100,000 consumers or
5.27 more, excluding personal data controlled or processed solely for the purpose of completing
5.28 a payment transaction; or

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

6.1 (b) A controller or processor acting as a technology provider under section 13.32 shall
6.2 comply with both this chapter and section 13.32, except that, when the provisions of section
6.3 13.32 conflict with this chapter, section 13.32 prevails.

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

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

6.7 (2) a federally recognized Indian tribe;

6.8 (3) information that meets the definition of:

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

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

6.12 (iii) patient identifying information for purposes of Code of Federal Regulations, title
6.13 42, part 2, established pursuant to United States Code, title 42, section 290dd-2;

6.14 (iv) identifiable private information for purposes of the federal policy for the protection
6.15 of human subjects, Code of Federal Regulations, title 45, part 46; identifiable private
6.16 information that is otherwise information collected as part of human subjects research
6.17 pursuant to the good clinical practice guidelines issued by the International Council for
6.18 Harmonisation; the protection of human subjects under Code of Federal Regulations, title
6.19 21, parts 50 and 56; or personal data used or shared in research conducted in accordance
6.20 with one or more of the requirements set forth in this paragraph;

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

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

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

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

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

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

7.2 (iii) a program or a qualified service organization as defined by Code of Federal
7.3 Regulations, title 42, part 2, established pursuant to United States Code, title 42, section
7.4 290dd-2;

7.5 (6) information that is:

7.6 (i) maintained by an entity that meets the definition of health care provider at Code of
7.7 Federal Regulations, title 45, section 160.103, to the extent that the entity maintains the
7.8 information in the manner required of covered entities with respect to protected health
7.9 information for purposes of the Health Insurance Portability and Accountability Act of
7.10 1996, Public Law 104-191, and related regulations; or

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

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

7.16 (8) an activity involving the collection, maintenance, disclosure, sale, communication,
7.17 or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit
7.18 capacity, character, general reputation, personal characteristics, or mode of living by a
7.19 consumer reporting agency, as defined in United States Code, title 15, section 1681a(f), by
7.20 a furnisher of information, as set forth in United States Code, title 15, section 1681s-2, who
7.21 provides information for use in a consumer report, as defined in United States Code, title
7.22 15, section 1681a(d), and by a user of a consumer report, as set forth in United States Code,
7.23 title 15, section 1681b, except that information is only excluded under this paragraph to the
7.24 extent that such activity involving the collection, maintenance, disclosure, sale,
7.25 communication, or use of such information by that agency, furnisher, or user is subject to
7.26 regulation under the federal Fair Credit Reporting Act, United States Code, title 15, sections
7.27 1681 to 1681x, and the information is not collected, maintained, used, communicated,
7.28 disclosed, or sold except as authorized by the Fair Credit Reporting Act;

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

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

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

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

8.10 (13) data collected or maintained:

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

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

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

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

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

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

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

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

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

9.6 (19) a small business as defined by the United States Small Business Administration
9.7 under Code of Federal Regulations, title 13, part 121, except that such a small business is
9.8 subject to section 325O.075; and

9.9 (20) a nonprofit organization that is established to detect and prevent fraudulent acts in
9.10 connection with insurance.

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

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

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

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

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

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

9.30 (c) A contract between a controller and a processor shall govern the processor's data
9.31 processing procedures with respect to processing performed on behalf of the controller. The
9.32 contract shall be binding and clearly set forth instructions for processing data, the nature
9.33 and purpose of processing, the type of data subject to processing, the duration of processing,

10.1 and the rights and obligations of both parties. The contract shall also require that the
10.2 processor:

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

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

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

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

10.18 (1) at the choice of the controller, the processor shall delete or return all personal data
10.19 to the controller as requested at the end of the provision of services, unless retention of the
10.20 personal data is required by law;

10.21 (2) upon a reasonable request from the controller, the processor shall make available to
10.22 the controller all information necessary to demonstrate compliance with the obligations in
10.23 this chapter; and

10.24 (3) the processor shall allow for, and contribute to, reasonable assessments and inspections
10.25 by the controller or the controller's designated assessor. Alternatively, the processor may
10.26 arrange for a qualified and independent assessor to conduct, at least annually and at the
10.27 processor's expense, an assessment of the processor's policies and technical and organizational
10.28 measures in support of the obligations under this chapter. The assessor must use an
10.29 appropriate and accepted control standard or framework and assessment procedure for such
10.30 assessments as applicable, and shall provide a report of such assessment to the controller
10.31 upon request.

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

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

11.10 **Sec. 6. [3250.05] CONSUMER PERSONAL DATA RIGHTS.**

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

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

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

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

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

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

11.29 (g) If a consumer's personal data is profiled in furtherance of decisions that produce
11.30 legal effects concerning a consumer or similarly significant effects concerning a consumer,
11.31 the consumer has the right to question the result of such profiling and be informed of the
11.32 reason that the profiling resulted in the decision, as well as the actions that the consumer
11.33 might have taken to secure a different decision and the actions that the consumer might take

12.1 to secure a different decision in the future. The consumer has the right to review the
12.2 customer's personal data used in the profiling. If the decision is determined to have been
12.3 based upon inaccurate personal data, the consumer has the right to have the data corrected
12.4 and the profiling decision reevaluated based upon the corrected data.

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

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

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

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

12.19 (1) not unfairly disadvantage another controller;

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

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

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

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

12.29 (b) If a consumer's opt-out request is exercised through the platform, technology, or
12.30 mechanism required under paragraph (a), and the request conflicts with the consumer's
12.31 existing controller-specific privacy setting or voluntary participation in a controller's bona
12.32 fide loyalty, rewards, premium features, discounts, or club card program, the controller
12.33 must comply with the consumer's opt-out preference signal but may also notify the consumer

13.1 of the conflict and provide the consumer a choice to confirm the controller-specific privacy
13.2 setting or participation in such program.

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

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

13.7 Subd. 4. **Controller response to consumer requests.** (a) Except as provided in this
13.8 chapter, a controller must comply with a request to exercise the rights pursuant to subdivision
13.9 1.

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

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

13.17 (d) A controller must comply with a request to exercise the right in subdivision 1,
13.18 paragraph (f), as soon as feasibly possible, but no later than 45 days of receipt of the request.

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

13.25 (f) If a controller does not take action on a consumer's request, the controller must inform
13.26 the consumer without undue delay and at the latest within 45 days of receipt of the request
13.27 of the reasons for not taking action and instructions for how to appeal the decision with the
13.28 controller as described in subdivision 5.

13.29 (g) Information provided under this section must be provided by the controller free of
13.30 charge, up to twice annually to the consumer. Where requests from a consumer are manifestly
13.31 unfounded or excessive, in particular because of their repetitive character, the controller
13.32 may either charge a reasonable fee to cover the administrative costs of complying with the

14.1 request, or refuse to act on the request. The controller bears the burden of demonstrating
14.2 the manifestly unfounded or excessive character of the request.

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

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

14.16 (1) Social Security number;

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

14.18 (3) financial account number;

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

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

14.21 (6) biometric data.

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

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

14.27 (1) retaining a record of the deletion request, retaining the minimum data necessary for
14.28 the purpose of ensuring the consumer's personal data remains deleted from the business's
14.29 records, and not using the retained data for any other purpose pursuant to the provisions of
14.30 this chapter; or

14.31 (2) opting the consumer out of the processing of such personal data for any purpose
14.32 except for those exempted pursuant to the provisions of this chapter.

15.1 Subd. 5. **Appeal process required.** (a) A controller must establish an internal process
15.2 whereby a consumer may appeal a refusal to take action on a request to exercise any of the
15.3 rights under subdivision 1 within a reasonable period of time after the consumer's receipt
15.4 of the notice sent by the controller under subdivision 4, paragraph (f).

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

15.7 (c) Within 45 days of receipt of an appeal, a controller must inform the consumer of any
15.8 action taken or not taken in response to the appeal, along with a written explanation of the
15.9 reasons in support thereof. That period may be extended by 60 additional days where
15.10 reasonably necessary, taking into account the complexity and number of the requests serving
15.11 as the basis for the appeal. The controller must inform the consumer of any such extension
15.12 within 45 days of receipt of the appeal, together with the reasons for the delay. If the appeal
15.13 is denied, the controller must also provide the consumer with an email address or other
15.14 online mechanism through which the consumer may submit the appeal, along with any
15.15 action taken or not taken by the controller in response to the appeal and the controller's
15.16 written explanation of the reasons in support thereof, to the attorney general.

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

15.23 Sec. 7. **[3250.06] PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS**
15.24 **DATA.**

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

15.27 (1) reidentify deidentified data;

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

15.31 (3) comply with an authenticated consumer request to access, correct, delete, or port
15.32 personal data pursuant to section 3250.05, subdivision 1, if all of the following are true:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17.7 (7) a description of the controller's retention policies for personal data;

17.8 (8) the date the privacy notice was last updated.

17.9 (b) If a controller sells personal data to third parties, processes personal data for targeted
17.10 advertising, or engages in profiling in furtherance of decisions that produce legal effects
17.11 concerning a consumer or similarly significant effects concerning a consumer, it must
17.12 disclose such processing in the privacy notice and provide access to a clear and conspicuous
17.13 method outside the privacy notice for a consumer to opt out of the sale, processing, or
17.14 profiling in furtherance of decisions that produce legal effects concerning a consumer or
17.15 similarly significant effects concerning a consumer. This method may include but is not
17.16 limited to an internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your Privacy
17.17 Rights" that directly effectuates the opt-out request or takes consumers to a web page where
17.18 the consumer can make the opt-out request.

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

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

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

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

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

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

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

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

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

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

19.1 (f) A controller may not process the personal data of a consumer for purposes of targeted
19.2 advertising, or sell the consumer's personal data, without the consumer's consent, under
19.3 circumstances where the controller knows that the consumer is between the ages of 13 and
19.4 16.

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

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

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

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

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

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

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

20.1 **Sec. 9. [325O.075] REQUIREMENTS FOR SMALL BUSINESSES.**

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

20.6 (b) Penalties and attorney general enforcement procedures under section 325O.10 apply
20.7 to a small business that violates this section.

20.8 **Sec. 10. [325O.08] DATA PRIVACY AND PROTECTION ASSESSMENTS.**

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

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

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

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

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

20.19 (iii) establish, implement, and maintain reasonable administrative, technical, and physical
20.20 data security practices to protect the confidentiality, integrity, and accessibility of personal
20.21 data;

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

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

20.26 (vi) identify and remediate violations of this act;

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

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

20.30 (ii) the sale of personal data;

- 21.1 (iii) the processing of sensitive data;
- 21.2 (iv) any processing activities involving personal data that present a heightened risk of
21.3 harm to consumers; and
- 21.4 (v) the processing of personal data for purposes of profiling, where such profiling presents
21.5 a reasonably foreseeable risk of:
- 21.6 (A) unfair or deceptive treatment of, or disparate impact on, consumers;
- 21.7 (B) financial, physical, or reputational injury to consumers;
- 21.8 (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or
21.9 concerns, of consumers, where such intrusion would be offensive to a reasonable person;
21.10 or
- 21.11 (D) other substantial injury to consumers; and
- 21.12 (4) a description of the data dictionary, metadata catalog, or other means by which the
21.13 controller maintains its inventory of data that must be managed to exercise its responsibilities
21.14 under section 325O.05.
- 21.15 (b) A data privacy and protection assessment must take into account the type of personal
21.16 data to be processed by the controller, including the extent to which the personal data are
21.17 sensitive data, and the context in which the personal data are to be processed.
- 21.18 (c) A data privacy and protection assessment must identify and weigh the benefits that
21.19 may flow directly and indirectly from the processing to the controller, consumer, other
21.20 stakeholders, and the public against the potential risks to the rights of the consumer associated
21.21 with such processing, as mitigated by safeguards that can be employed by the controller to
21.22 reduce such risks. The use of deidentified data and the reasonable expectations of consumers,
21.23 as well as the context of the processing and the relationship between the controller and the
21.24 consumer whose personal data will be processed, must be factored into this assessment by
21.25 the controller.
- 21.26 (d) As part of a civil investigative demand, the attorney general may request, in writing,
21.27 that a controller disclose any data privacy and protection assessment that is relevant to an
21.28 investigation conducted by the attorney general. The controller must make a data privacy
21.29 and protection assessment available to the attorney general upon such a request. The attorney
21.30 general may evaluate the data privacy and protection assessments for compliance with this
21.31 chapter . Data privacy and protection assessments are classified as nonpublic data, as defined
21.32 by section 13.02, subdivision 9. The disclosure of a data privacy and protection assessment
21.33 pursuant to a request from the attorney general under this paragraph does not constitute a

22.1 waiver of the attorney-client privilege or work product protection with respect to the
22.2 assessment and any information contained in the assessment.

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

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

22.8 **Sec. 11. [3250.09] LIMITATIONS AND APPLICABILITY.**

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

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

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

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

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

22.18 (5) provide a product or service specifically requested by a consumer, perform a contract
22.19 to which the consumer is a party, including fulfilling the terms of a written warranty, or
22.20 take steps at the request of the consumer prior to entering into a contract;

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

22.24 (7) prevent, detect, protect against, or respond to security incidents, identity theft, fraud,
22.25 harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity
22.26 or security of systems; or investigate, report, or prosecute those responsible for any such
22.27 action;

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

22.30 (9) engage in public or peer-reviewed scientific, historical, or statistical research in the
22.31 public interest that adheres to all other applicable ethics and privacy laws and is approved,

23.1 monitored, and governed by an institutional review board, human subjects research ethics
23.2 review board, or a similar independent oversight entity which has determined that:

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

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

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

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

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

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

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

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

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

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

23.26 (c) The obligations imposed on controllers or processors under this chapter do not apply
23.27 where compliance by the controller or processor with this chapter would violate an
23.28 evidentiary privilege under Minnesota law and do not prevent a controller or processor from
23.29 providing personal data concerning a consumer to a person covered by an evidentiary
23.30 privilege under Minnesota law as part of a privileged communication.

23.31 (d) A controller or processor that discloses personal data to a third-party controller or
23.32 processor in compliance with the requirements of this chapter is not in violation of this

24.1 chapter if the recipient processes such personal data in violation of this chapter, provided
24.2 that, at the time of disclosing the personal data, the disclosing controller or processor did
24.3 not have actual knowledge that the recipient intended to commit a violation. A third-party
24.4 controller or processor receiving personal data from a controller or processor in compliance
24.5 with the requirements of this chapter is likewise not in violation of this chapter for the
24.6 obligations of the controller or processor from which it receives such personal data.

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

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

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

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

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

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

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

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

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

24.29 **Sec. 12. [3250.10] ATTORNEY GENERAL ENFORCEMENT.**

24.30 (a) In the event that a controller or processor violates this chapter, the attorney general,
24.31 prior to filing an enforcement action under paragraph (b), must provide the controller or
24.32 processor with a warning letter identifying the specific provisions of this chapter the attorney

25.1 general alleges have been or are being violated. If, after 30 days of issuance of the warning
25.2 letter, the attorney general believes the controller or processor has failed to cure any alleged
25.3 violation, the attorney general may bring an enforcement action under paragraph (b). This
25.4 paragraph expires January 31, 2026.

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

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

25.12 (d) Nothing in this chapter establishes a private right of action, including under section
25.13 8.31, subdivision 3a, for a violation of this chapter or any other law.

25.14 Sec. 13. **[3250.11] PREEMPTION OF LOCAL LAW; SEVERABILITY.**

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

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

25.21 Sec. 14. **EFFECTIVE DATE.**

25.22 This act is effective July 31, 2025, except that postsecondary institutions regulated by
25.23 the Office of Higher Education and nonprofit corporations governed by Minnesota Statutes,
25.24 chapter 317A, are not required to comply with this act until July 31, 2029.